# Contents

## Preface

<table>
<thead>
<tr>
<th>Audience</th>
<th>viii</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation Accessibility</td>
<td>viii</td>
</tr>
<tr>
<td>Related Documents</td>
<td>ix</td>
</tr>
<tr>
<td>Conventions</td>
<td>ix</td>
</tr>
</tbody>
</table>

## 1 Get Started with Administration

<table>
<thead>
<tr>
<th>About Oracle Analytics Cloud</th>
<th>1-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region Availability</td>
<td>1-2</td>
</tr>
<tr>
<td>Service Limits</td>
<td>1-2</td>
</tr>
<tr>
<td>Service Quotas</td>
<td>1-3</td>
</tr>
<tr>
<td>Service Events</td>
<td>1-3</td>
</tr>
<tr>
<td>Typical Workflow for Administrators</td>
<td>1-5</td>
</tr>
<tr>
<td>Before You Begin with Oracle Analytics Cloud</td>
<td>1-6</td>
</tr>
</tbody>
</table>

## 2 Create Services with Oracle Analytics Cloud

<table>
<thead>
<tr>
<th>Typical Workflow to Create a Service</th>
<th>2-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before You Create a Service</td>
<td>2-2</td>
</tr>
<tr>
<td>Plan Your Service</td>
<td>2-2</td>
</tr>
<tr>
<td>Which Feature Set Do You Need?</td>
<td>2-2</td>
</tr>
<tr>
<td>Where Do You Want to Deploy Your Service?</td>
<td>2-2</td>
</tr>
<tr>
<td>Do You Need a Public or Private Endpoint?</td>
<td>2-3</td>
</tr>
<tr>
<td>What Sizing Options Are Available to You?</td>
<td>2-3</td>
</tr>
<tr>
<td>What Name Do You Want for Your Service?</td>
<td>2-8</td>
</tr>
<tr>
<td>Give Another User Permission to Set Up Oracle Analytics Cloud</td>
<td>2-8</td>
</tr>
<tr>
<td>Create a Compartment</td>
<td>2-8</td>
</tr>
<tr>
<td>Create a Service</td>
<td>2-9</td>
</tr>
<tr>
<td>Create a Service using the Console</td>
<td>2-9</td>
</tr>
<tr>
<td>Create a Service using the REST API</td>
<td>2-13</td>
</tr>
<tr>
<td>Create a Service using the Command Line</td>
<td>2-13</td>
</tr>
<tr>
<td>After You Create a Service</td>
<td>2-13</td>
</tr>
</tbody>
</table>
3

Administer Services

Typical Workflow to Administer a Service 3-1
View or Update a Service 3-2
  View or Update a Service using the Console 3-2
  View or Update a Service using the REST API 3-3
  View or Update a Service using the Command Line 3-3
Scale a Service 3-4
  About Scaling 3-4
  Scale Up or Down using the Console 3-6
  Scale Up or Down using the REST API 3-7
  Scale Up or Down using the Command Line 3-7
Pause and Resume a Service 3-7
  Pause and Resume using the Console 3-8
  Pause and Resume using the REST API 3-8
  Pause and Resume using the Command Line 3-8
Delete a Service 3-9
  Delete a Service using the Console 3-9
  Delete a Service using the REST API 3-9
  Delete a Service using the Command Line 3-10
Monitor a Service 3-10
  Monitor Status using the Console 3-10
  Monitor Status using the REST API 3-12
  Monitor Status using the Command Line 3-12
Find Oracle Analytics Cloud Resources 3-13
Read Usage Reports 3-14
Analyze Usage Costs for Oracle Analytics Cloud 3-14
Review Audit Logs for Oracle Analytics Cloud 3-15
Manage "Other Analytics" Services (North America and EMEA Only) 3-17
  FAQs About Managing Services Deployed in North America and EMEA 3-17
  View and Manage "Other Analytics" Services 3-22

4

Manage Service Access and Security

Give Users Permissions to Manage Analytics Cloud Instances 4-1
  About Permissions to Manage Oracle Analytics Cloud Instances 4-1
<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a Private Access Channel</td>
</tr>
<tr>
<td>Delete a Private Access Channel using the Console</td>
</tr>
<tr>
<td>Delete a Private Access Channel using the REST API</td>
</tr>
<tr>
<td>Delete a Private Access Channel using the Command Line</td>
</tr>
<tr>
<td>Connect to a Database Deployed on Oracle Cloud Infrastructure with a Public IP Address</td>
</tr>
<tr>
<td>Connect to a Database Deployed on Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Prerequisites</td>
</tr>
<tr>
<td>Record Database Information</td>
</tr>
<tr>
<td>Enable Database Access Through Port 1521</td>
</tr>
<tr>
<td>Connect to Your Database from Oracle Analytics Cloud</td>
</tr>
<tr>
<td>Connect to Your Database for Data Visualization</td>
</tr>
<tr>
<td>Connect to Your Database for Data Modeler</td>
</tr>
<tr>
<td>Connect to Your Database in Oracle Analytics Cloud Developer Client Tool</td>
</tr>
<tr>
<td>Connect to Oracle Autonomous Data Warehouse with a Public IP Address</td>
</tr>
<tr>
<td>Connect to Oracle Autonomous Data Warehouse</td>
</tr>
<tr>
<td>Prerequisites</td>
</tr>
<tr>
<td>Enable Access to Oracle Autonomous Data Warehouse</td>
</tr>
<tr>
<td>Connect to Oracle Autonomous Data Warehouse</td>
</tr>
<tr>
<td>Connect to Autonomous Data Warehouse for Data Visualization</td>
</tr>
<tr>
<td>Connect to Autonomous Data Warehouse for Data Modeler</td>
</tr>
<tr>
<td>Connect to Autonomous Data Warehouse in Oracle Analytics Cloud Developer Client Tool</td>
</tr>
<tr>
<td>Connect to a Database Deployed on Oracle Cloud Infrastructure Classic with a Public IP Address</td>
</tr>
<tr>
<td>Connect to a Database Deployed on Oracle Cloud Infrastructure Classic</td>
</tr>
<tr>
<td>Prerequisites</td>
</tr>
<tr>
<td>Record Database Information</td>
</tr>
<tr>
<td>Enable Database Access Through Port 1521</td>
</tr>
<tr>
<td>Connect to Your Database from Oracle Analytics Cloud</td>
</tr>
<tr>
<td>Connect to Your Database for Data Visualization</td>
</tr>
<tr>
<td>Connect to Your Database for Data Modeler</td>
</tr>
<tr>
<td>Connect to Your Database in Oracle Analytics Cloud Developer Client Tool</td>
</tr>
<tr>
<td>Federate with Oracle Identity Cloud Service Manually</td>
</tr>
<tr>
<td>Set Up a Custom Vanity URL</td>
</tr>
<tr>
<td>About Vanity URLs</td>
</tr>
<tr>
<td>Typical Workflow to Set Up a Vanity URL</td>
</tr>
<tr>
<td>Prerequisites for a Vanity URL</td>
</tr>
<tr>
<td>Configure a Vanity URL</td>
</tr>
<tr>
<td>Configure a Vanity URL using the Console</td>
</tr>
</tbody>
</table>
Preface

Learn how to create and manage services with Oracle Analytics Cloud on Oracle Cloud Infrastructure.

Topics:

• Audience
• Documentation Accessibility
• Related Documents
• Conventions

Audience

Administering Oracle Analytics Cloud on Oracle Cloud Infrastructure (Gen 2) is intended for administrators who set up Oracle Analytics Cloud on Oracle Cloud Infrastructure.

• **Administrators** set up services with Oracle Analytics Cloud and manage access to those services.
• **Analysts** load and model data and create reports and data visualizations 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 and data visualizations. Dashboards allow consumers to quickly analyze and manage activity across their system.

Documentation Accessibility

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

Access to Oracle Support

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

These related Oracle resources provide more information.

- Getting Started with Oracle Analytics Cloud
- Visualizing Data and Building Reports in Oracle Analytics Cloud
- Preparing Data in Oracle Analytics Cloud

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><strong>boldface</strong></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><strong>italic</strong></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></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 and what you need to know to get started with deployment and administration on Oracle Cloud Infrastructure Gen 2.

**Note:**

If your Oracle Analytics Cloud subscription started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2, read these topics to find out what's new and different:

- **North America:** See Get Started with Oracle Analytics Cloud (North America) - Accounts Started Before 14th February 2020.
- **EMEA:** See Get Started with Oracle Analytics Cloud (EMEA) - Accounts Started Before 2nd March 2020.

**Topics**

- About Oracle Analytics Cloud
- Typical Workflow for Administrators
- Before You Begin with Oracle Analytics Cloud

**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.

Oracle Analytics Cloud is available on Oracle Cloud Infrastructure in several regions in North America, EMEA, APAC, and LAD when you subscribe through Universal Credits. You can subscribe to Professional Edition or Enterprise Edition.

When you deploy Oracle Analytics Cloud, you complete some initial setup steps, and then Oracle takes care of most service management, patching, backup and restore, and other maintenance tasks. You determine the size of your service when you set up the service and you can increase or decrease capacity if your requirements change.

Oracle Analytics Cloud offers two sizing options, you can specify the number of Oracle Compute Units (OCPUs) you want to deploy or how many people you expect to use the service.

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

Oracle Analytics Cloud is currently available on several data regions in North America, Europe, the Middle East and Africa (EMEA), Asia-Pacific (APAC), and Latin American (LAD). Thereafter, Oracle Analytics Cloud will expand to other regions.

For the latest information on availability in regions, see Data Regions for Platform and Infrastructure Services.

Service Limits

Oracle Analytics Cloud has various default limits. Whenever you create an Oracle Analytics Cloud instance or scale up, the system ensures that your request is within the bounds of your limit. The limit that applies to you depends on which edition you subscribe to: Professional Edition or Enterprise Edition.

<table>
<thead>
<tr>
<th>Resource Limit</th>
<th>Limit Short Name</th>
<th>Default Value (Universal Credits)</th>
<th>Default Value (Trials)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Edition OCPUs</td>
<td>ee-ocpu-count</td>
<td>12</td>
<td>4</td>
<td>Maximum number of OCPUs available with Oracle Analytics Cloud Enterprise Edition.</td>
</tr>
</tbody>
</table>

You can submit a request to increase your limits from Limits, Quotas, and Usage page in Oracle Cloud Infrastructure Console.

See About Service Limits and Usage.
Service Quotas

You can use quotas to determine how other users allocate Oracle Analytics Cloud resources across compartments in Oracle Cloud Infrastructure. Whenever you create an Oracle Analytics Cloud instance or scale up, the system ensures that your request is within the bounds of the quota for that compartment.

The quota that you use to allocate Oracle Analytics Cloud resources depends on which edition you subscribe to: Professional Edition or Enterprise Edition.

<table>
<thead>
<tr>
<th>Quota Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>se-ocpu-count</td>
<td>Regional</td>
<td>Number of Professional Edition OCPUs.</td>
</tr>
<tr>
<td>ee-ocpu-count</td>
<td>Regional</td>
<td>Number of Enterprise Edition OCPUs.</td>
</tr>
<tr>
<td>se-user-count</td>
<td>Regional</td>
<td>Number of Professional Edition users.</td>
</tr>
<tr>
<td>ee-user-count</td>
<td>Regional</td>
<td>Number of Enterprise Edition users.</td>
</tr>
</tbody>
</table>

Example Quota Statements for Oracle Analytics Cloud

- **Limit the number of OCPUs that users can allocate to self-service analytics services they create in MyDVCompartment to 2.**
  
  ```
  set analytics quota se-ocpu-count to 2 in compartment MyDVCompartment
  ```

- **Limit the number of OCPUs that users can allocate to enterprise analytics services they create in MyEnterpriseCompartment to 10.**
  
  ```
  set analytics quota ee-ocpu-count to 10 in compartment MyEnterpriseCompartment
  ```

- **Limit the user count for enterprise analytics services that users create in MyEnterpriseCompartment to 100.**
  
  ```
  set analytics quota ee-user-count to 100 in compartment MyEnterpriseCompartment
  ```

- **Don’t allow users to allocate any OCPUs to enterprise analytics services in MyTestCompartment.**
  
  ```
  zero analytics quota ee-ocpu-count in compartment MyTestCompartment
  ```

See [About Compartment Quotas](#).

Service Events

Actions that you perform on Oracle Analytics Cloud instances emit events.

You can define rules that trigger a specific action when an event occurs. For example, you might define a rule that sends a notification to administrators when someone deletes an instance. See [Overview of Events](#) and [Get Started with Events](#).

This table lists the Oracle Analytics Cloud events that you can reference.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics - Instance - Create Instance</td>
<td>com.oraclecloud.analytics.createanalyticsinstance</td>
</tr>
<tr>
<td>Analytics - Instance - Delete Instance</td>
<td>com.oraclecloud.analytics.deleteanalyticsinstance</td>
</tr>
<tr>
<td>Analytics - Instance - Scale Instance Up or Down Begin</td>
<td>com.oraclecloud.analytics.scaleanalyticsinstance.begin</td>
</tr>
<tr>
<td>Analytics - Instance - Scale Instance Up or Down End</td>
<td>com.oraclecloud.analytics.scaleanalyticsinstance.end</td>
</tr>
<tr>
<td>Analytics - Instance - Start Instance Begin</td>
<td>com.oraclecloud.analytics.startanalyticsinstance.begin</td>
</tr>
<tr>
<td>Analytics - Instance - Start Instance End</td>
<td>com.oraclecloud.analytics.startanalyticsinstance.end</td>
</tr>
<tr>
<td>Analytics - Instance - Stop Instance Begin</td>
<td>com.oraclecloud.analytics.stopanalyticsinstance.begin</td>
</tr>
<tr>
<td>Analytics - Instance - Stop Instance End</td>
<td>com.oraclecloud.analytics.stopanalyticsinstance.end</td>
</tr>
<tr>
<td>Analytics - Instance - Update Instance</td>
<td>com.oraclecloudanalytics.updateanalyticsinstance</td>
</tr>
<tr>
<td>Analytics - Instance - Change Compartment</td>
<td>com.oraclecloud.analytics.changeanalyticsinstance.compartment</td>
</tr>
</tbody>
</table>

**Example**

This example shows information associated with the event **Analytics - Instance - Create Instance**:

```json
{
    "cloudEventsVersion": "0.1",
    "contentType": "application/json",
    "source": "analytics",
    "eventID": "<unique_ID>",
    "eventType": "com.oraclecloud.analytics.createanalyticsinstance",
    "eventTime": "2019-10-19T00:53:04.126Z",
    "data": {
        "additionalDetails": {},
        "availabilityDomain": "<availability_domain>",
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
        "compartmentName": "my_compartment",
        "freeformTags": {},
        "resourceId": "ocid1.analyticsinstance.oc1..<unique_ID>",
        "resourceName": "my_analytics_cloud"
    },
    "extensions": {
        "compartmentId": "ocid1.compartment.oc1..<unique_ID>"
    }
}
```
## Typical Workflow for Administrators

If you’re setting up Oracle Analytics Cloud 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>Place an order for Oracle Analytics Cloud or sign up for a free Oracle Cloud promotion</td>
<td>Sign up for a free credit promotion or subscribe to Oracle Analytics Cloud through Universal Credits. See Data Regions for Platform and Infrastructure Services.</td>
<td>Request and Manage Free Oracle Cloud Promotions Upgrade to a Paid Account</td>
</tr>
<tr>
<td>Activate your Oracle Cloud account and sign in for the first time</td>
<td>You receive a welcome email when your account is ready. To activate your account, you must sign in with the credentials provided in the email. As the Cloud Account Administrator, you can complete all the setup tasks for Oracle Analytics Cloud.</td>
<td>Signing in for the First Time</td>
</tr>
<tr>
<td>Determine your service requirements</td>
<td>Plan your Oracle Analytics Cloud deployment. Think about what you need before you start.</td>
<td>Plan Your Service</td>
</tr>
<tr>
<td>(Optional) Enable other users to set up services</td>
<td>If you don’t want to set up Oracle Analytics Cloud yourself, give other users permissions to create services.</td>
<td>Give Another User Permission to Set Up Oracle Analytics Cloud</td>
</tr>
<tr>
<td>(Recommended) Create a compartment for your service</td>
<td>Create a compartment for your Oracle Analytics Cloud deployment.</td>
<td>Create a Compartment</td>
</tr>
<tr>
<td>(Optional) Federate your account with Oracle Identity Cloud Service</td>
<td>If you want to federate with a secondary Oracle Identity Cloud Service instance or your tenancy is a government region where federation isn’t set up automatically, you must federate with Oracle Identity Cloud Service manually.</td>
<td>Federate with Oracle Identity Cloud Service Manually</td>
</tr>
<tr>
<td>Create a service</td>
<td>Deploy a new service with Oracle Analytics Cloud.</td>
<td>Create a Service</td>
</tr>
<tr>
<td>Verify your service</td>
<td>When your service is ready, check that you can sign in and your service is up and running.</td>
<td>Verify Your Service and Sign In</td>
</tr>
<tr>
<td>Set up users and groups</td>
<td>Set up users and groups for Oracle Analytics Cloud in Oracle Identity Cloud Service and assign them to application roles.</td>
<td>Set Up Users, Groups, and Application Roles</td>
</tr>
<tr>
<td>Set service-level options</td>
<td>Configure service-level options for everyone using your service.</td>
<td>Configure Options for Your Service</td>
</tr>
<tr>
<td>Migrate content</td>
<td>Leverage your existing content in Oracle Analytics Cloud.</td>
<td>Migrate to Oracle Analytics Cloud from Other Environments</td>
</tr>
<tr>
<td>Administer services</td>
<td>Monitor services and perform administrative tasks such as pause, resume, scale, delete, and so on. Delegate administrative responsibilities to others through security policies.</td>
<td>Administer Services Give Users Permissions to Manage Analytics Cloud Instances</td>
</tr>
</tbody>
</table>
Before You Begin with Oracle Analytics Cloud

When you order Oracle Analytics Cloud through Universal Credits, you automatically get access to other required services, including Oracle Cloud Infrastructure and Oracle Identity Cloud Service.

Here’s some information about how Oracle Analytics Cloud uses other services and what you need to do if you’re setting up Oracle Analytics Cloud for the first time.

<table>
<thead>
<tr>
<th>Service</th>
<th>What is it for?</th>
<th>Do I need to do anything?</th>
</tr>
</thead>
</table>
| Oracle Cloud Infrastructure Identity and Access Management | You use compartments within your tenancy to organize resources on Oracle Cloud Infrastructure. In Oracle Cloud Infrastructure, you use IAM security policies to grant permissions. | Yes. Before you create your first Oracle Analytics Cloud instance, Oracle recommends that you set up one or more compartments in which you can deploy and secure your cloud resources.  
  - Setting Up Your Tenancy  
  - Managing Compartments  
  Optionally, you can give other users (or groups) permissions to set up and manage Oracle Analytics Cloud. See Give a User Permissions to Manage Analytics Cloud Instances. |
| Oracle Identity Cloud Service               | In most cases, Oracle Analytics Cloud is automatically federated with the primary Oracle Identity Cloud Service instance associated with your tenancy.  
You use Oracle Identity Cloud Service to create user accounts for the people in your organization who will use the Oracle Analytics Cloud services that you deploy. | Yes.  
You add users and groups and give them access to your Oracle Analytics Cloud deployments.  
You can add users and groups before you create the Oracle Analytics Cloud instance or after; you can decide. See Set Up Users, Groups, and Application Roles.  
**Note:** If you want to federate with a secondary Oracle Identity Cloud Service instance or your tenancy is a government region where federation isn't set up automatically, you must federate with Oracle Identity Cloud Service manually. See Federate with Oracle Identity Cloud Service Manually. |
Create Services with Oracle Analytics Cloud

As Cloud Account Administrator, you can create and set up services in Oracle Analytics Cloud for your organization.

Topics

• Typical Workflow to Create a Service
• Before You Create a Service
• Create a Service
• After You Create a Service

Typical Workflow to Create a Service

If you're about to create an Oracle Analytics Cloud instance on Oracle Cloud Infrastructure in using Oracle Cloud Infrastructure Console 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><strong>Before you start</strong></td>
<td>As the Cloud Account Administrator, you can complete all setup tasks for Oracle Analytics Cloud.</td>
<td>Request and Manage Free Oracle Cloud Promotions  Upgrade to a Paid Account</td>
</tr>
<tr>
<td>Activate your order and sign in to your Oracle Cloud account</td>
<td>Plan your Oracle Analytics Cloud deployment. Think about what you need before you start.</td>
<td>Plan Your Service</td>
</tr>
<tr>
<td>Determine your service requirements</td>
<td>If you don’t want to set up Oracle Analytics Cloud yourself, give other users permissions to create services.</td>
<td>Give Another User Permission to Set Up Oracle Analytics Cloud</td>
</tr>
<tr>
<td>(Optional) Enable other users to set up services</td>
<td>Create a compartment for your Oracle Analytics Cloud deployment.</td>
<td>Create a Compartment</td>
</tr>
<tr>
<td>(Recommended) Create a compartment for your service</td>
<td>Use Oracle Cloud Infrastructure Console to deploy a new service.</td>
<td>Create a Service</td>
</tr>
<tr>
<td><strong>Create the service</strong></td>
<td>When your service is ready, check that you can sign in and your service is up and running.</td>
<td>Verify Your Service and Sign In</td>
</tr>
<tr>
<td><strong>Complete the setup</strong></td>
<td>Set up users and groups for Oracle Analytics Cloud in Oracle Identity Cloud Service and assign them to application roles.</td>
<td>Set Up Users, Groups, and Application Roles</td>
</tr>
</tbody>
</table>
Before You Create a Service

Before you set up Oracle Analytics Cloud on Oracle Cloud Infrastructure using Oracle Cloud Infrastructure Console, Oracle recommends that you take some time to plan your service.

- Plan Your Service
- Give Another User Permission to Set Up Oracle Analytics Cloud (Optional)
- Create a Compartment (Recommended)

Plan Your Service

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

- Which Feature Set Do You Need?
- Where Do You Want to Deploy Your Service?
- Do You Need a Public or Private Endpoint?
- What Sizing Options Are Available to You?
- What Name Do You Want for Your Service?

Which Feature Set Do You Need?

When you set up a service you must decide which feature set you want to deploy.

<table>
<thead>
<tr>
<th>Feature Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Service Analytics</td>
<td>Data visualization</td>
</tr>
<tr>
<td>Enterprise Analytics</td>
<td>Enterprise modeling, reporting, and data visualization</td>
</tr>
</tbody>
</table>

Where Do You Want to Deploy Your Service?

Oracle Cloud Infrastructure (Gen 2) is hosted in several different geographic areas, called regions. When you sign up for Oracle Analytics Cloud, Oracle creates a tenancy for your company with access to one or more regions. If multiple regions are available to you, decide where you want to deploy your Oracle Analytics Cloud instance.

To find out more, see Region Availability.
**Note:**

The way you deploy and manage Oracle Analytics Cloud depends on the region, type, and start date of your subscription. If your Oracle Analytics Cloud subscription started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure (Gen 2), the deployment process is different. See:

- **North America:** See Get Started with Oracle Analytics Cloud (North America) - Accounts Started Before 14th February 2020.
- **EMEA:** See Get Started with Oracle Analytics Cloud (EMEA) - Accounts Started Before 2nd March 2020.

**Do You Need a Public or Private Endpoint?**

When you create an Oracle Analytics Cloud instance, you specify how you want to access your service: through a *public internet accessible endpoint* or a *private endpoint*.

After you've created Oracle Analytics Cloud, you can't switch from a public endpoint to a private endpoint (or the other way around). So it's important to decide what type of access your organization needs and complete the required prerequisites before you start. See Prerequisites for a Public Endpoint and Prerequisites for a Private Endpoint.

If you're not sure, see About Public Endpoints and Access Control Rules and About Private Endpoints.

**What Sizing Options Are Available to You?**

When you create an Oracle Analytics Cloud instance, you either specify the number of Oracle Compute Units (OCPUs) you want to deploy or the number of people you expect to use the service.

- **How Many OCPUs Do You Think You'll Need?**
- **How Many People Do You Expect to Use the Service?**

**How Many OCPUs Do You Think You'll Need?**

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

The compute size you select also determines some configuration limits for the different types of content that users can create:

- Data visualization projects
- Classic analyses and dashboards
- Classic pixel-perfect reports

For example, limits such as the maximum number of input rows you can return from a data source query or the maximum number of rows you can download from a report to a file (for example, when you export to a CSV file).
• Limits Querying Data (Data Visualization Projects, Classic Analyses and Dashboards)
• Limits Displaying Data (Data Visualization Projects, Classic Analyses and Dashboards)
• Limits Exporting Data (Data Visualization Projects)
• Limits Exporting Data (Classic Analyses and Dashboards)
• Limits Delivering by Email (Classic Analyses and Dashboards)
• Data Size Limits (Classic Pixel-Perfect Reports)
• Processing Limits (Classic Pixel-Perfect Reports)

Limits Querying Data (Data Visualization Projects, Classic Analyses and Dashboards)

When you query a data source for data visualization projects or classic analyses and dashboards, the compute size determines the maximum number of rows that are returned from the data source.

<table>
<thead>
<tr>
<th>Which compute size do you think you'll need?</th>
<th>Limits when querying data for visualizations, analyses, and dashboards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max input rows returned from any data source query</td>
</tr>
<tr>
<td>1 OCPU (trials only)</td>
<td>125,000</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>8 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>10 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>12 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>16 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>24 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>36 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>52 OCPU</td>
<td>4,000,000</td>
</tr>
</tbody>
</table>

Limits Displaying Data (Data Visualization Projects, Classic Analyses and Dashboards)

When you display data in data visualization projects or classic analyses and dashboards, the compute size determines the maximum number of summarized rows returned from the data source that are displayed.
<table>
<thead>
<tr>
<th>Which compute size do you think you'll need?</th>
<th>Limits when displaying data in visualization projects, analyses, and dashboards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max summarized rows returned from any data source query</td>
</tr>
<tr>
<td>1 OCPU (trials only)</td>
<td>125,000</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>8 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>10 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>12 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>16 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>24 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>36 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>52 OCPU</td>
<td>1,000,000</td>
</tr>
</tbody>
</table>

**Limits Exporting Data (Data Visualization Projects)**

When you export data from a data visualization project, the compute size determines the maximum number of rows you can export.

<table>
<thead>
<tr>
<th>Which compute size do you think you'll need?</th>
<th>Limits when exporting data from data visualizations projects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum number of rows</td>
</tr>
<tr>
<td>1 OCPU (trials only)</td>
<td>125,000</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>8 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>10 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>12 OCPU</td>
<td>500,000</td>
</tr>
<tr>
<td>16 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>24 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>36 OCPU</td>
<td>1,000,000</td>
</tr>
<tr>
<td>52 OCPU</td>
<td>1,000,000</td>
</tr>
</tbody>
</table>

**Limits Exporting Data (Classic Analyses and Dashboards)**

When you export data from analyses and dashboards, the compute size determines the maximum number of rows you can export. There are different limits for formatted reports and unformatted reports.

- Unformatted report limits: formats such as CSV, Excel, XML, and Tab Delimited.
• Formatted report limits: formats such as PDF, Excel, Powerpoint, and Web Archive/HTML.

<table>
<thead>
<tr>
<th>Which compute size do you think you'll need?</th>
<th>Limits when exporting data from analyses and dashboards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max rows exported to unformatted reports</td>
</tr>
<tr>
<td>1 OCPU (trials only)</td>
<td>125,000</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>8 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>10 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>12 OCPU</td>
<td>2,000,000</td>
</tr>
<tr>
<td>16 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>24 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>36 OCPU</td>
<td>4,000,000</td>
</tr>
<tr>
<td>52 OCPU</td>
<td>4,000,000</td>
</tr>
</tbody>
</table>

Limits Delivering by Email (Classic Analyses and Dashboards)

When you send analyses and dashboards by email, the compute size determines the maximum number of rows you can deliver in a single email. There are different limits for delivering formatted reports and unformatted reports.

• Unformatted report limits: formats such as CSV, Excel, XML, and Tab Delimited.
• Formatted report limits: formats such as PDF, Excel, Powerpoint, and Web Archive/HTML.

<table>
<thead>
<tr>
<th>Which compute size do you think you'll need?</th>
<th>Limits when delivering analyses and dashboards by email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max rows in unformatted reports delivered by email</td>
</tr>
<tr>
<td>1 OCPU (trials only)</td>
<td>1,000</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>8 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>10 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>12 OCPU</td>
<td>50,000</td>
</tr>
<tr>
<td>16 OCPU</td>
<td>100,000</td>
</tr>
<tr>
<td>24 OCPU</td>
<td>100,000</td>
</tr>
<tr>
<td>36 OCPU</td>
<td>100,000</td>
</tr>
<tr>
<td>52 OCPU</td>
<td>100,000</td>
</tr>
</tbody>
</table>
## Data Size Limits (Classic Pixel-Perfect Reports)

The compute size determines several limits associated with generating reports.

<table>
<thead>
<tr>
<th>Which compute size do you think you’ll need?</th>
<th>Report data size limits when generating pixel-perfect reports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 OCPU (trials only)</td>
<td>Max data size for online reports</td>
<td>200MB</td>
</tr>
<tr>
<td>2 OCPU</td>
<td>Max data size for offline (scheduled) reports</td>
<td>500MB</td>
</tr>
<tr>
<td>4 OCPU</td>
<td>Max data size for bursting reports</td>
<td>500MB</td>
</tr>
<tr>
<td>6 OCPU</td>
<td>Max data size for data generation</td>
<td>500MB</td>
</tr>
<tr>
<td>8 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
<tr>
<td>10 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
<tr>
<td>12 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
<tr>
<td>24 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
<tr>
<td>36 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
<tr>
<td>52 OCPU</td>
<td></td>
<td>500MB</td>
</tr>
</tbody>
</table>

## Processing Limits (Classic Pixel-Perfect Reports)

The compute size determines several limits associated with processing reports.

<table>
<thead>
<tr>
<th>Which compute size do you think you’ll need?</th>
<th>Data model and report processing limits when generating pixel-perfect reports</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 OCPU (trials only)</td>
<td>SQL Query timeout (seconds)</td>
<td>1,800</td>
</tr>
<tr>
<td>2 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>4 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>6 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>8 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>10 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>12 OCPU</td>
<td></td>
<td>1,800</td>
</tr>
<tr>
<td>16 OCPU</td>
<td></td>
<td>3,600</td>
</tr>
<tr>
<td>24 OCPU</td>
<td></td>
<td>3,600</td>
</tr>
<tr>
<td>36 OCPU</td>
<td></td>
<td>3,600</td>
</tr>
<tr>
<td>52 OCPU</td>
<td></td>
<td>3,600</td>
</tr>
</tbody>
</table>
How Many People Do You Expect to Use the Service?

With Oracle Analytics Cloud, you can opt to specify how many people you expect to use the service. Typically, services have between 10 and 3000 users.

Configuration limits are equivalent to those available with 4 OCPUs. For example, the maximum number of input rows you can return from any data source query is 1,100,000 rows, the maximum number of rows you can export to a formatted report (such as PDF) is 200,000 rows, and so on.

What Name Do You Want for Your Service?

Think about a suitable name for your service. The name that you specify is displayed in Oracle Cloud Infrastructure Console and the URL for your service.

Name restrictions:

- Must contain between 1 and 25 characters.
- Must start with an ASCII letter: a to z or A to Z.
- Must contain only ASCII letters or numbers.
- Mustn't contain any other special characters.
- Must be unique within the identity domain.

Give Another User Permission to Set Up Oracle Analytics Cloud

When you activate your order for Oracle Analytics Cloud, you get the Cloud Account Administrator role. This role gives you full administration privileges in Oracle Cloud Infrastructure so you can complete all aspects of Oracle Analytics Cloud setup and much more. There's no need to delegate this responsibility but, if you want to, you can give someone else privileges to create and manage Oracle Analytics Cloud instances through the manage analytics-instances permission.

In Oracle Cloud Infrastructure you use IAM security policies to grant permissions. First, you must add the user to a group, and then you create a security policy that grants the group the manage analytics-instances permission on a specific compartment or the tenancy (any compartment in the tenancy). For example, you might create a policy statement that looks like one of these:

- allow group MyAdminGroup to manage analytics-instances in tenancy
- allow group MyAdminGroup to manage analytics-instances in compartment MyOracleAnalytics

To find out how to create security policy statements specifically for Oracle Analytics Cloud, see Give Users Permissions to Manage Analytics Cloud Instances.

Create a Compartment

When you sign up for Oracle Cloud Infrastructure, Oracle creates your tenancy with a root compartment that holds all your cloud resources. You then create additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment. Before you create an Oracle
Analytics Cloud instance, Oracle recommends that you set up the compartment where you want the instance to belong.

You create compartments in Oracle Cloud Infrastructure Identity and Access Management (IAM). See Setting Up Your Tenancy and Managing Compartments.

Create a Service

You can create an Oracle Analytics Cloud instance using the Console, API, or command line.

Note:

Required IAM Policy
Verb: manage
Resource Type: analytics-instance, analytics-instances
Custom Permission: ANALYTICS_INSTANCE_CREATE
See About Permissions to Manage Oracle Analytics Cloud Instances.

Additional IAM Policy Required to Create a Public Endpoint
Verb: read
Resource Type: virtual-network-family, compartment, compartments
See Prerequisites for a Public Endpoint.

Additional IAM Policy Required to Create a Private Endpoint
Verb: manage
Resource Type: virtual-network-family
Verb: read
Resource Type: compartment, compartments
To learn about other, more detailed access policy options, see Prerequisites for a Private Endpoint.

Topics
• Create a Service using the Console
• Create a Service using the REST API
• Create a Service using the Command Line

Create a Service using the Console

You can use Oracle Cloud Infrastructure Console to set up a service instance with Oracle Analytics Cloud.

1. Sign in to your Oracle Cloud account.
You must sign in as a federated Oracle Identity Cloud Service user and belong to an OCI group that is granted the required policies to create an Analytics instance. See Give Users Permissions to Manage Analytics Cloud Instances.

2. In Console, click in the top left corner.

3. Under Solutions and Platform, select Analytics, then Analytics Cloud.

4. From the Compartment list, select the compartment in which you want to create the service.

5. Click Create Instance.

6. Enter an Instance Name and a brief description. The name must start with a letter and can contain only letters and numbers.

7. Select the Feature Set you want to deploy.
• **Self-Service Analytics**: Deploys an instance with data visualization.

• **Enterprise Analytics**: Deploys an instance with enterprise modeling, reporting, and data visualization.

8. For **Capacity**, select the size of your deployment.

Configure the capacity type that matches your subscription, that is, either *OCPU per hour* or *User per month*.

• **OCPU**: For production services, select the number of OCPUs you want to deploy (between 2 and 52). If you want to create an instance for trial purposes, you can select 1 OCPU.

  Select this option if you plan to use your Oracle Middleware on-premise license with Oracle Analytics Cloud (BYOL).

• **Users**: Enter the number of users you expect to use this service.

  You can split your capacity over multiple services. For example, if you subscribe to 100 users per month, you might deploy a test instance for 10 users and a production instance with the remaining 90 users.

9. For **Licensing**, select **License Included** to subscribe to an Oracle Cloud license for Oracle Analytics Cloud or **Bring Your Own License (BYOL)** to use your Oracle Middleware on-premise license with Oracle Analytics Cloud and be charged the Bring Your Own License (BYOL) rate.

The **Bring Your Own License (BYOL)** option is available when you select **OCPU** for Capacity.

If you select **Users**, you must have an Oracle Cloud license for Oracle Analytics Cloud.

10. Use **Network Access** to specify how you want users to access Oracle Analytics Cloud: over the public internet or through a private network.

• **Public**: Enable access over the public internet.

  The Public option deploys Oracle Analytics Cloud with a public internet accessible endpoint. If required, you can configure access control rules to restrict access by public IP address, public CIDR block range, and VCN. See *Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint*.

• **Private**: Enable private access from an on-premise network or hosts on a virtual cloud network (VCN). Private access means that traffic doesn't go over the internet.

  The Private option deploys Oracle Analytics Cloud with a private endpoint. Before you configure this option, you must set up the Oracle Cloud Infrastructure VCN that you plan to use with a subnet for Oracle Analytics Cloud. See *Deploy Oracle Analytics Cloud with a Private Endpoint*.

You can modify the access control rules for a public endpoint or change the VCN and subnet for a private endpoint later on, if required. However, you can't change your network access selection from public to private (or private to public).

11. Verify that the details are correct, and click **Create**.

For example:
It takes about 20 minutes to create the service. Display the Instance page to check the current status.
Create a Service using the REST API

You can use the CreateAnalyticsInstance operation to set up a service instance with Oracle Analytics Cloud.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:

• CreateAnalyticsInstance

Create a Service using the Command Line

You can use the analytics-instance create command to set up a service instance with Oracle Analytics Cloud.

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use this command:

• analytics-instance create

After You Create a Service

After creating a service with Oracle Analytics Cloud, you must set up your users and configure additional options for your service. If you’re migrating to Oracle Analytics Cloud from on-premises or another cloud service you might want to migrate your existing content now.

• Verify Your Service and Sign In
• Set Up Users, Groups, and Application Roles
• Configure Options for Your Service
• Migrate to Oracle Analytics Cloud from Other Environments

Verify Your Service and Sign In

Oracle sends an email to the designated email address when your Oracle Analytics Cloud service is ready. Navigate to your service in Oracle Cloud Infrastructure Console, click the Analytics Home Page button, and then sign in to verify your Oracle Analytics Cloud service is up and running.

Note:

Required IAM Policy

Verb: read

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_READ

See About Permissions to Manage Oracle Analytics Cloud Instances.
1. In Console, click in the top left corner.

2. Under **Solutions and Platform**, select **Analytics**, then **Analytics Cloud**.

3. Select the compartment in which you created the instance.

4. Click the name of the new instance.

5. Click **Analytics Home Page**.

6. Sign in with your administrator credentials.

**Set Up Users, Groups, and Application Roles**

One of the first jobs you do after setting up a service with Oracle Analytics Cloud is to add user accounts in Oracle Identity Cloud Service for everyone you expect to use the service and then assign them suitable permissions in Oracle Analytics Cloud (also known as **application roles**).

Oracle Identity Cloud Service is available with your Oracle Analytics Cloud account.

1. **Add users and groups**.
   
   Use Oracle Identity Cloud Service to add users and groups. See Manage Users and Groups in Oracle Identity Cloud Service in *Administering Oracle Identity Cloud Service*.

2. **Assign users and groups permissions in Oracle Analytics Cloud**.
   
   Use the Console (Users and Roles page) in your Oracle Analytics Cloud service to give users and groups suitable application roles. See Manage What Users Can See and Do in *Configuring Oracle Analytics Cloud*.

**Configure Options for Your Service**

Administrators perform many critical duties; they control user permissions and amend accounts, set up database connections for data modelers, manage data storage to avoid exceeding storage limits, take regular snapshots so users don't risk losing their
work, authorize access to external content by registering safe domains, troubleshoot user queries, and much more. After setting up a service with Oracle Analytics Cloud, you can review typical administrator tasks for your service.

See Administrator Task List in *Configuring Oracle Analytics Cloud*.

**Migrate to Oracle Analytics Cloud from Other Environments**

Do you have content in an existing on-premise system or another cloud service that you want to leverage in Oracle Analytics Cloud? After setting up your service, you can migrate the content to the new environment.

<table>
<thead>
<tr>
<th>Migrate From...</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Oracle Analytics Cloud deployments on Oracle Cloud Infrastructure</td>
<td>Migrate Oracle Analytics Cloud Using Snapshots</td>
</tr>
<tr>
<td>Oracle Analytics Cloud - Classic deployed on Oracle Cloud Infrastructure Classic</td>
<td>Migrating Oracle Analytics Cloud - Classic Instances to Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Oracle BI Cloud Service</td>
<td>Migrating Oracle Business Intelligence Cloud Service Instances to Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Oracle Data Visualization Cloud Service</td>
<td>Migrating Oracle Data Visualization Cloud Service Instances to Oracle Cloud Infrastructure</td>
</tr>
<tr>
<td>Oracle BI Enterprise Edition</td>
<td>Migrating Oracle Business Intelligence Enterprise Edition to Oracle Analytics Cloud</td>
</tr>
</tbody>
</table>
Administer Services

You administer Oracle Analytics Cloud for your organization through Oracle Cloud Infrastructure Console.

Topics

- Typical Workflow to Administer a Service
- View or Update a Service
- Scale a Service
- Pause and Resume a Service
- Delete a Service
- Monitor a Service
- Find Oracle Analytics Cloud Resources
- Read Usage Reports
- Analyze Usage Costs for Oracle Analytics Cloud
- Review Audit Logs for Oracle Analytics Cloud
- Manage "Other Analytics" Services (North America and EMEA Only)

Typical Workflow to Administer a Service

After you create an Oracle Analytics Cloud instance with Oracle Cloud Infrastructure 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>
</table>
| View and update service       | View instances, edit details, move your instance to a different compartment, and
<p>| details                       | more. Use the search facility to find instances across compartments.        | View or Update a Service using the Console                                      |
|                               |                                                                            | Find Oracle Analytics Cloud Resources                                           |
| Scale a service up or down    | Increase or decrease the number of Oracle Compute Units (OCPUs) allocated to your service. | Scale a Service                                                                 |
| Pause or resume a service     | Pause a service to temporarily prevent users from accessing the service.    | Pause and Resume a Service                                                        |
| Delete a service              | Delete services that you don’t want anymore.                                | Delete a Service                                                                 |
| Monitor services              | Monitor the status of your service.                                         | Monitor a Service                                                                |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track usage and billing</td>
<td>Track usage and costs associated with your services.</td>
<td>Read Usage Reports&lt;br&gt;Analyze Usage Costs for Oracle Analytics Cloud&lt;br&gt;Review Audit Logs for Oracle Analytics Cloud</td>
</tr>
</tbody>
</table>

## View or Update a Service

You can access services and update instance details using the Console, API, or command line. You can edit details such as the description, license type, or tags.

**Note:**

**Required IAM Policy**

**Verb:** inspect (to view), manage (to update)

**Resource Types:** analytics-instance, analytics-instances

**Permission:** ANALYTICS_INSTANCE_INSPECT (to view), ANALYTICS_INSTANCE_UPDATE (to update)

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

### Topics

- View or Update a Service using the Console
- View or Update a Service using the REST API
- View or Update a Service using the Command Line

### View or Update a Service using the Console

You can use Oracle Cloud Infrastructure Console to view and edit Oracle Analytics Cloud instances.

1. Sign in to your Oracle Cloud account.

2. In Console, click in the top left corner.

3. Under **Solutions and Platform**, select **Analytics**, then **Analytics Cloud**.

4. Select the compartment that contains the Oracle Analytics Cloud instances you're looking for.
5. If required, filter the list by **State** or **Feature Set** to find the instance you want.

6. To change the description or the license type, click : for the instance, and select **Update**.

7. To edit or add tags, click the name of your instance to show the details page, and then click **Tags** or **Add Tags**.

**View or Update a Service using the REST API**

You use the `GetAnalyticsInstance` and `UpdateAnalyticsInstance` operations to return and edit Oracle Analytics Cloud instances. If you want to move the instance to a different container you use `ChangeAnalyticsInstanceCompartment`.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use these operations:

- `GetAnalyticsInstance`
- `UpdateAnalyticsInstance`
- `ChangeAnalyticsInstanceCompartment`

**View or Update a Service using the Command Line**

You can use the `analytics-instance list`, `analytics-instance get`, `analytics-instance update`, and `analytics-instance change-compartment` commands to return and update Oracle Analytics Cloud instances.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use these commands:

- `analytics-instance list`
- `analytics-instance get`
- `analytics-instance update`
- `analytics-instance change-compartment`
Scale a Service

You can scale the number of Oracle Compute Units (OCPUs) or users that your service uses as your needs change.

Note:

Required IAM Policy
Verb: manage
Resource Types: analytics-instance, analytics-instances
Custom Permission: ANALYTICS_INSTANCE_MANAGE
See About Permissions to Manage Oracle Analytics Cloud Instances.

Topics:

• About Scaling
• Scale Up or Down using the Console
• Scale Up or Down using the REST API
• Scale Up or Down using the Command Line

About Scaling

If you subscribe to Oracle Analytics Cloud through Universal Credits and your service performs poorly, you can scale up the number of Oracle Compute Units (OCPUs) allocated to the service to improve performance. To save costs or if your workload is reduced, you might scale down. Similarly, if you set up Oracle Analytics Cloud to support a specific number of users and your user requirements change, you can scale the number of users up or down.

You can scale services up and down within the OCPU range (or user range) available to your service (see table) and within the overall service limit for your tenancy (see Service Limits). Users don't experience any downtime when you scale a service up or down; your service stays up and running.

• Scale the Number of OCPUs
  With Universal Credits, you can either scale between 2 and 8 OCPUs or between 10 and 12 OCPUs. If you want to scale across these ranges (for example, scale up from 8 to 12 OCPUs or scale down from 12 to 6 OCPUs), you must create a service instance with the OCPUs that you want and migrate your content to the new service.
<table>
<thead>
<tr>
<th>Current OCPUs</th>
<th>OCPU Range</th>
<th>Scale Up within Range?</th>
<th>Scale Down within Range?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Incremental + increase)</td>
<td>(Incremental - decrease)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>No (not applicable for trials)</td>
<td>No (not applicable for trials)</td>
</tr>
<tr>
<td>2</td>
<td>2 - 8</td>
<td>Yes (+2, +4, +6)</td>
<td>No (minimum for this range)</td>
</tr>
<tr>
<td>4</td>
<td>2 - 8</td>
<td>Yes (+2, +4)</td>
<td>Yes (-2)</td>
</tr>
<tr>
<td>6</td>
<td>2 - 8</td>
<td>Yes (+2)</td>
<td>Yes (-2, -4)</td>
</tr>
<tr>
<td>8</td>
<td>2 - 8</td>
<td>No (maximum for this range)</td>
<td>Yes (-2, -4, -6)</td>
</tr>
<tr>
<td>10</td>
<td>10 - 12</td>
<td>Yes (+2)</td>
<td>No (minimum for this range)</td>
</tr>
<tr>
<td>12</td>
<td>10 - 12</td>
<td>No (maximum for this range)</td>
<td>Yes (-2)</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>24</td>
<td>24</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>36</td>
<td>36</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>52</td>
<td>52</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Note:

Scale options aren't available for trial services (1 OCPU). At the end of your trial, you must create a new instance with the OCPUs or users that you want (minimum 2 OCPU or 10 users). If you want to keep the content that you created in the trial service, you can save it to a snapshot and copy it to the new service.

• **Scale the Number of Users**

With Universal Credits, you can size your service based on the number of users you expect to use Oracle Analytics Cloud. If your user requirements increase or decrease, you can scale within specific user ranges.

<table>
<thead>
<tr>
<th>Minimum Users</th>
<th>Maximum Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>400</td>
</tr>
<tr>
<td>401</td>
<td>600</td>
</tr>
<tr>
<td>601</td>
<td>900</td>
</tr>
<tr>
<td>901</td>
<td>1400</td>
</tr>
<tr>
<td>1401</td>
<td>2200</td>
</tr>
<tr>
<td>2201</td>
<td>3000</td>
</tr>
</tbody>
</table>

For example, if you currently subscribe with 200 users, you can increase to 400 or decrease to 10. If you want to scale across these ranges (for example, scale up from 300 to 500 or scale down from 500 to 300), you must create a service instance with the number of users that you want and migrate your content to the new service.
Scale Up or Down using the Console

You can use the Console to scale up or scale down the number of OCPUs allocated to your service.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to scale.
5. Note how many OCPUs or users your service currently uses.
   The current Capacity is displayed on the Instance Information tab.
6. Click Change Capacity.
   You can't scale up or down while your service is being backed up, restored, or undergoing similar administrative operations. If you see the message System is not in a READY state. Current state is CONFIGURING, wait a few minutes for the current operation to complete and try again.
7. Select the number of OCPUs or Users you want.
   The values available to you depend on how many OCPUs (or users) your service currently uses. Remember that you can add or remove capacity within the OCPU range (or user range) of your service.
   - Change the number of OCPUs:
     ![Change Capacity OCPUs](image)
   - Change the number of users:
     ![Change Capacity Users](image)

You see a message if scale options aren't available for your environment. For example, you can't scale a trial instance.
8. Click **Save Changes** to confirm. The scale up (or down) operation takes a few minutes to complete. While in progress, the status of the service changes to **Updating**.

Scale Up or Down using the REST API

You can use the `ScaleAnalyticsInstance` operation to scale up or scale down an Oracle Analytics Cloud instance. 

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- `ScaleAnalyticsInstance`

Scale Up or Down using the Command Line

You can use the `analytics-instance scale` command to scale up or scale down an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `analytics-instance scale`

Pause and Resume a Service

When you subscribe to Oracle Analytics Cloud through Universal Credits, you can pause a service if you want to temporarily prevent anyone accessing the service and reduce costs. You can pause and resume an Oracle Analytics Cloud instance using the Console, API, or command line.

**Note:**

Pause disables access, and resume enables access to your instance. Pause and resume *doesn't* restart your instance.

**Note:**

**Required IAM Policy**

**Verb:** use

**Resource Types:** analytics-instance, analytics-instances

**Permission:** ANALYTICS_INSTANCE_USE

See *About Permissions to Manage Oracle Analytics Cloud Instances*.

For information about metering and billing implications when you pause a service, see *Oracle PaaS and IaaS Universal Credits Service Descriptions*. 
Pause and Resume using the Console

You can use the Console to pause a service if you want to temporarily prevent anyone accessing the service.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to pause or resume.
5. To temporarily pause a service, click Stop.
   While in progress, the status of the service changes to Updating.
   After a few minutes, the service status changes to Inactive.
6. To resume the service, click Start.
   While in progress, the status of the service changes to Updating.
   After a few minutes, the service status changes to Active.
   When complete, users can sign in to the service and billing resumes.

Pause and Resume a Service using the REST API

You use the StopAnalyticsInstance and StartAnalyticsInstance operations to pause and resume an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use these operations:

- StopAnalyticsInstance
- StartAnalyticsInstance

Pause and Resume using the Command Line

You can use the analytics-instance stop and analytics-instance start commands to pause and resume an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use these commands:

- analytics-instance stop
- analytics-instance start
Delete a Service

You can delete an Oracle Analytics Cloud instance using the Console, API, or command line.

Note:

Required IAM Policy

Verb: manage

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_DELETE

See About Permissions to Manage Oracle Analytics Cloud Instances.

Topics

• Delete a Service using the Console
• Delete a Service using the REST API
• Delete a Service using the Command Line

Delete a Service using the Console

You can use the Console to delete services you created but don't need anymore.

1. In Oracle Analytics Cloud, take a snapshot of your content and download the snapshot to your local system in case you want to restore the content in the future. See Take a Snapshot and Download a Snapshot.

2. In Oracle Cloud Infrastructure Console, click in the top left corner.

3. Under Solutions and Platform, select Analytics, then Analytics Cloud.

4. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.

5. Click for the instance you want to delete, and then select Delete.

6. Click Delete Instance to confirm.

The Status of the instance changes to Deleting. After a few moments, the status changes to Deleted.

Delete a Service using the REST API

You can use the DeleteAnalyticsInstance operation to delete an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:
Delete Analytics Instance

Delete a Service using the Command Line

You can use the `analytics-instance delete` command to delete an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `analytics-instance delete`

Monitor a Service

You can monitor the current status and progress of operations for an Oracle Analytics Cloud instance using the Console, API, or command line.

### Note:

**Required IAM Policy**
- **Verb**: read
- **Resource Types**: `analytics-instance`, `analytics-instances`
- **Permission**: `ANALYTICS_INSTANCE_READ`

See About Permissions to Manage Oracle Analytics Cloud Instances.

### Topics

- Monitor Status using the Console
- Monitor Status using the REST API
- Monitor Status using the Command Line

### Monitor Status using the Console

You can use Oracle Cloud Infrastructure Console to check the status of your Oracle Analytics Cloud instances and any operations that are in progress.

1. In Console, click ☰ in the top left corner.
2. Under **Solutions and Platform**, select **Analytics**, then **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instances you're looking for.
   - A list of all the instances in the compartment are displayed.
4. Check the **Status** column to determine the current status of your instance.
   - **Creating**: Instance is in the process of being created.
   - **Active**: Instance is running normally.
• **Updating**: Instance is being updated. For example, in the process of scaling up or down.

• **Inactive**: Instance has been temporarily stopped or is stopping.

• **Failed**: Instance isn’t running due to an error.

• **Deleting**: Instance is in the process of being deleted.

• **Deleted**: Instance has been deleted and resources released.

5. Click the name of your service to access the activity details.

Use the **Activity Log** section to track the history and status of activities related to the instance. For example, work requests such as create, start, stop, scale, and so on.

• **ACCEPTED**: The request is in the queue to be processed.

• **IN PROGRESS**: The work request started but isn’t complete.

• **SUCCEEDED**: A work request record exists for this request and an associated WORK_COMPLETED record is in the state SUCCEEDED.

• **FAILED**: A work request record exists for this request and an associated WORK_COMPLETED record is in the state FAILED.

• **CANCELING**: The work request is in the process of canceling.

• **CANCELED**: The work request has been canceled.
Monitor Status using the REST API

You use `GetWorkRequest` to get the current status of operations you perform on Oracle Analytics Cloud instances. If you want to cancel an operation, you use `DeleteWorkRequest`. To check errors and access logs, you use `ListWorkRequestErrors` and `ListWorkRequestLogs`.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use these operations:

- `GetWorkRequest`
- `DeleteWorkRequest`
- `ListWorkRequestErrors`
- `ListWorkRequestLogs`

Monitor Status using the Command Line

You use the `work-request list` and `work-request get` commands to get the current status of operations you perform on Oracle Analytics Cloud instances. If you want to cancel an operation, you use `work-request delete`. To check errors and access logs, you use `work-request-error list` and `work-request-log list`.

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use this command:

- `work-request list`
- `work-request get`
- `work-request delete`
- `work-request-error list`
Find Oracle Analytics Cloud Resources

You can use the simple and advanced search features in Oracle Cloud Infrastructure Console to find Oracle Analytics Cloud instances across compartments in your tenancy.

Simple Search

If you know the name of the resource you're looking for, enter all or part of the name in the search bar. For example, myanalytics.

Results matching your search display. If you don't find what you're looking for, or you want to perform more sophisticated searches, click the Advanced Search button.

Advanced Search

You can enter advanced search queries to search for Oracle Analytics Cloud instances. Click Advanced Search, then either select one of the predefined, sample queries or enter one of your own.
For example:

- To find all the Oracle Analytics Cloud instances in your tenancy:

```plaintext
query
  analyticsinstance resources
```

- To find all the Oracle Analytics Cloud instances that are tagged with the term "test":

```plaintext
query
  analyticsinstance resources
  where
    (freeformTags.key = 'Environment' && freeformTags.value = 'test')
```

- To find all the Oracle Analytics Cloud instances that are currently up and running normally (active):

```plaintext
query
  analyticsinstance resources
  where lifeCycleState = 'ACTIVE'
```

To learn more, see Overview of Search.

### Read Usage Reports

A usage report is a comma-separated value (CSV) file that gives you a detailed breakdown of Oracle Analytics Cloud resources in Oracle Cloud Infrastructure, for audit or invoice reconciliation. You must be assigned to a security policies that allows you to read usage reports.

For example, if you have a federated Oracle Identity Cloud Service user group called `OCI_Analytics_Admins` mapped to an OCI user group called `AnalyticsServiceAdmins`, you might want to allow this group to read usage reports.

The policy statement will look like this:

```plaintext
define tenancy usage-report as
  ocid1.tenancy.oc1..aaaaaaaaned4fkpisbwj1r56u7cj63lf3wffb1vqknstqtvzub7vhhkggq
endorse group AnalyticsServiceAdmins to read objects in tenancy usage-report
```

To learn more, see Usage Reports Overview and Accessing Usage Reports.

### Analyze Usage Costs for Oracle Analytics Cloud

You can analyze the cost of the Oracle Analytics Cloud instances that you're using in the Cost Analysis page.

The way you're billed for a particular instance depends which edition you subscribe to (Professional or Enterprise) and whether you have an Oracle Cloud subscription or a Bring Your Own License (BYOL) subscription:
• Oracle Analytics Cloud - Professional - OCPU Per Hour
• Oracle Analytics Cloud - Professional - Users Per Month
• Oracle Analytics Cloud - Professional - BYOL - OCPU Per Hour
• Oracle Analytics Cloud - Enterprise - OCPU Per Hour
• Oracle Analytics Cloud - Enterprise - Users Per Month
• Oracle Analytics Cloud - Enterprise - BYOL - OCPU Per Hour

To open the Cost Analysis Page, navigate to **Account Management**, and click **Cost Analysis**. Expand the **Analytics** section to view your costs for Oracle Analytics Cloud.

You must be assigned to a security policy that allows you to read cost information. For example, if you have a federated Oracle Identity Cloud Service user group called **OCI_Analytics_Admins** mapped to an OCI user group called **AnalyticsServiceAdmins**, you might want to allow this group to see cost information.

The policy statement will look like this:

```plaintext
allow group AnalyticsServiceAdmins to read usage-reports
```

To learn more, see **Checking Your Balance and Usage**.

### Review Audit Logs for Oracle Analytics Cloud

Oracle Cloud Infrastructure logs API operations on Oracle Analytics Cloud instances for audit purposes.

You can view the audit logs for these Oracle Analytics Cloud operations from the **Audit** page:

• ListAnalyticsInstances
• CreateAnalyticsInstance
• GetAnalyticsInstance
• UpdateAnalyticsInstance
• DeleteAnalyticsInstance
• StartAnalyticsInstance
• StopAnalyticsInstance
• ScaleAnalyticsInstance
• ChangeAnalyticsInstanceCompartment
• ListWorkRequests
• GetWorkRequest
• DeleteWorkRequest
• ListWorkRequestErrors
• ListWorkRequestLogs

To open the Audit page, navigate to Governance, click Audit, and select the compartment you want. You can filter the log to audit a particular Oracle Analytics Cloud operation, such as StopAnalyticsInstance, by entering the name of the operation in the Keyword field. You can also filter by date or API operation (POST, DELETE, PUT, and so on).

You must be assigned to a security policy that allows you to read audit events. For example, if you have a federated Oracle Identity Cloud Service user group called OCI_Analytics_Admins mapped to an OCI user group called AnalyticsServiceAdmins, you might want to allow this group to view audit logs for the whole tenancy or for a particular compartment.

For example, a policy statement that look something like this:

allow group AnalyticsServiceAdmins to read audit-events in tenancy

allow group AnalyticsServiceAdmins to read audit-events in compartment MyEnterpriseAnalytics
To learn more, see Overview of Audit.

Manage "Other Analytics" Services (North America and EMEA Only)

This topic applies only if your subscription to Oracle Analytics Cloud started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2 in North America (14th February 2020) and EMEA (2nd March 2020). After these dates, the way you access any existing Oracle Analytics Cloud environments that you deployed in North America (Ashburn, Phoenix, or Toronto) and EMEA (Frankfurt or London) is different. You access services through a new administration console, where your existing services are listed under a tab called Other Analytics.

Read the FAQs to understand how and when this change impacts you.

• FAQs About Managing Services Deployed in North America and EMEA
• View and Manage "Other Analytics" Services

FAQs About Managing Services Deployed in North America and EMEA

The way you manage Oracle Analytics Cloud deployments on regions in North America and EMEA recently changed. Read these FAQs to find out when and how the change impacts you.

• When and how do I access the new administration console for Oracle Cloud Infrastructure (Gen 2)?
• I want to set up a brand new Oracle Analytics Cloud environment. Should I use the new administration console and create the service on Oracle Cloud Infrastructure Gen 2 or continue using the administration pages I use today?
• I followed the instructions to create a service on Oracle Cloud Infrastructure Gen 2. Why do I see the error "Analytics entitlement is not available in your account"?
• How can I tell whether or not my Oracle Analytics Cloud service is deployed on Oracle Cloud Infrastructure Gen 2?
• I see my existing services listed under Other Analytics. Can I manage them (start/stop/delete) from here too?
• I don’t see all my existing services listed under Other Analytics. Why is this?
• I don’t see any of my existing services listed under Other Analytics. Why is this?
• I can still create services with the administration pages I used before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2. How long can I do this for?
• What happens if I extend my subscription to other regions?
• Where do I manage usage and costs?
When and how do I access the new administration console for Oracle Cloud Infrastructure (Gen 2)?

Before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2 in North America and EMEA, you managed your Oracle Analytics Cloud environments through the Analytics menu under Platform Services.

When Oracle Analytics Cloud is available to you on Oracle Cloud Infrastructure Gen 2, you manage your existing Oracle Analytics Cloud environments and create environments through the Analytics Cloud menu under Solutions and Platform.

You might not see this change immediately. Oracle plans to roll-out Oracle Analytics Cloud on Oracle Cloud Infrastructure Gen 2 to existing customers over several weeks, starting with North America (from 14th February 2020) and then EMEA (from 2nd March 2020). This means it might take a few weeks to upgrade your Oracle Analytics Cloud account.
I want to set up a brand new Oracle Analytics Cloud environment. Should I use the new administration console and create the service on Oracle Cloud Infrastructure Gen 2 or continue using the administration pages I use today?

If you're setting up a new service, Oracle recommends that you use the new administration console. This takes advantage and provides a seamless integration with Oracle Cloud Infrastructure Gen 2. Oracle plans to enhance these infrastructure capabilities further in the next few months and in the future.

For details, see Create Services with Oracle Analytics Cloud.

I followed the instructions to create a service on Oracle Cloud Infrastructure Gen 2. Why do I see the error "Analytics entitlement is not available in your account"?

Oracle plans a phased roll-out of Oracle Analytics Cloud on Oracle Cloud Infrastructure Gen 2 to existing customers who are deploying Oracle Analytics Cloud on regions in North America and EMEA. This means it might take a few weeks to upgrade your Oracle Analytics Cloud entitlement. If you're keen to get started and would like to speed up your upgrade, raise a service request with Oracle Support.
You must provide the name of your Oracle Cloud account, your Oracle Identity Cloud Service tenant name (also called the identity domain ID), and the region where you want to deploy the new Oracle Analytics Cloud service.

**How can I tell whether or not my Oracle Analytics Cloud service is deployed on Oracle Cloud Infrastructure Gen 2?**

The new administration console lists your services under **Analytics** or **Other Analytics**:

- **Analytics** - Lists services deployed on Oracle Cloud Infrastructure Gen 2.
- **Other Analytics** - Lists services deployed prior to Oracle Cloud Infrastructure Gen 2.

You can also tell whether a service is deployed on Oracle Cloud Infrastructure Gen 2 from its URL. If the URL contains an additional *region identifier*, it's deployed on Oracle Cloud Infrastructure Gen 2. For example:

```text
https://myoacs-ervice-idabcd0efghj-ia.analytics.ocp.oraclecloud.com/ui/
```

This URL includes the region identifier -ia, which indicates that the service is deployed in the Ashburn region.

**I see my existing services listed under Other Analytics. Can I manage them (start/stop/delete) from here too?**

No. Click the **Manage Instances** button or **Manage Instances** menu option to navigate to the administration pages that you used to create these services. You manage these service from here, as you did before. See also *Administering Oracle Analytics Cloud*.

**I don't see all my existing services listed under Other Analytics. Why is this?**

The new administration console lists services under **Analytics** and **Other Analytics** by *region*, for example, regions such as **US East** (Ashburn), **US West** (Phoenix), or **Canada Southeast** (Toronto). This means, if you’re logged into US East, you only see services deployed in Ashburn. This is different to the way you currently manage your services, which is by *geo-region*. The North America geo-region includes three regions (Ashburn, Phoenix, and Toronto) which is why your current administration console shows services deployed in all three regions in a single list.

**I don't see any of my existing services listed under Other Analytics. Why is this?**

If other services exist but they're not listed under **Other Analytics**, remember you can always click the **Manage Instances** button to view and manage them from the administration page that you used to create them.

In addition, check that you signed-in correctly and have the required privileges to view instances:

- Check that you're in the correct region. If you subscribe to multiple regions, you might need to switch to a different region to see your services. See *Switching Regions*.
- Check that you have the inspect analytics-instances permission in the current tenancy or the current compartment. See *Give Users Permissions to Manage Analytics Cloud Instances*. 

---

**Chapter 3**

**Manage "Other Analytics" Services (North America and EMEA Only)**
• Check that you’re signed-in as a federated Oracle Identity Cloud Service user, and that you have the application role required to manage services: AUTONOMOUS_ANALYTICS_ServiceAdministrator

1. In Console, click the navigation menu.

2. Under Governance and Administration, go to Identity and click Federation.

3. Click your Oracle Identity Cloud Service federation. For most tenancies, the federation is named OracleIdentityCloudService.

4. Click the name of the user (on the Identity Provider Details page), and click Manage Service Roles.

5. Navigate to AUTOANALYTICS, click the Actions icon (three dots), click Manage service access, and select the AUTONOMOUS_ANALYTICS_ServiceAdministrator role.

• If your federated Oracle Identity Cloud Service has multiple instances, check that you're signed-in to the correct Oracle Identity Cloud Service instance. For example, to view services deployed in Ashburn, Phoenix, or Toronto, you must use the North American identity instance to sign-in. See About Primary and Secondary Service Instances.

If you still can't see any instances, raise a service request with Oracle Support.

I can still create services with the administration pages I used before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2. How long can I do this for?

Oracle doesn't have an end date yet. However, in the future, all Oracle Analytics Cloud deployments will be on Oracle Cloud Infrastructure Gen 2.

What happens if I extend my subscription to other regions?

You see the Other Analytics tab in the new administration console if your subscription started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2 in North America (14th February 2020) and EMEA (2nd March 2020) and you deployed services in North America (Ashburn, Phoenix, or Toronto) or EMEA (Frankfurt or London).

After these dates, you can extend your subscription to other regions as required. Oracle Analytics Cloud is currently available on several regions in Asia-Pacific (APAC) and Latin America (LAD), and some new regions in EMEA will be available soon. When you create a service on a region in APAC or LAD (or a brand new region in North America and EMEA), the service is always deployed on Oracle Cloud Infrastructure Gen 2 and listed under the Analytics tab. You use the new administration console to manage these services.

Where do I manage usage and costs?

When you start to deploy services on Oracle Cloud Infrastructure Gen 2, Oracle recommends that you start to view your service usage costs from the Account Management page in Oracle Cloud Infrastructure Console. From here, you can view usage information for the new services you deploy on Oracle Cloud Infrastructure Gen 2, alongside your existing services. See Checking Your Balance and Usage in Oracle Cloud Infrastructure documentation.

You can still see usage information from the Manage Account tile on the Oracle Cloud Infrastructure Classic Console but you must set the Scope to Cloud Account.
In Manage Account view, any new services that you deploy on Oracle Cloud Infrastructure Gen 2 appear under the home region for your Oracle Cloud account, regardless of where you deployed them, so the Scope by geo-region option might not filter usage as you expect.

**View and Manage "Other Analytics" Services**

This topic applies only if your subscription to Oracle Analytics Cloud started before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2 in North America (14th February 2020) and EMEA (2nd March 2020).

Before Oracle Analytics Cloud was available on Oracle Cloud Infrastructure Gen 2, you managed your services through the Analytics menu under Platform Services in Oracle Cloud Infrastructure Console. When Oracle Analytics Cloud is available on Oracle Cloud Infrastructure Gen 2, you access your services through the Analytics Cloud menu under Solutions and Platform. From the new administration console, you can start to deploy new services on Oracle Cloud Infrastructure Gen 2 and these new services are listed under a tab called Analytics. Your existing services, services that you deployed in North America (Ashburn, Phoenix, or Toronto) and EMEA (Frankfurt or London) before the dates mentioned, are listed under a tab called Other Analytics.

To view and manage existing services available under the Other Analytics tab:

1. Sign in to your Oracle Cloud account.
   
   You must sign-in as a federated Oracle Identity Cloud Service user and have the AUTONOMOUS_ANALYTICS_ServiceAdministrator application role required to access your existing Oracle Analytics Cloud environments. If you're not sure, check this FAQ for more information: I don't see any of my existing services. Why is this?

2. In Console, click in the top left corner.

3. Under Solutions and Platform, select Analytics, then Analytics Cloud.
4. To access your existing services, select a **Compartment** from the list.

You must have the `inspect analytics-instances` permission in this compartment (or the current tenancy) to view your existing services. See Give Users Permissions to Manage Analytics Cloud Instances.

A message indicates that, as an existing customer, you might have some existing services on regions in North America and EMEA.

5. Click **Other Analytics** to view your existing services.

A list of services deployed in the current region is displayed. For example, if you're signed into **US East (Ashburn)**, you only see services that you deployed in **Ashburn**. If you deployed services on other regions in North America, such as Phoenix and Toronto, they're not listed here.

If you don't see any services, check this FAQ for more information: [I don’t see any of my existing services. Why is this?](#)

6. To manage existing services (such as, start, stop, scale, and delete), click **Manage Instances**.

This opens the administration page that you used to create these services. You still manage all your existing services from here.

7. To sign-in to a service, click the service menu (three dots), and click **Open URL**.
Manage Service Access and Security

As administrator, you manage access to your Oracle Analytics Cloud environment for your organization using security features in Oracle Cloud Infrastructure and Oracle Identity Cloud Service.

Topics
- Give Users Permissions to Manage Analytics Cloud Instances
- Give Data Sources Access to Analytics Cloud Instances
- Connect to a Database Deployed on Oracle Cloud Infrastructure with a Public IP Address
- Deploy Oracle Analytics Cloud with a Private Endpoint
- Connect to Private Data Sources Through a Private Access Channel
- Connect to Oracle Autonomous Data Warehouse with a Public IP Address
- Connect to a Database Deployed on Oracle Cloud Infrastructure Classic with a Public IP Address
- Federate with Oracle Identity Cloud Service Manually
- Set Up a Custom Vanity URL
- Query Data Models Remotely Using JDBC

Give Users Permissions to Manage Analytics Cloud Instances

You can give other users permissions to manage Oracle Analytics Cloud instances through security policies.

Topics
- About Permissions to Manage Oracle Analytics Cloud Instances
- Example Policy Statements to Manage Analytics Cloud Instances
- Typical Workflow for Setting Up Policies to Manage Analytics Cloud Instances
- Give a User Permissions to Manage Analytics Cloud Instances

About Permissions to Manage Oracle Analytics Cloud Instances

You use authorization policies to control access to resources in your tenancy. For example, you can create a policy that authorizes users to create and manage Oracle Analytics Cloud instances.

You create policies using the Oracle Cloud Infrastructure Console. For detailed information, see Managing Policies.
## Resource Types for Oracle Analytics Cloud

<table>
<thead>
<tr>
<th>Resource Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analytics-instance</td>
<td>A single Oracle Analytics Cloud instance.</td>
</tr>
<tr>
<td>analytics-instances</td>
<td>One or more Oracle Analytics Cloud instances.</td>
</tr>
<tr>
<td>analytics-instance-work-request</td>
<td>A single work request for Oracle Analytics Cloud. Each operation you perform on an Oracle Analytics Cloud instance, creates a work request. For example, operations such as create, start, stop, and so on.</td>
</tr>
<tr>
<td>analytics-instance-work-requests</td>
<td>One or more work requests.</td>
</tr>
</tbody>
</table>

### Supported Variables

The values of these variables are supplied by Oracle Analytics Cloud. In addition, other general variables are supported. See [General Variables for All Requests](#).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>target.analytics-instance.id</td>
<td>ocid</td>
<td>OCID for the Analytics Cloud instance.</td>
<td>target.analytics-instance.id = 'oci1.analyticsinstance.oc1..abc123'</td>
</tr>
<tr>
<td>target.analytics-instance.name</td>
<td>string</td>
<td>Name of the Analytics Cloud instance.</td>
<td>target.analytics-instance.name = 'myanalytics_1'</td>
</tr>
<tr>
<td>target.analytics-instance.source-compartment.id</td>
<td>ocid</td>
<td>OCID of the source compartment, in a &quot;move compartment&quot; operation.</td>
<td>target.analytics-instance.source-compartment.id = 'ocid1.compartment.oc1..aaa100'</td>
</tr>
<tr>
<td>target.analytics-instance.destination-compartment.id</td>
<td>ocid</td>
<td>OCID of the destination compartment in a &quot;move compartment&quot; operation.</td>
<td>target.analytics-instance.destination-compartment.id = 'ocid1.compartment.oc1..aaa200'</td>
</tr>
</tbody>
</table>

### Details for Verb and Resource-Type Combinations

Oracle Cloud Infrastructure offers a standard set of verbs to define permissions across Oracle Cloud Infrastructure resources ([Inspect, Read, Use, Manage](#)). These tables list the Oracle Analytics Cloud permissions associated with each verb. The level of access is cumulative as you go from **Inspect** to **Read** to **Use** to **Manage**.

#### INSPECT

<table>
<thead>
<tr>
<th>Resource-Type</th>
<th>INSPECT Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>• analytics-instance</td>
<td>• ANALYTICS_INSTANCE_INSPECT</td>
</tr>
<tr>
<td>• analytics-instances</td>
<td>• ANALYTICS_INSTANCE_WR_INSPECT</td>
</tr>
<tr>
<td>• analytics-instance-work-request</td>
<td>•</td>
</tr>
<tr>
<td>• analytics-instance-work-requests</td>
<td>•</td>
</tr>
</tbody>
</table>
## Permissions Required for Each API Operation

This table shows the API operations available for Oracle Analytics Cloud, grouped by resource type.

<table>
<thead>
<tr>
<th>REST API Operation</th>
<th>CLI Command Operation</th>
<th>Permission Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListAnalyticsInstances</td>
<td>analytics-instance list</td>
<td>ANALYTICS_INSTANCE_INSPECT</td>
</tr>
<tr>
<td>CreateAnalyticsInstance</td>
<td>analytics-instance create</td>
<td>ANALYTICS_INSTANCE_CREATE</td>
</tr>
<tr>
<td>GetAnalyticsInstance</td>
<td>analytics-instance get</td>
<td>ANALYTICS_INSTANCE_READ</td>
</tr>
<tr>
<td>UpdateAnalyticsInstance</td>
<td>analytics-instance update</td>
<td>ANALYTICS_INSTANCE_UPDATE</td>
</tr>
<tr>
<td>DeleteAnalyticsInstance</td>
<td>analytics-instance delete</td>
<td>ANALYTICS_INSTANCE_DELETE</td>
</tr>
<tr>
<td>StartAnalyticsInstance</td>
<td>analytics-instance start</td>
<td>ANALYTICS_INSTANCE_USE</td>
</tr>
<tr>
<td>StopAnalyticsInstance</td>
<td>analytics-instance stop</td>
<td>ANALYTICS_INSTANCE_USE</td>
</tr>
</tbody>
</table>
## REST API Operation

<table>
<thead>
<tr>
<th>REST API Operation</th>
<th>CLI Command Operation</th>
<th>Permission Required to Use the Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScaleAnalyticsInstance</td>
<td>analytics-instance scale</td>
<td>ANALYTICS_INSTANCE_MANAGE</td>
</tr>
<tr>
<td>ChangeAnalyticsInstanceComartment</td>
<td>analytics-instance change-compartment</td>
<td>ANALYTICS_INSTANCE_MOVE</td>
</tr>
<tr>
<td>ChangeAnalyticsInstanceNetworkEndpoint</td>
<td>analytics-instance change-network-endpoint</td>
<td>ANALYTICS_INSTANCE_MANAGE</td>
</tr>
<tr>
<td>ListWorkRequests</td>
<td>work-request list</td>
<td>ANALYTICS_INSTANCE_WRITE.inspect</td>
</tr>
<tr>
<td>GetWorkRequest</td>
<td>work-request get</td>
<td>ANALYTICS_INSTANCE_WRITE.READ</td>
</tr>
<tr>
<td>DeleteWorkRequest</td>
<td>work-request delete</td>
<td>ANALYTICS_INSTANCE_WRITE.DELETE</td>
</tr>
<tr>
<td>ListWorkRequestErrors</td>
<td>work-request-error list</td>
<td>ANALYTICS_INSTANCE_WRITE.inspect</td>
</tr>
<tr>
<td>ListWorkRequestLogs</td>
<td>work-request-log list</td>
<td>ANALYTICS_INSTANCE_WRITE.inspect</td>
</tr>
</tbody>
</table>

### Example Policy Statements to Manage Analytics Cloud Instances

Here are typical policy statements that you might use to authorize access to Oracle Analytics Cloud instances.

When you create a policy for your tenancy, you grant users access to all compartments by way of policy inheritance. Alternatively, you can restrict access to individual Oracle Analytics Cloud instances or compartments.

**Let users in the Administrators group fully manage any Analytics instance**

# Full manage permissions (Create, View, Update, Delete, Scale, Start, Stop...)
allow group Administrators to manage analytics-instances in tenancy
allow group Administrators to manage analytics-instance-work-requests in tenancy

**Let users in the analytics_power_users group read, start, and stop all Analytics instances in compartment MyOACProduction**

# Use permissions (List, Get, Start, Stop)
allow group analytics_power_users to use analytics-instances in compartment MyOACProduction

**Let users in the analytics_test_users group create and manage a single Analytics instance (myanalytics_1) in compartment MyOACTest**

# Full manage permissions on a single instance
allow group analytics_test_users to manage analytics-instances in compartment MyOACTest where target.analytics-instances.name = 'myanalytics_1'
Let users in the analytics_power_users group move Analytics instances between two named compartments

# Custom permissions to move instances between two specific compartments.
allow group analytics_power_users to {ANALYTICS_INSTANCE_INSPECT, ANALYTICS_INSTANCE_READ, ANALYTICS_INSTANCE_MOVE} in tenancy
where all {
    target.analytics-instance.source-compartment.id = 'ocid1.compartment.oc1..aaa100',
    target.analytics-instance.destination-compartment.id = 'ocid1.compartment.oc1..aaa200'
}

Let users in the analytics_users group inspect any Analytics instance and their associated work requests

# Inspect permissions (list analytics instances and work requests) using metaverbs.
allow group analytics_users to inspect analytics-instances in tenancy
allow group analytics_users to inspect analytics-instance-work-requests in tenancy

# Inspect permissions (list analytics instances and work requests) using permission names.
allow group analytics_users to {ANALYTICS_INSTANCE_INSPECT} in tenancy
allow group analytics_users to {ANALYTICS_INSTANCE_WR_INSPECT} in tenancy

Let users in the analytics_users2 group read details about any Analytics instance and their associated work requests

# Read permissions (read complete analytics instance and work request metadata) using metaverbs.
allow group analytics_users2 to read analytics-instances in tenancy
allow group analytics_users2 to read analytics-instance-work-requests in tenancy

# Read permissions (read complete analytics instance and work request metadata) using permission names.
allow group analytics_users2 to {ANALYTICS_INSTANCE_INSPECT, ANALYTICS_INSTANCE_READ} in tenancy
allow group analytics_users2 to {ANALYTICS_INSTANCE_WR_INSPECT, ANALYTICS_INSTANCE_WR_READ} in tenancy

Let users in the analytics_power_users2 group read, start, and stop all Analytics instances and read their associated work requests

# Use permissions (read, stop, start on analytics instance, read on work request) using metaverbs.
allow group analytics_power_users2 to use analytics-instances in tenancy
allow group analytics_power_users2 to read analytics-instance-workrequests in tenancy

# Use permissions (read, stop, start on analytics instance, read on work request) using permission names.

allow group analytics_power_users2 to {ANALYTICS_INSTANCE_INSPECT, ANALYTICS_INSTANCE_READ, ANALYTICS_INSTANCE_USE} in tenancy
allow group analytics_power_users2 to {ANALYTICS_INSTANCE_WR_INSPECT, ANALYTICS_INSTANCE_WR_READ} in tenancy

Let users in the Administrators2 group manage any Analytics instance and their associated work requests

# Full manage permissions (use, scale, delete on analytics instance, read and cancel on work request) using metaverbs.
allow group Administrators2 to manage analytics-instances in tenancy
allow group Administrators2 to manage analytics-instance-work-requests in tenancy

# Full manage permissions (use, create, scale, delete on analytics instance, read and cancel on work request) using permission names.

allow group Administrators2 to {ANALYTICS_INSTANCE_INSPECT, ANALYTICS_INSTANCE_READ, ANALYTICS_INSTANCE_USE, ANALYTICS_INSTANCE_CREATE, ANALYTICS_INSTANCE_DELETE, ANALYTICS_INSTANCE_UPDATE, ANALYTICS_INSTANCE_MOVE, ANALYTICS_INSTANCE_MANAGE} in tenancy
allow group Administrators2 to {ANALYTICS_INSTANCE_WR_INSPECT, ANALYTICS_INSTANCE_WR_READ, ANALYTICS_INSTANCE_WR_DELETE} in tenancy
Typical Workflow for Setting Up Policies to Manage Analytics Cloud Instances

If you’re setting up policies for Oracle Analytics Cloud for the first time, take some time to understand what’s required before you start.

High-level steps:

1. Create users in the federated Oracle Identity Cloud Service (IDCS).
2. Create one or more groups and assign users to each group, as required. Give the groups suitable names and include only those users that you want to manage Oracle Analytics Cloud instances in Oracle Cloud Infrastructure (Gen 2). For example, prefix them with \OCI and indicate the level of access for users in the group: OCI_Users, OCI_Power_Users, OCI_Analytics_Admins, and so on.
3. Create groups in Oracle Cloud Infrastructure (OCI). Give the groups suitable names. For example, prefix them with \analytics and mirror the naming convention that you used in Oracle Identity Cloud Service: analytics_users, analytics_power_users, analytics_service_admins, and so on.
4. Map the groups you created in OCI to the groups in IDCS.
5. Create one or more policies, as required. Give users in OCI groups suitable access permissions to compartments and Oracle Analytics Cloud instances.

For more detailed steps, see the next topic.

Give a User Permissions to Manage Analytics Cloud Instances

You can create security policies to give users suitable access to Oracle Analytics Cloud instances in Oracle Cloud Infrastructure Console.

1. Sign-in to your Cloud Account as Cloud Account Administrator.
2. Navigate to the federated Oracle Identity Cloud Service.
   a. Under Governance and Administration, click Identity, then Federation.
   b. Click the link to your Oracle Identity Cloud Service Console.
3. In Oracle Identity Cloud Service, add one or more users.
   a. In the Users section, click Add a User.
   b. Enter details about the user, and click Finish.
4. In Oracle Identity Cloud Service, create one or more groups and assign users to the appropriate group.
   a. Click **Groups** in the Navigator, and then click **Add**.
   b. Enter details about the group, and click **Next**.
      For example, if you're creating a policy that gives users permissions to fully manage Oracle Analytics Cloud instances you might name the group `OCI_Analytics_Admins` (or similar) and include a short description such as "Users with permissions to set up and manage Oracle Analytics Cloud instances on Oracle Cloud Infrastructure" (or similar).
   c. Add one or more users to the group.

5. In Oracle Cloud Infrastructure Console, create an OCI group that corresponds to each of the groups you created in Oracle Identity Cloud Service.
   a. Under **Governance and Administration**, click **Identity**, then **Groups**.
   b. Click **Create Group**.
   c. Enter details about the group.
      For example, if you're creating a policy that gives users permissions to fully manage Oracle Analytics Cloud instances you might name the group `analytics_service_admin` (or similar) and include a short description such as "Users with permissions to set up and manage Oracle Analytics Cloud instances on Oracle Cloud Infrastructure" (or similar).

6. Map OCI groups to the corresponding groups in Oracle Identity Cloud Service.
   a. Under **Governance and Administration**, click **Identity**, then **Federation**.
   b. Navigate to your Oracle Identity Cloud Service federation.
      For most tenancies, the federation is named `OracleIdentityCloudService`.
   c. Click **Add Mapping** and select the name of a group you created in Oracle Identity Cloud Service. For example, `OCI_Analytics_Admins`.
   d. Select the OCI group you want to map to. For example, `analytics_service_admin`.

7. Create a policy that gives users belonging to an OCI group, specific access permissions to Oracle Analytics Cloud instances or compartments.
   a. Under **Governance and Administration**, click **Identity**, then **Policies**.
   b. Select a compartment, and click **Create Policy**.
      For details and examples, see About Permissions to Manage Oracle Analytics Cloud Instances and Example Policy Statements to Manage Analytics Cloud Instances.
      Users belonging to any groups mentioned in the policy statement get their new permission when they next sign in to the Console.

---

**Give Data Sources Access to Analytics Cloud Instances**

You can connect Oracle Analytics Cloud to a wide range of data sources. Some data sources, such as Oracle Autonomous Data Warehouse, require you to include the IP address of your Oracle Analytics Cloud instance in their allowlist.

**Topics:**
• Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance
• Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists
• Public IP Ranges and Gateway IPs for Oracle Analytics Cloud Instances

Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance

You can find the hostname and IP address information for your Oracle Analytics Cloud deployment on the Instance Details tab in Oracle Cloud Infrastructure Console.

You’ll find this information useful for several scenarios.

• **Gateway IP Address**: Some data sources use an allowlist to control access to their data. To include your Oracle Analytics Cloud instance in an allowlist, copy the Gateway IP Address that is displayed on the Additional Details tab and add it to the allowlist so that Oracle Analytics Cloud can connect and access the data.

• **IP Address**: If you set up a vanity URL, you must add a DNS entry that maps the custom domain name you want to use to the IP Address of your Oracle Analytics Cloud instance.

• **Egress IP Addresses**: If you set up a private access channel for Oracle Analytics Cloud, you can also find the egress IP addresses that Oracle Analytics Cloud uses to access private data sources. You copy the Egress IP Address information and add it to the allowlist for the private data source so that Oracle Analytics Cloud can connect and access the data.

1. In Oracle Cloud Infrastructure Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you’re looking for.
4. Click the name of the instance.
5. Click Additional Details.

The Hostname, IP Address and Gateway IP Address of your instance is displayed in the Network section.

6. To find the egress IP addresses that Oracle Analytics Cloud uses to access private data sources over a private access channel.
   a. On the Instance Details page, navigate to the Resources section, click Private Access Channel, and then click the name of the private access channel.
b. In the Private Access Details section, note down the **Egress IP Addresses**.

![Image of Private Access Channel Details](image.png)

Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists

Before you try to connect Oracle Analytics Cloud to an Oracle Cloud database, ask the database administrator to add the **Gateway IP Address** (or address range) for your Oracle Analytics Cloud instance to the target database's allowlist. The database administrator must add a security rule on the target Oracle Cloud database that allows TCP/IP traffic from Oracle Analytics Cloud on a specific database port.

This topic describes how to add Oracle Analytics Cloud to the allowlist for an Oracle Cloud database. If you want to connect to other data sources, follow similar steps, as required.

1. Make a note of the Gateway IP Address of your Oracle Analytics Cloud instance or the Egress IP address of the private access channel that you or your database administrator must allow access to.

   See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.

2. Include the Gateway IP Address that you made a note of in Step 1 in the security list for your Oracle Cloud database.

   The way you register the IP address of your Oracle Analytics Cloud instance depends on whether the database you're trying to connect to is deployed on Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic:

   - **Database on Oracle Cloud Infrastructure**
     - a. Add an ingress rule.
b. Specify the IP address in the **SOURCE CIDR** field.

- **Database on Oracle Cloud Infrastructure Classic**

  a. Add an access rule.
b. Specify the IP address in the field below the **Source** field

![Create Access Rule](image)

**Public IP Ranges and Gateway IPs for Oracle Analytics Cloud Instances**

If you want to connect Oracle Analytics Cloud with a *public endpoint* to a database in Oracle Cloud, you must add the public gateway IP Address (or IP address range) where your Oracle Analytics Cloud instance is located on Oracle Cloud Infrastructure to the database’s allowlist.

The public IP address information that you provide depends on the type of database you want to connect to and whether or not your Oracle Analytics Cloud instance is deployed in the same region as the database.

<table>
<thead>
<tr>
<th>Database</th>
<th>Oracle Autonomous Data Warehouse</th>
<th>Oracle Autonomous Transaction Processing</th>
<th>Any Other Oracle Cloud Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same region as Oracle Analytics Cloud</td>
<td>Allow 240.0.0.0/4</td>
<td>Allow 240.0.0.0/4</td>
<td>Allow the region-specific IP address.</td>
</tr>
<tr>
<td>Different region to Oracle Analytics Cloud</td>
<td>Allow the region-specific IP address.</td>
<td>Allow the region-specific IP address.</td>
<td>Allow the region-specific IP address.</td>
</tr>
</tbody>
</table>

**Region-Specific Public IP Address Information for Oracle Analytics Cloud**

Use Oracle Cloud Infrastructure Console to find the public gateway IP address (or IP address range) of your Oracle Analytics Cloud instance that you or your database administrator must add to the database’s allowlist. See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).

Alternatively, if you know the region where you deployed your Oracle Analytics Cloud instance, find that region in the table below and make a note of the public IP address information listed in the **IP Address Range** column or the **Gateway IP Address** column.

The security policy enforced by your company or organization determines whether you must provide the IP address ranges or Gateway IP address. If you’re not sure, check with your network administrator.

For example, if you deployed your Oracle Analytics Cloud instance in Tokyo, Japan East (ap-tokyo-1) and your company’s security policy requires you to provide an IP address range, you add 192.29.39.56/29. Alternatively, if you’re required to provide a Gateway IP address, you add 192.29.39.59.
<table>
<thead>
<tr>
<th>Region Where Oracle Analytics Cloud Deployed</th>
<th>Region Identifier</th>
<th>IP Address Range</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asia Pacific (APAC)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia Southeast (Melbourne)</td>
<td>ap-melbourne-1</td>
<td>192.29.211.152/29</td>
<td>192.29.211.154</td>
</tr>
<tr>
<td>Australia East (Sydney)</td>
<td>ap-sydney-1</td>
<td>192.29.144.152/29</td>
<td>192.29.144.154</td>
</tr>
<tr>
<td>India South (Hyderabad)</td>
<td>ap-hyderabad-1</td>
<td>129.148.128.56/29</td>
<td>129.148.128.61</td>
</tr>
<tr>
<td>India West (Mumbai)</td>
<td>ap-mumbai-1</td>
<td>192.29.48.240/29</td>
<td>192.29.48.246</td>
</tr>
<tr>
<td>Japan Central (Osaka)</td>
<td>ap-osaka-1</td>
<td>192.29.242.208/29</td>
<td>192.29.242.211</td>
</tr>
<tr>
<td>Japan East (Tokyo)</td>
<td>ap-tokyo-1</td>
<td>192.29.39.56/29</td>
<td>192.29.39.59</td>
</tr>
<tr>
<td>South Korea Central (Seoul)</td>
<td>ap-seoul-1</td>
<td>192.29.20.96/29</td>
<td>192.29.20.98</td>
</tr>
<tr>
<td>South Korea North (Chuncheon)</td>
<td>ap-chuncheon-1</td>
<td>129.148.144.24/29</td>
<td>129.148.144.31</td>
</tr>
<tr>
<td><strong>Europe, the Middle East and Africa (EMEA)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany Central (Frankfurt)</td>
<td>eu-frankfurt-1</td>
<td>147.154.148.0/29</td>
<td>147.154.148.171</td>
</tr>
<tr>
<td></td>
<td></td>
<td>138.1.64.32/29</td>
<td>138.1.64.33</td>
</tr>
<tr>
<td>Netherlands Northwest (Amsterdam)</td>
<td>eu-amsterdam-1</td>
<td>192.29.193.72/29</td>
<td>192.29.193.76</td>
</tr>
<tr>
<td>Switzerland North (Zurich)</td>
<td>eu-zurich-1</td>
<td>192.29.60.112/29</td>
<td>192.29.60.112</td>
</tr>
<tr>
<td>Saudi Arabia West (Jeddah)</td>
<td>me-jeddah-1</td>
<td>192.29.225.72/29</td>
<td>192.29.225.78</td>
</tr>
<tr>
<td>UAE East (Dubai)</td>
<td>me-dubai-1</td>
<td>129.148.214.184/29</td>
<td>129.148.214.189</td>
</tr>
<tr>
<td>UK South (London)</td>
<td>uk-london-1</td>
<td>147.154.229.168/29</td>
<td>147.154.229.170</td>
</tr>
<tr>
<td>UK West (Newport)</td>
<td>uk-cardiff-1</td>
<td>129.149.20.112/29</td>
<td>129.149.20.118</td>
</tr>
<tr>
<td><strong>Latin America</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil East (Sao Paulo)</td>
<td>sa-saopaulo-1</td>
<td>192.29.128.232/29</td>
<td>192.29.128.238</td>
</tr>
<tr>
<td><strong>North America</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada Southeast (Montreal)</td>
<td>ca-montreal-1</td>
<td>192.29.82.176/29</td>
<td>192.29.82.176</td>
</tr>
<tr>
<td>Canada Southeast (Toronto)</td>
<td>ca-toronto-1</td>
<td>192.29.13.0/29</td>
<td>192.29.13.6</td>
</tr>
<tr>
<td>US East (Ashburn)</td>
<td>us-ashburn-1</td>
<td>147.154.20.0/29</td>
<td>147.154.20.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>147.154.3.184/29</td>
<td>147.154.3.185</td>
</tr>
<tr>
<td></td>
<td></td>
<td>147.154.0.0/29</td>
<td>147.154.0.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>147.154.3.8/29</td>
<td>147.154.3.13</td>
</tr>
<tr>
<td>US West (Phoenix)</td>
<td>us-phoenix-1</td>
<td>147.154.104.160/29</td>
<td>147.154.104.165</td>
</tr>
<tr>
<td></td>
<td></td>
<td>138.1.32.24/29</td>
<td>138.1.32.29</td>
</tr>
<tr>
<td>US West (San Jose)</td>
<td>us-sanjose-1</td>
<td>129.148.161.112/29</td>
<td>129.148.161.117</td>
</tr>
</tbody>
</table>
Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint

If you deploy Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict access through one or more rules.

Topics:
- About Public Endpoints and Access Control Rules
- Prerequisites for a Public Endpoint
- Typical Workflow to Restrict Public Access using Rules
- Create Oracle Analytics Cloud with a Public Endpoint
- Manage Access Rules for a Public Endpoint using the Console

About Public Endpoints and Access Control Rules

When you set up an Oracle Analytics Cloud instance you have the option to deploy Oracle Analytics Cloud with a public internet accessible endpoint. For security reasons, you might want to restrict access through one or more access control rules.

You can add and edit access control rules whenever you want and manage access in several ways. You can manage access with:
- A specific set of IP addresses
- A CIDR block range (Classless Inter-Domain Routing)
- An Oracle Cloud Infrastructure VCN (Virtual Cloud Network)
- Any combination of the above, that is, IP addresses, CIDR ranges, VCNs

For example:
- **Scenario 1** - Allow access to Oracle Analytics Cloud over the public internet. Restrict access to a fixed set of IP addresses.
- **Scenario 2** - Allow access to Oracle Analytics Cloud over the public internet. Restrict access to hosts within a fixed CIDR block range.
- **Scenario 3** - Allow access to Oracle Analytics Cloud from an Oracle Cloud Infrastructure VCN that's deployed in the same region as Oracle Analytics Cloud, without going over the public internet. At the same time, allow other third-party cloud services or users to access Oracle Analytics Cloud over the public internet.
- **Scenario 4** - Allow access to Oracle Analytics Cloud from your on-premise network without going through the public internet. At the same time, allow other third-party cloud services or users to access Oracle Analytics Cloud over the public internet.
The sample diagram shows Oracle Analytics Cloud deployed with a public endpoint and two access control rules. The first rule allows access from the IP address 204.204.100.100 and the second rule allows access from the Oracle Cloud Infrastructure VCN customer-oci-vcn. The VCN is peered to an on-premise network, and access to Oracle Analytics Cloud is routed through the VCN’s service gateway.

While Oracle Analytics Cloud is accessible from the public internet, you can implement your own access control rules to provide any additional security that you need. In this example, only the third-party service with the egress gateway IP address 204.204.100.100 accessed Oracle Analytics Cloud over the public internet. Traffic from the on-premise network never uses the public internet, instead it uses the service gateway configured inside the VCN.

Prerequisites for a Public Endpoint

Before you create an Oracle Analytics Cloud instance that’s accessible from the public internet, consider whether or not your organization wants to restrict access.

No Restrictions

No prerequisites. If you want Oracle Analytics Cloud to be accessible from anywhere, you can create the Oracle Analytics Cloud instance with no access control.

Restrict Access to a Specific IP Address or CIDR Block Range

If you plan to limit access to traffic from a specific IP address or CIDR block range, record all the IP addresses or CIDR ranges that you want to allow. When you create your Oracle Analytics Cloud instance, you use this information to define one or more access control rules for Oracle Analytics Cloud.

Restrict Access to a Specific VCN

If you plan to limit access to traffic from a specific Oracle Cloud Infrastructure VCN, ensure that the VCN exists and you have the required policies to access the VCN.

1. Set up an Oracle Cloud Infrastructure VCN in the same region as the Oracle Analytics Cloud instance you plan to create.

   See Set up the VCN and subnets.
2. Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway.

   See Setting Up a Service Gateway in the Console.

3. Ensure that you (or whoever plans to create the Oracle Analytics Cloud instance) have the required policies to access the VCN.

   • **READ policy for the compartment:**

     ```
     ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
     ```

   • **READ policy for the VCN:**

     ```
     ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY
     ```

### Typical Workflow to Restrict Public Access using Rules

If you want to deploy an Oracle Analytics Cloud instance with a public endpoint for the first time with one or more access control rules, follow these tasks as a guide.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand prerequisites for a public endpoint</td>
<td>Consider whether or not your organization plans to restrict access. If required, record the IP addresses, CIDR ranges, and VCNs that you plan to allow access to.</td>
<td>Prerequisites for a Public Endpoint</td>
</tr>
<tr>
<td>Create Oracle Analytics Cloud with a public endpoint</td>
<td>Use Oracle Cloud Infrastructure Console to deploy a new service.</td>
<td>Create Oracle Analytics Cloud with a Public Endpoint</td>
</tr>
<tr>
<td>Allow access by IP address, CIDR range, or VCN</td>
<td>Add one or more access control rules. You can allow access to Oracle Analytics Cloud by public IP address, public CIDR block range, or VCN.</td>
<td>Manage Access Control Rules</td>
</tr>
<tr>
<td>(Optional) Set up private access from your on-premise network</td>
<td>Set up an Oracle Cloud Infrastructure VCN that connects to your on-premise network using FastConnect private peering or VPN Connect. The VCN must be deployed in the same region as Oracle Analytics Cloud. Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway. Add an access control rule in your Oracle Analytics Cloud instance that allows access from your VCN. Configure VCN peering to your on-premise network through FastConnect or VPN Connect to enable access from your on-premise network. Configure transit routing with the VCN to give your on-premise network private access to Oracle Analytics Cloud.</td>
<td>Working with VCNs and Subnets Setting Up a Service Gateway in the Console Manage Access Control Rules Access to Your On-Premises Network Setting Up Private Access to Oracle Services</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>More Information</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>(Optional) Set up private access from hosts on your VCN</td>
<td>Set up an Oracle Cloud Infrastructure VCN in the same region as Oracle Analytics Cloud. Set up a service gateway in your VCN, and a route table to send traffic to Oracle Analytics Cloud through the service gateway. Add an access control rule in your Oracle Analytics Cloud instance that allows access from your VCN.</td>
<td>Working with VCNs and Subnets Setting Up a Service Gateway in the Console Manage Access Control Rules</td>
</tr>
</tbody>
</table>

**Create Oracle Analytics Cloud with a Public Endpoint**

You can use Oracle Cloud Infrastructure Console, API, or command line to deploy Oracle Analytics Cloud with a public endpoint.

If you're new to Oracle Analytics Cloud, see Create a Service for all the steps.

This topic highlights only the information you must configure to enable access over the public internet and define any access control rules that you require.
1. For **Network Access**, select **Public**.

2. To configure access control rules, select **Configure Access Control Rules**, and then add one or more rules using the specific public IP addresses, public CIDR block ranges, and VCNs that you want to allow access to.

   You can add, edit, and delete access control rules at any time. So if you prefer, you can add your rules later on.
Manage Access Control Rules

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict access to your service through an access control list (ACL) that contains one or more rules. You can add and edit access control rules whenever you want and allow access by public IP address, public CIDR block range, or VCN using the Console, API, or command line.

### Note:

**Required IAM Policy to Edit Analytics Instance**

**Verb:** manage

**Resource Types:** analytics-instance, analytics-instances

**Permission:** ANALYTICS_INSTANCE_MANAGE

See [About Permissions to Manage Oracle Analytics Cloud Instances](#).

**Additional IAM Policy Required to Edit a Public Endpoint**

**Verb:** read

**Resource Type:** virtual-network-family, compartment, compartments

See [Prerequisites for a Public Endpoint](#).

### Topics

- Manage Access Rules for a Public Endpoint using the Console
- Manage Access Rules for a Public Endpoint using the REST API
- Manage Access Rules for a Public Endpoint using the Command Line

### Manage Access Rules for a Public Endpoint using the Console

If you deployed Oracle Analytics Cloud with a public internet accessible endpoint, you can restrict access to your service through an access control list (ACL) that contains one or more rules. You can add and edit access control rules whenever you want and allow access by public IP address, public CIDR block range, or VCN.

1. In Console, click ☰ in the top left corner.
2. Under **Solutions and Platform**, select **Analytics**, then **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to control access to.
5. On the Instance Information page, click the **Edit** icon next to the **Access Control Rules** option.
6. Add or edit access control rules as required.

You can specify the following types of rule:

- **IP Address**: Select IP Address to a specific public IP address.
- **CIDR Block**: Select CIDR Block to specify a range of public IP addresses using CIDR notation.
- **Virtual Cloud Network**: Select Virtual Cloud Network to specify an existing Oracle Cloud Infrastructure VCN. The drop-down list shows all the VCNs in the current compartment that you have access to. If you can't see the VCN or subnet you want, check you have the required permissions. See About Public Endpoints and Access Control Rules.

Click Change Compartment to select a VCN from a different compartment.

Manage Access Rules for a Public Endpoint using the REST API

You can use the `ChangeAnalyticsInstanceNetworkEndpoint` operation to change access control rules for an Oracle Analytics Cloud instance with a public endpoint.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:

- `ChangeAnalyticsInstanceNetworkEndpoint`
Manage Access Rules for a Public Endpoint using the Command Line

You can use the `change-network-endpoint` command to change access control rules for an Oracle Analytics Cloud instance with a public endpoint.

For example:

```bash
oci
   analytics analytics-instance change-network-endpoint \
   --analytics-instance-id ocid1.analyticsinstance.oc1.us- 
   ashburn-1.aaaaaaaa5ynfzx2e6wpshkhkoajoiqizwmhc6x7ogp4aw66whyq76fdk32q \
   --network-endpoint-details '{
   "networkEndpointType": "PUBLIC",
   "whitelistedIps": ["168.122.67.231", "168.122.59.5", "10.20.30.35/26",
   "240.0.0.0/4"],
   "whitelistedVcns": [{"id": "ocid1.vcn.oc1.us-
   ashburn-1.amaaaaaarfop2rqah112uacphjiousx3v346f67rsrsmgcekfg6uni3axzna"}
   ]}
}
```

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use this command:

• `change-network-endpoint`

Deploy Oracle Analytics Cloud with a Private Endpoint

If you want only hosts within your virtual cloud network (VCN) or your on-premise network to have access to Oracle Analytics Cloud, you can deploy your Oracle Analytics Cloud instance with a private endpoint.

Topics:

• About Private Endpoints
• Prerequisites for a Private Endpoint
• Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint
• Create Oracle Analytics Cloud with a Private Endpoint
• Change a Private Endpoint using the Console
• Connect to Your On-premise Network using FastConnect or VPN Connect

About Private Endpoints

When you set up an Oracle Analytics Cloud instance you have the option to restrict access through a private endpoint. Private access means that traffic doesn’t go over the internet. Private access can be from hosts within your virtual cloud network (VCN) or your on-premise network.

For example:

• **Scenario 1** - Allow access to Oracle Analytics Cloud from an on-premise (corporate) network. Don’t allow access to anyone outside the corporate network.
**Scenario 2** - Allow access to Oracle Analytics Cloud from an Oracle Cloud Infrastructure VCN that’s deployed in the same region as Oracle Analytics Cloud. Don’t allow access to anyone outside the virtual cloud network.

When you deploy an Oracle Analytics Cloud instance with a private endpoint, the Oracle Analytics Cloud URL is only accessible from a browser if the client machine supports host name resolution. This means you must configure Domain Name Server (DNS) resolution on your private network to access the private endpoint. For example, you might use a DNS resolution strategy similar to that described in the article *Hybrid DNS Configuration using DNS VM in VCN*.

The diagram shows Oracle Analytics Cloud deployed with a private endpoint. The private Oracle Analytics Cloud is only accessible through an Oracle Cloud Infrastructure VCN in your tenancy; you can't access Oracle Analytics Cloud from the public internet.

You must peer the VCN to your on-premise network. To enable access to Oracle Analytics Cloud, the on-premise network DNS must provide host name resolution for Oracle Analytics Cloud.

**Prerequisites for a Private Endpoint**

Before you create an Oracle Analytics Cloud instance with a private endpoint, complete the required prerequisites.

The prerequisites are the same for both scenarios:

- Private access from an on-premise network through an Oracle Cloud Infrastructure VCN
- Private access from hosts in an Oracle Cloud Infrastructure VCN

1. Set up the Oracle Cloud Infrastructure VCN with a subnet for Oracle Analytics Cloud.

The VCN must be in the region where you plan to deploy Oracle Analytics Cloud. See *Working with VCNs and Subnets*. 
Note:
If you plan to access Oracle Analytics Cloud from an on-premise network, keep some address space available in the VCN for additional subnets in case you need them for host name resolution.

2. Ensure that you (or whoever plans to create the Oracle Analytics Cloud instance) have the required policies to access the VCN.

Several options are available. Choose the most appropriate level for you:

**Broad Resource Access Policy**

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN TENANCY

**Limited Resource Access Policy**

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN compartment <compartment name of VCN>

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN compartment <compartment name of subnet>

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN compartment <compartment name of AnalyticsInstance>

**Moderate Resource Access Policy - Option 1**

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN TENANCY

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN TENANCY

**Moderate Resource Access Policy - Option 2**

- ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY
• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE virtual-network-family IN compartment <compartment name of VCN>

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN compartment <compartment name of AnalyticsInstance>

Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint

If you want to deploy an Oracle Analytics Cloud instance with a private endpoint 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>Understand prerequisites for a private endpoint</td>
<td>Set up an Oracle Cloud Infrastructure virtual cloud network (VCN) with a subnet for Oracle Analytics Cloud. The VCN must be in the region where you plan to deploy Oracle Analytics Cloud.</td>
<td>Prerequisites for a Private Endpoint</td>
</tr>
<tr>
<td>Create Oracle Analytics Cloud with a private endpoint</td>
<td>Use Oracle Cloud Infrastructure Console to deploy a new service.</td>
<td>Create Oracle Analytics Cloud with a Private Endpoint</td>
</tr>
<tr>
<td>Configure the connection to your on-premise network using FastConnect or VPN Connect.</td>
<td>Use FastConnect or VPN to peer your on-premise network with the Oracle Cloud Infrastructure VCN through which you plan to access Oracle Analytics Cloud.</td>
<td>Connect to Your On-premise Network using FastConnect or VPN Connect</td>
</tr>
<tr>
<td>Change the VCN or subnet used to access Oracle Analytics Cloud</td>
<td>If you want to access Oracle Analytics Cloud through a different VCN or subnet, you can edit the configuration at any time.</td>
<td>Change a Private Endpoint using the Console</td>
</tr>
</tbody>
</table>

Create Oracle Analytics Cloud with a Private Endpoint

You can use Oracle Cloud Infrastructure Console, API, or command line to deploy Oracle Analytics Cloud with a private endpoint.

If you're new to Oracle Analytics Cloud, see Create a Service for all the steps.

This topic highlights only the information you must configure to enable private access through a private endpoint.
1. For **Network Access**, select **Private**.

2. Select the **Virtual Cloud Network** and the **Subnet** that you want to use to access Oracle Analytics Cloud.

**Connect to Your On-premise Network using FastConnect or VPN**

If you want to access an Oracle Analytics Cloud instance that is deployed with a private endpoint in an Oracle Cloud Infrastructure VCN from your on-premise network, you must peer your on-premise network with the Oracle Cloud Infrastructure VCN. You
can use FastConnect or VPN to peer your on-premise network with a VCN on Oracle Cloud Infrastructure.

Typically, these tasks are performed by the network administrator responsible for the on-premise network and the Oracle Cloud Infrastructure network. You can complete these steps before or after you create your Oracle Analytics Cloud instance.

1. In Oracle Cloud Infrastructure Console, navigate to the Additional Details tab to determine the Hostname of your Oracle Analytics Cloud instance.

   ![Hostname Example](image)

   See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.

2. Peer your on-premise network with the Oracle Cloud Infrastructure VCN through FastConnect or VPN Connect.

   See Access to Your On-Premises Network.

3. In your on-premise network, configure a suitable host name resolution solution for Oracle Analytics Cloud.

   Several options are available to you:
   
   • (Testing purposes only) From a client machine in your on-premise network, add a host name entry in the /etc/hosts file for Oracle Analytics Cloud. Use the hostname that you copied in Step 1. For example:

     `<myinstanceid>.analytics.ocp.oraclecloud.com`

   • Add a DNS record in your on-premise intranet DNS server (Domain Name System) for Oracle Analytics Cloud, that is, specify the host name for Oracle Analytics Cloud and its private IP address.

   • Set up a hybrid DNS solution. For example, see Hybrid DNS configuration using DNS VM in OCI VCN.
     
     a. Configure your on-premise intranet DNS server with conditional DNS forwarding to the DNS server configured in the VCN, and specify the host name for Oracle Analytics Cloud.

     b. Configure your on-premise intranet DNS server with DNS forwarding to the DNS server configured in the VCN, and specify the entire Oracle Analytics Cloud domain, that is, `analytics.ocp.oraclecloud.com`.

4. Test that you can access Oracle Analytics Cloud from your on-premise network.
Change the VCN or Subnet Used to Access a Private Endpoint

If you want to access Oracle Analytics Cloud through a different VCN or subnet, you can edit the configuration using the Console, API, or command line.

Note:

Required IAM Policy to Edit Analytics Instance

Verb: manage

Resource Types: analytics-instance, analytics-instances

Permission: ANALYTICS_INSTANCE_MANAGE

See About Permissions to Manage Oracle Analytics Cloud Instances.

IAM Policy Required to Change a Private Endpoint

Verb: manage

Resource Type: virtual-network-family

Verb: read

Resource Type: compartment, compartments

To learn about other, more detailed access policy options, see Prerequisites for a Private Endpoint.

Topics

• Change a Private Endpoint using the Console
• Change a Private Endpoint using the REST API
• Change a Private Endpoint using the Command Line

Change a Private Endpoint using the Console

If you want to access Oracle Analytics Cloud through a different VCN or subnet, you can edit the configuration.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to change access to.
5. On the Instance Information page, click the Edit icon next to Subnet.
6. Select a different Virtual Cloud Network, Subnet, or both.
Click **Change Compartment** to select resources from a different compartment. If you can't see the VCN or subnet you want, check you have the required permissions. See [Prerequisites for a Private Endpoint](#).

![Private Endpoint Image](image)

### Change a Private Endpoint using the REST API

You can use the `ChangeAnalyticsInstanceNetworkEndpoint` operation to command to change the VCN or subnet used to access an Oracle Analytics Cloud instance with a private endpoint.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- `ChangeAnalyticsInstanceNetworkEndpoint`

### Change a Private Endpoint using the Command Line

You can use the `change-network-endpoint` command to change the VCN or subnet used to access an Oracle Analytics Cloud instance with a private endpoint.

For example:

```bash
oci \
  analytics analytics-instance change-network-endpoint \
  --analytics-instance-id ocid1.analyticsinstance.oc1.us-ashburn-1.aaaaaaaa5pynfxr2e6wpshkhkoajoigizwmhc6x7ogp4aw66whyq76fdk32q \
  --network-endpoint-details '{"networkEndpointType": "PRIVATE", "vcnId": "ocid1.vcn.oc1.us-ashburn-1.amaaaaaarfo2rqav4x2wox6dt72o57jmnevpugq63gcsdtrbk42bvz446sa", "subnetId": "ocid1.subnet.oc1.us-ashburn-1.aaaaaaaa15xb6vodov35nbqhswoypeieowgy44vambmnokzpwhv22pvjxoq" }'
```

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `change-network-endpoint`
Connect to Private Data Sources Through a Private Access Channel

If the data you want to analyze is stored on a private host, you can set up a private access channel between your Oracle Analytics Cloud instance and your data source.

**Topics:**
- About Private Access Channels
- About Private Data Sources
- Prerequisites for a Private Access Channel
- Typical Workflow to Set Up a Private Access Channel
- Configure a Private Access Channel
- Edit a Private Access Channel
- Delete a Private Access Channel

**About Private Access Channels**

If you want Oracle Analytics Cloud to access data on a private host, you can set up a private access channel. A private access channel can give Oracle Analytics Cloud access to private data sources within your virtual cloud network (VCN) on Oracle Cloud Infrastructure or other networks peered to the VCN such as your corporate network.

You can set up a private access channel for Oracle Analytics Cloud instances deployed with the [Enterprise Analytics](#) feature set. Private access channels aren't available to Oracle Analytics Cloud instances that offer only [Self-Service Analytics](#).

It doesn't matter whether your Oracle Analytics Cloud instance has a public endpoint or a private endpoint. Oracle Analytics Cloud can access private data sources through a private access channel for both network scenarios.

**Note:**

Private access channels enable you to connect to private data source hosts. You can't use a private access channel to access any other types of private host, such as a private FTP or SMTP host.

**Private Access Channel for Oracle Analytics Cloud Instances with Public Endpoint**

If Oracle Analytics Cloud has a public endpoint you must specify the VCN and subnet you want the private access channel to use.
Private Access Channel for Oracle Analytics Cloud Instances with Private Endpoint

If Oracle Analytics Cloud has a private endpoint, the private access channel uses the same VCN and subnet as the private endpoint.

About Private Data Sources

Oracle Analytics Cloud can access private data sources with a Fully Qualified Domain Name (FQDN) that resolves through the Domain Name System (DNS) in your tenancy. For example, domain names such as custcorp.com, example.com, and so on.

You configure private access in two stages:
• In Oracle Cloud Infrastructure Console, you set up a private access channel and register the domain names of the data sources that require private access.

When you set up (or edit) a private access channel you alter the configuration of your Oracle Analytics Cloud instance. Some users might experience a temporary disruption in service during the configuration process so Oracle recommends that you plan private access channel configuration activities on critical instances accordingly.

• In Oracle Analytics Cloud, you connect to the data source and analyze the data in the usual way.

For more guidance, see Typical Workflow to Set Up a Private Access Channel.

Supported Data Sources

You can use a private access channel to connect to a range of certified data sources. To check whether or not you can use a private access change to connect to your data source, see Supported Data Sources.

Note:

Private access channels enable you to connect to private data source hosts. You can't use a private access channel to access any other types of private host, such as a private FTP or SMTP host.

Limitations

Oracle Analytics Cloud can't access private data sources on an Oracle Database that use IP forwarding. If you want to connect Oracle Analytics Cloud to an Oracle Database that uses a Single Client Access Name (SCAN) that is configured with IP forwarding (instead of FQDN hostname forwarding), use one of the following methods to set up the connection in Oracle Analytics Cloud:

• Configure the data source connection using the Advanced Connection String option and connect directly to the Oracle Database nodes, instead of SCAN. For example:

  (DESCRIPTION=
  (ADDRESS_LIST= (LOAD_BALANCE=on) (FAILOVER=ON)
  (ADDRESS=(PROTOCOL=tcp) (HOST=<DB Host 1>) (PORT=1521))
  (ADDRESS=(PROTOCOL=tcp) (HOST=<DB Host 2>) (PORT=1521))))
  (CONNECT_DATA=(SERVICE_NAME=<DB Service Name>)))

• Configure an Oracle Connection Manager in front of SCAN and then configure a data source connection in Oracle Analytics Cloud that connects to the Oracle Connection Manager endpoint.

Prerequisites for a Private Access Channel

Before you configure a private access channel, you need to know the domain names of the DNS zones you want Oracle Analytics Cloud to access, check that your Oracle
Analytics Cloud deployment includes the Enterprise Analytics feature set, and verify you have the correct permissions.

If your Oracle Analytics Cloud is deployed with a public endpoint, you also need to know the VCN and subnet on Oracle Cloud Infrastructure that you want Oracle Analytics Cloud to use to access the private sources. If you deployed Oracle Analytics Cloud instance with a private endpoint, the private access channel automatically uses the same VCN and subnet you configured for the instance so you don’t need to do step 3.

1. Verify that your Oracle Analytics Cloud deployment includes the Enterprise Analytics feature set (Oracle Analytics Cloud - Enterprise Edition).

   Feature set information is available on the Instance Details page. See Verify Your Service.

   Private access channels aren't available on Oracle Analytics Cloud deployments that include the Self-Service Analytics feature set (Oracle Analytics Cloud - Professional Edition).

2. Record the domain name of each private data source (DNS zone) you want Oracle Analytics Cloud to access through the private channel.

   For example, domain names such as example.com, companyabc.com, and so on.

   • Private data source in a corporate network peered to an Oracle Cloud Infrastructure VCN

      Register a DNS zone in the format: <domain name>

      For example:

      – If the data source FQDN hostname is data-source-ds01.companyabc.com, add the DNS Zone as companyabc.com.

      – If the data source FQDN hostname is db01.dbdomain.companyabc.com, add the DNS Zone as dbdomain.companyabc.com to only give Oracle Analytics Cloud access to hosts under dbdomain.companyabc.com.

   • Private data source in an Oracle Cloud Infrastructure VCN

      Register a DNS zone in the format: <VCN DNS label>.oraclevcn.com

      For example: companyabc.oraclevcn.com

      Tip: If you want to connect to a private source on the same VCN as the private access channel, select the checkbox Virtual Cloud Network’s Domain Name as DNS Zone on the Configure Private Access Channel page to auto-fill the domain name value.

   • Private Oracle Autonomous Data Warehouse or Oracle Autonomous Transaction Processing in an Oracle Cloud Infrastructure VCN

      Register a DNS zone in the format: adb.<region>.<realm public domain>

      For example:

      – adb.ap-sydney-1.oraclecloud.com

      – adb.uk-gov-cardiff-1.oraclegovcloud.uk

3. Determine the Oracle Cloud Infrastructure VCN and subnet that you want Oracle Analytics Cloud to use for the private channel.

VCN Prerequisites
• **Region:** The VCN must be in the same region as Oracle Analytics Cloud.

**Subnet Prerequisites**

• **Size:** Each private access channel requires at least four IP addresses. Two IP addresses are required for network traffic egress, one IP address for the private access channel, and one reserved for future use. This means that the minimum subnet size for a single private access channel is "/29". For example, subnet CIDR 10.0.0.0/29.

If you have more than one Oracle Analytics Cloud instance, you might need to configure multiple private access channels. If you want to use a single subnet for multiple channels, you must ensure that the subnet is sized accordingly. Alternatively, use a dedicated subnet for each private access channel.

• **Egress Rule:** The subnet must include an egress rule that enables communication to the private data source (IP address and port).

• **Ingress Rule:** The subnet must include an ingress rule that enables communication from the private data source.

If you’re not sure, ask your network administrator.

VCN and subnet configuration tasks are typically performed by the network administrator responsible for the Oracle Cloud Infrastructure network. More information is available in Task 1 Set up the VCN and subnet at Scenario B: Private Subnet with a VPN or Scenario C: Public and Private Subnets with a VPN.

4. Ensure that you (or whoever plans to configure the private access channel for Oracle Analytics Cloud) belongs to a group that is granted the required policies to access the VCN.

Several options are available. Choose the most appropriate level for you:

**Broad Resource Access Policy**

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN TENANCY

**Limited Resource Access Policy**

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN compartment <compartment name of VCN>

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN compartment <compartment name of subnet>

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN compartment <compartment name of AnalyticsInstance>
• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE private-ips IN compartment <compartment name of AnalyticsInstance>

Moderate Resource Access Policy - Option 1

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ virtual-network-family IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE subnets IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE vnics IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE private-ips IN compartment <compartment name of AnalyticsInstance>

Moderate Resource Access Policy - Option 2

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO READ compartments IN TENANCY

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO USE virtual-network-family IN compartment <compartment name of VCN>

• ALLOW GROUP <ANALYTICS ADMIN GROUP> TO MANAGE virtual-network-family IN compartment <compartment name of AnalyticsInstance>

Typical Workflow to Set Up a Private Access Channel

If you want to set up a private access channel for an Oracle Analytics Cloud instance 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>Understand prerequisites for a private access channel</td>
<td>Make a list of the private data sources (DNS zones) that you want Oracle Analytics Cloud to access through the private access channel and ensure you have the required permissions to set up the private access channel in Oracle Cloud Infrastructure.</td>
<td>Prerequisites for a Private Access Channel</td>
</tr>
<tr>
<td>Create an Oracle Analytics Cloud instance</td>
<td>Deploy Oracle Analytics Cloud with the Enterprise Analytics feature set.</td>
<td>Create a Service</td>
</tr>
<tr>
<td>Configure a private access channel</td>
<td>Use Oracle Cloud Infrastructure Console to configure a private access channel and list any data sources (DNS zones) that Oracle Analytics Cloud must connect to privately.</td>
<td>Configure a Private Access Channel</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>More Information</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create connections to private data sources</td>
<td>Use Oracle Analytics Cloud to create a connection to the private data source.</td>
<td>Connect to Data for Visualizations and Analyses</td>
</tr>
<tr>
<td></td>
<td>The way you create the connection depends on how you want to use the data source, that is, whether you want to build a visualization, analysis, pixel-perfect report, or data model.</td>
<td>Manage Database Connections for Data Models</td>
</tr>
<tr>
<td>Manage the data sources available through a private access channel</td>
<td>Add, edit, or delete the private data sources (DNS zones) that Oracle Analytics Cloud can access through the private access channel.</td>
<td>Connect to Data for Pixel-Perfect Reports</td>
</tr>
<tr>
<td>Edit network details for a private access channel</td>
<td>Change the VCN or subnet on Oracle Cloud Infrastructure that Oracle Analytics Cloud uses to access private data sources.</td>
<td>Manage the DNS Zones You Can Access on a Private Access Channel using the Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit a Private Access Channel using the REST API</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit a Private Access Channel using the Command Line</td>
</tr>
<tr>
<td>Delete a private access channel</td>
<td>Delete a private access channel that you configured for Oracle Analytics Cloud but don't need anymore.</td>
<td>Delete a Private Access Channel</td>
</tr>
</tbody>
</table>
Configure a Private Access Channel

You can configure a private access channel using the Console, API, or command line.

**Note:**

**Required IAM Policy**

Verb: manage

**Resource Type:** analytics-instance, analytics-instances

**Custom Permission:** ANALYTICS_INSTANCE_MANAGE

See About Permissions to Manage Oracle Analytics Cloud Instances.

Verb: manage

**Resource Type:** virtual-network-family

Verb: read

**Resource Type:** compartment, compartments

To learn about other, more detailed access policy options, see Prerequisites for a Private Access Channel.

**Topics**

- Configure a Private Access Channel using the Console
- Edit a Private Access Channel using the REST API
- Configure a Private Access Channel using the Command Line

**Configure a Private Access Channel using the Console**

You can use Oracle Cloud Infrastructure Console to configure a private access channel for your Oracle Analytics Cloud instance.

When you set up a private access channel you alter the configuration of your Oracle Analytics Cloud instance. Some users might experience a temporary disruption in service during the configuration process so Oracle recommends that you plan private access channel configuration activities on critical instances accordingly.

1. In Console, click ☑️ in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you’re looking for.
4. Click the name of the instance you want to configure a private access channel for. The instance must offer the Enterprise Analytics feature set.
5. On the Instance Details page, navigate to the **Resources** section, click **Private Access Channel**, and then click **Configure Private Access Channel**.

![Private Access Channel](image)

6. For **Name**, enter any name to identify the private access channel.

7. If your Oracle Analytics Cloud instance has a **public endpoint**, select the **Virtual Cloud Network** and the **Subnet** that you want Oracle Analytics Cloud to use to access private data sources.

   Click **Change Compartment** to select resources from a different compartment. If you can’t see the VCN or subnet you want, check you have the required permissions.

   If your Oracle Analytics Cloud instance has a **private endpoint**, the private access channel automatically uses the same VCN and subnet as the private endpoint. See [Create Oracle Analytics Cloud with a Private Endpoint](#).

8. Enable access to at least one private data source:
   a. Optional. To add the domain name associated with the selected VCN as a private source, select **Virtual Cloud Network's Domain Name as DNS Zone**.
   b. In **DNS Zone**, enter the name of a domain you want to give access to.

   For example: `companyabc.com`

   - **Private data source in a corporate network peered to an Oracle Cloud Infrastructure VCN**

     Register a DNS zone in the format: `<domain name>`

     For example:

     - If the data source FQDN hostname is `data-source-ds01.companyabc.com`, add the DNS Zone as `companyabc.com`.
     - If the data source FQDN hostname is `db01.dbdomain.companyabc.com`, add the DNS Zone as
dbdomain.companyabc.com to only give Oracle Analytics Cloud access to hosts under dbdomain.companyabc.com.

- **Private data source in an Oracle Cloud Infrastructure VCN**
  Register a DNS zone in the format: `<VCN DNS label>.oraclevcn.com`
  For example: companyabc.oraclevcn.com
  Tip: If you want to connect to a private source on the same VCN as the private access channel, select the checkbox **Virtual Cloud Network’s Domain Name as DNS Zone** on the Configure Private Access Channel page to auto-fill the domain name value.

- **Private Oracle Autonomous Data Warehouse or Oracle Autonomous Transaction Processing in an Oracle Cloud Infrastructure VCN**
  Register a DNS zone in the format: `adb.<region>.<realm public domain>`
  For example:
  - adb.ap-sydney-1.oraclecloud.com
  - adb.uk-gov-cardiff-1.oraclegovcloud.uk

  c. Enter a useful description for the domain.
  d. To add additional domains, click **Add DNS Zone**.

9. Click **Configure**.

   On the Analytics Instances page, the status changes to **Active** when the configuration process is complete.

10. To test that the private access channel is working, connect Oracle Analytics Cloud to one of the private data sources you configured and verify you can access the data in Oracle Analytics Cloud.

   a. Sign-in to Oracle Analytics Cloud.
   b. Create a connection to the private data source.

      For example, if you registered the domain `companyabc.com` as a private source, set up a connection that includes this domain name.

      The way you create the connection depends on how you want to use the data source, that is, whether you want to build a visualization, analysis, pixel-perfect report, or data model.

      • Connect to Data for Visualizations and Analyses
      • Manage Database Connections for Data Models
      • Connect to Data for Pixel-Perfect Reports

c. Create a visualization, analysis, or pixel-perfect report that uses the connection and verify you can access the data.

**Configure a Private Access Channel using the REST API**

You can use the `CreatePrivateAccessChannel` operation to set up a private access channel for an Oracle Analytics Cloud instance.

Refer to the **Oracle Cloud Infrastructure REST API Reference** for information about how to use this operation:
Configure a Private Access Channel using the Command Line

You can use the `analytics-instance create-private-access-channel` command to set up a private access channel for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `analytics-instance create-private-access-channel`

Edit a Private Access Channel

You can edit a private access channel using the Console, API, or command line.

**Note:**

**Required IAM Policy**

**Verb:** manage

**Resource Type:** analytics-instance, analytics-instances

**Custom Permission:** ANALYTICS_INSTANCE_MANAGE

See *About Permissions to Manage Oracle Analytics Cloud Instances*.

**Verb:** manage

**Resource Type:** virtual-network-family

**Verb:** read

**Resource Type:** compartment, compartments

To learn about other, more detailed access policy options, see *Prerequisites for a Private Access Channel*.

Topics

- Edit Network Details for a Private Access Channel using the Console
- Manage the DNS Zones You Can Access on a Private Access Channel using the Console
- Edit a Private Access Channel using the REST API
- Edit a Private Access Channel using the Command Line
Edit Network Details for a Private Access Channel using the Console

If you deployed your Oracle Analytics Cloud instance with a public endpoint, you can change the VCN and subnet on Oracle Cloud Infrastructure that Oracle Analytics Cloud uses to access private sources.

When you deployed Oracle Analytics Cloud with a private endpoint, the private access channel uses the same VCN and subnet you configured for the private endpoint. To edit network settings for both the private endpoint and private network channel, see Change the VCN or Subnet Used to Access a Private Endpoint.

**Note:**
Changing the VCN or subnet impacts any private data sources that you configured for this private access channel. You must ensure that the new network configuration provides a network route to these sources.

1. In Console, click ✖️ in the top left corner.
2. Under **Solutions and Platform**, select **Analytics**, then **Analytics Cloud**.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure private data sources for.
5. On the Instance Details page, navigate to the **Resources** section, and click **Private Access Channel**.
6. Click the name of the private access channel you want to edit.
7. Click **Edit Configuration**.

8. Select the new **Virtual Cloud Network** or **Subnet** that you want Oracle Analytics Cloud to use to access private sources.
The private access channel and all the private sources that are associated with it inherit these changes.

You can select a VCN and subnet if your Oracle Analytics Cloud instance has a public endpoint. If your Oracle Analytics Cloud instance has a private endpoint, the private access channel automatically uses the same VCN and subnet as the private endpoint.

Click Change Compartment to select resources from a different compartment. If you can't see the VCN or subnet you want, check you have the required permissions.

9. Click Save Changes.

On the Analytics Instances page, the status changes to Active when the configuration is complete. Some users might experience a temporary disruption in service during the configuration process.

10. Test that you can access the resources from Oracle Analytics Cloud.

Sign-in to Oracle Analytics Cloud, connect to one of the private data sources that you listed, and verify you have access.

Manage the DNS Zones You Can Access on a Private Access Channel using the Console

You can add, edit, or delete the DNS zones of private sources available through the private channel at any time.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure private data sources for.
5. On the Instance Details page, navigate to the Resources section, and click Private Access Channel.
6. Click the name of the private access channel you want to edit.
7. Click Edit Private Sources.
8. To enable access to an additional DNS zone:
   a. Click **Add DNS Zone**.
   b. Enter the name of the domain you want to give access to.
      For example: companyabc.com
   c. Enter a useful description for the domain.

9. To edit an existing DNS zone:
   a. Edit the name of the domain.

   **Note:**

   If your Oracle Analytics Cloud instance has working data source connections that reference the current domain name, the connections won’t work after you remove the domain from the private access channel.

   b. Edit the description.

10. To revoke access to a DNS zone you configured earlier, click the X icon for the DNS zone.

11. Click **Save Changes**.

    On the Analytics Instances page, the status changes to Active when the configuration is complete. Some users might experience a temporary disruption in service during the configuration process.

12. Test that you can access the resources from Oracle Analytics Cloud.

    Sign-in to Oracle Analytics Cloud, connect to one of the private data sources that you listed, and verify you have access.
Edit a Private Access Channel using the REST API

You can use the `UpdatePrivateAccessChannel` operation to edit a private access channel that you configured for an Oracle Analytics Cloud instance.

You can manage the DNS zones accessible through the private access channel and, if your Oracle Analytics Cloud has a public endpoint, you can change the VCN and subnet that the private access channel uses to access the private data sources.

Refer to the *Oracle Cloud Infrastructure REST API Reference* for information about how to use this operation:

- `UpdatePrivateAccessChannel`

Edit a Private Access Channel using the Command Line

You can use the `analytics-instance update-private-access-channel` command to edit a private access channel that you configured for an Oracle Analytics Cloud instance.

You can manage the DNS zones accessible through the private access channel and, if your Oracle Analytics Cloud has a public endpoint, you can change the VCN and subnet that the private access channel uses to access the private data sources.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `analytics-instance update-private-access-channel`

Delete a Private Access Channel

You can delete a private access channel using the Console, API, or command line.

**Note:**

**Required IAM Policy**

**Verb:** `manage`

**Resource Type:** `analytics-instance`, `analytics-instances`

**Custom Permission:** `ANALYTICS_INSTANCE_MANAGE`

See About Permissions to Manage Oracle Analytics Cloud Instances.

**Verb:** `manage`

**Resource Type:** `virtual-network-family`

**Verb:** `read`

**Resource Type:** `compartment`, `compartments`

To learn about other, more detailed access policy options, see Prerequisites for a Private Access Channel.
Delete a Private Access Channel using the Console

You can delete a private access channel that you configured for Oracle Analytics Cloud but don't need anymore.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to edit.
5. On the Instance Details page, navigate to the Resources section, and click Private Access Channel.
6. Click the name of the private access channel you want to delete.
7. Click the Delete button, and then click Delete again to confirm.

On the Analytics Instances page, the status changes to Active when the deletion is complete. Some users might experience a temporary disruption in service during the configuration process.

Delete a Private Access Channel using the REST API

You can use the DeletePrivateAccessChannel operation to delete a private access channel for an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:

• DeletePrivateAccessChannel

Delete a Private Access Channel using the Command Line

You can use the analytics-instance delete-private-access-channel command to delete a private access channel for an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use this command:

• analytics-instance delete-private-access-channel
Connect to a Database Deployed on Oracle Cloud Infrastructure with a Public IP Address

Configure Oracle Analytics Cloud to connect to a database deployed on Oracle Cloud Infrastructure with a public IP address, so that end users can analyze that data in visualizations, analyses, and pixel-perfect reports.

Topics

- Typical Workflow to Connect to a Database Deployed on Oracle Cloud Infrastructure
- Prerequisites
- Record Database Information
- Enable Database Access Through Port 1521
- Connect to Your Database from Oracle Analytics Cloud

Typical Workflow to Connect to a Database Deployed on Oracle Cloud Infrastructure

If you’re connecting to an database deployment on Oracle Cloud Infrastructure 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>Verify the prerequisites</td>
<td>Verify that your environment satisfies the prerequisites required for this configuration.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>Record database information</td>
<td>Record connection information for database.</td>
<td>Record Database Information</td>
</tr>
<tr>
<td>Enable database access</td>
<td>Add an ingress rule to give Oracle Analytics Cloud access to the database.</td>
<td>Enable Database Access Through Port 1521</td>
</tr>
<tr>
<td>Connect to the database</td>
<td>Create and test your connections.</td>
<td>Connect to Your Database from Oracle Analytics Cloud</td>
</tr>
</tbody>
</table>

Prerequisites

Before you start, make sure you have the required environment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Important Information to Note</th>
</tr>
</thead>
</table>
| Set up Oracle Analytics Cloud                             | Deploy Oracle Analytics Cloud.                                              | Region
|                                                           |                                                                             | Availability Domain                                    |
| Set up a Virtual Cloud Network (VCN) on Oracle Cloud Infrastructure | Set up a VCN for the database deployment on Oracle Cloud Infrastructure. | Virtual Cloud Network Subnet
|                                                           | Note: The VCN must be in the same Region and Availability Domain as Oracle Analytics Cloud. | Same:
|                                                           |                                                                             | · Region
|                                                           |                                                                             | · Availability Domain                                  |
Connect to a Database Deployed on Oracle Cloud Infrastructure with a Public IP Address

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Important Information to Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy a database:</td>
<td>Deploy a database on the VCN in Oracle Cloud Infrastructure.</td>
<td>Public IP</td>
</tr>
<tr>
<td>• Deploy the database on the VCN in Oracle Cloud Infrastructure</td>
<td>Database Unique Name</td>
<td></td>
</tr>
<tr>
<td>• Populate the database with data</td>
<td>Host Domain Name</td>
<td></td>
</tr>
<tr>
<td>• Set up a database user with permissions to read database tables</td>
<td>Database User/Password</td>
<td></td>
</tr>
<tr>
<td>Note: The database must be in the same Region and Availability Domain as the VCN.</td>
<td>Same:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Region</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Availability Domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Cloud Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Client Subnet</td>
<td></td>
</tr>
</tbody>
</table>

Record Database Information

All the information you need to connect to a database is available in the Oracle Cloud Infrastructure Console. Record the information now, so you have the required details when you set up the connection in Oracle Analytics Cloud.

1. In Oracle Cloud Infrastructure Console, click the navigation icon.

2. Under Database, click Bare Metal, VM, and Exadata, and then click DB Systems.

3. Locate the database you want to connect to and record the Public IP address.

4. Click the name of the database you want to connect to and write down the values in these fields: Database Unique Name, Host Domain Name, Virtual Cloud Network, Client Subnet, and Port.
5. Find out the user name and password of a database user with permissions to read from this database, and write them down as you need these later. For example, the user SYSTEM.

Enable Database Access Through Port 1521

Add an ingress rule that enables Oracle Analytics Cloud to access the database through port 1521.

1. Make a note of the Oracle Analytics Cloud IP addresses that you want to allow access to. See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.

2. In the Oracle Cloud Infrastructure home page, click the navigation icon, then under Databases, click Bare Metal, VM, and Exadata, and then DB Systems.

3. Click the database that you want to connect to.

4. Click the Virtual Cloud Network link.

5. Navigate to the appropriate subnet, and under Security Lists, click Default Security List For <VCN>. 


6. Click **Add Ingress Rules**.

7. For each IP address that you want to give access to, add an ingress rule to allow any incoming traffic from the public internet to reach port 1521 on this database node, with the following settings:
   - **SOURCE CIDR**: Enter the IP address that you wrote down in Step 1.
   - **IP PROTOCOL**: TCP
   - **SOURCE PORT RANGE**: All
   - **DESTINATION PORT RANGE**: 1521
   - **Allows**: TCP traffic for ports: 1521
Connect to Your Database from Oracle Analytics Cloud

After enabling access to the database, use the database connection information you wrote down earlier to connect Oracle Analytics Cloud to the database. The way you connect to the database depends on what you want to do with the data.

- Visualize the data.
- Model the data using Data Modeler, then generate analyses and dashboards.
- Model the data with Oracle Analytics Cloud Developer Client Tool, then generate analyses and dashboards.
- Publish the data in pixel-perfect reports.

Connect to Your Database for Data Visualization

In Oracle Analytics Cloud, create an Oracle Database connection for data visualizations in the usual way. See Create Database Connections.
Use the database details you recorded earlier to fill in the Create Connection dialog.
Specify these values:

- **New Connection Name**: A name for the database you want to connect to.
- **Host**: The Public IP address for the database instance. For example, 123.213.85.123.
- **Port**: The port number that enables access to the database. For example, 1521.
- **Username**: The name of a user with read access to the database.
- **Password**: The password for the specified database user.
- **Service Name**: A concatenated name comprising Database Unique Name and Host Domain Name, separated with a period. For example, CustDB_iad1vm.sub05031027070.customervcnwith.oraclevcn.com.

**Connect to Your Database for Data Modeler**

In Oracle Analytics Cloud Console, create a connection in the usual way. See Connect to Data in an Oracle Cloud Database.

Use the database details you recorded earlier to fill in the Create Connection dialog.
Specify these values:

- **Name** and **Description**: A name for the database you want to connect to.
- **Connect using**: Select **Host, Port, and Service Name**.
- **Host**: The **Public IP** address for the database. For example, 123.213.85.123.
- **Port**: The port number that enables access to the database. For example, 1521.
- **Service Name**: A concatenated name comprising **Database Unique Name** and **Host Domain Name**, separated with a period. For example, CustDB_iad1vm.sub05031027070.customervcnwith.oraclevcn.com.
- **Connect as**: The name of a user with read access to the database.
- **Password**: The password for the specified database user.
Connect to Your Database in Oracle Analytics Cloud Developer Client Tool

In Oracle Analytics Cloud Developer Client tool, click **File**, then **Open**, then **In the Cloud** to open your data model. See Edit a Data Model in the Cloud.

When you sign in, use connection information for your Oracle Analytics Cloud to fill in the Open in the Cloud dialog.

Create a connection pool for your database. In the Physical pane, expand the **DBaaS** node, right-click the database icon, and click **Properties** to display the Connection Pool dialog. Use the database details you recorded earlier to specify **Call Interface**, **Data Source Name**, **User Name**, and **Password**.

Specify these values:

- **Call interface**: Select **Default (Oracle Call Interface (OCI))**.
- **Data Source Name**: Specify the connection details. For example:
  
  `(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=129.213.85.177)(PORT=1521)))
  (CONNECT_DATA=(SERVICE_NAME=CustDB_iad1vm.sub05031027070.customervcnwith.oraclevcn.com)))`

  For **SERVICE_NAME**, specify the concatenated **Database Unique Name** and **Host Domain Name** separated by a period, for example, `db1_phx1tv.mycompany.com`. To find both these names in Oracle Cloud Infrastructure Console, click **Databases, Bare Metal, VM, and Exadata, DB Systems**, and then click the name of your database.
Connect to Oracle Autonomous Data Warehouse with a Public IP Address

Configure Oracle Analytics Cloud to connect to Autonomous Data Warehouse over a public IP address so that end users can analyze that data in visualizations, analyses, dashboards, and pixel-perfect reports.

Topics

- Typical Workflow to Connect to Oracle Autonomous Data Warehouse with a Public IP Address
- Prerequisites
- Enable Access to Oracle Autonomous Data Warehouse
- Connect to Oracle Autonomous Data Warehouse

Typical Workflow to Connect to Oracle Autonomous Data Warehouse with a Public IP Address

If you’re connecting Oracle Analytics Cloud to Autonomous Data Warehouse over a public IP address 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>Verify the prerequisites</td>
<td>Verify that your environment satisfies the prerequisites required for this configuration.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>Enable access to Autonomous Data Warehouse</td>
<td>Upload your Autonomous Data Warehouse Client Credentials file (wallet file) to Oracle Analytics Cloud.</td>
<td>Enable Access to Oracle Autonomous Data Warehouse</td>
</tr>
<tr>
<td>Connect to Autonomous Data Warehouse</td>
<td>Create and test your connections.</td>
<td>Connect to Oracle Autonomous Data Warehouse</td>
</tr>
</tbody>
</table>

Prerequisites

Before you start, make sure you have the required environment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Important Information to Note</th>
</tr>
</thead>
</table>
| Set up Oracle Analytics Cloud | Deploy Oracle Analytics Cloud. | Region  
Availibility Domain |
### Set up Oracle Autonomous Data Warehouse

- Deploy Autonomous Data Warehouse on Oracle Cloud Infrastructure.
- Populate Autonomous Data Warehouse with data.
- Set up a database user with permissions to read database tables on Autonomous Data Warehouse.

### Important Information to Note

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Port Number</th>
<th>Service Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Obtain these details from tnsnames.ora in the Autonomous Data Warehouse Client Credentials file.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Enable Access to Oracle Autonomous Data Warehouse

To enable secure communication between Oracle Analytics Cloud and Autonomous Data Warehouse, you upload trusted SSL certificates to Oracle Analytics Cloud.

1. In Autonomous Data Warehouse Console, obtain the Client Credentials file.
   The Client Credentials file is a ZIP file containing the files cwallet.sso and tnsnames.ora. See Download Client Credentials (Wallets) in Using Oracle Autonomous Data Warehouse.

2. Extract the cwallet.sso file from the Client Credentials file.

3. Upload the cwallet.sso file to Oracle Analytics Cloud.
   a. Sign in to Oracle Analytics Cloud, open the Console and click Connections.
   b. Click Upload Wallet to upload a wallet for the first time or Replace Wallet to update an existing wallet.
   c. Click Browse and locate the wallet file (cwallet.sso) you downloaded from Autonomous Data Warehouse.
   d. Select the file and click Open.
   e. Click Update and OK to update the existing wallet file.

### Connect to Oracle Autonomous Data Warehouse

After enabling access to Oracle Autonomous Data Warehouse, use the connection details you recorded earlier to connect Oracle Analytics Cloud to Autonomous Data Warehouse. The way you connect depends on what you want to do with the data.

- Visualize the data
- Model the data using Data Modeler, then generate analyses and dashboards.
- Model the data with Oracle Analytics Cloud Developer Client Tool, then generate analyses and dashboards.
- Publish the data in pixel-perfect reports.

### Connect to Autonomous Data Warehouse for Data Visualization

In Oracle Analytics Cloud, create an Autonomous Data Warehouse connection for data visualization. See Create Connections to Oracle Autonomous Data Warehouse.
Now create a new project and data set to visualize data from your Autonomous Data Warehouse.

**Connect to Autonomous Data Warehouse for Data Modeler**

In Oracle Analytics Cloud Console, create a connection in the usual way. See Connect to Data in an Oracle Cloud Database.

Use the database details you recorded earlier to fill in the Create Connection dialog.

---

`Connect to Autonomous Data Warehouse with a Public IP Address`
Specify these values:

- **Name** and **Description**: A short name and description to identify this connection in Oracle Analytics Cloud.
- **Connect Using**: Select Host, Port, and Service Name.
- **Host**: The host name of the Autonomous Data Warehouse instance that you obtained from the downloaded `tnsnames.ora` file. For example, `adwc.example.oraclecloud.com`.
- **Port**: The port number that you obtained from the downloaded `tnsnames.ora` file. For example, 1522.
- **Service Name**: The service name that you obtained from the downloaded `tnsnames.ora` file. For example, `adwc1_high.adwc.oraclecloud.com`.
- **Connect As**: The name of a user with read access to Autonomous Data Warehouse. For example, ADMIN.
- **Password**: The password for the specified database user.
Enable SSL: Select this option. In Data Modeler, you can now model data from your Autonomous Data Warehouse using this connection.

Connect to Autonomous Data Warehouse in Oracle Analytics Cloud Developer Client Tool

You can use Oracle Analytics Cloud Client Tool to edit a data model connected to Autonomous Data Warehouse.

1. On the machine where you installed Oracle Analytics Cloud Developer Client Tool, copy the cwallet.sso, sqlnet.ora, and tnsnames.ora from the zip file that you downloaded from Autonomous Data Warehouse to the folder:
   `<Developer Client Tool installation folder>\domains\bi\config\fmwconfig\bienv\core`

2. Edit sqlnet.ora so that the wallet location points to:
   `<Developer Client Tool installation folder>\domains\bi\config\fmwconfig\bienv\core`
   For example:
   ```
   WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA = (DIRECTORY="C:\ade\admintoolOAC18.2.1\domains\bi\config\fmwconfig\bienv\core"))) SSL_SERVER_DN_MATCH=yes
   ```

3. In Oracle Analytics Cloud Developer Client tool, click File, then Open, then In the Cloud to open your data model. See Edit a Data Model in the Cloud.
   When you log in, use the connection information for your Oracle Analytics Cloud instance to fill in the Open in the Cloud dialog.
   - For Port, specify 443.
   - For Host name, specify the host domain name of your Oracle Analytics Cloud instance.
   - Select SSL. For Trust Store and Password, point to a local JDK/JRE cacerts keystore that trusts certificates signed by well-known CAs.

4. Connect to Autonomous Data Warehouse.
a. Click **File**, then **Import Metadata** to start the Import Metadata wizard, and follow the on-screen instructions.

![Import Metadata wizard](image)

b. On the Select Data Source page, for the **Data Source Name** value, specify a long TNS connection string from the downloaded `tnsnames.ora` file. Include the entire description, enclosed in brackets.

For example:

```sql
(description=(address=(protocol=tcps)(port=1522)
  (host=adwc.example.oraclecloud.com))
  (connect_data=(service_name=adwc1_high.adwc.oraclecloud.com)
  (security=(ssl_server_cert_dn="CN=adwc.example.oraclecloud.com,OU=Oracle BMCS US,O=Oracle Corporation,L=Redwood City,ST=California,C=US")))
```

c. For **User Name** and **Password**, enter the credentials for the ADMIN user or another suitable Autonomous Data Warehouse user.

You’re now ready to model the data in Oracle Analytics Cloud Developer Client Tool, publish the data model to Oracle Analytics Cloud, and create analyses and data visualizations using data from Autonomous Data Warehouse.

## Connect to a Database Deployed on Oracle Cloud Infrastructure Classic with a Public IP Address

Configure Oracle Analytics Cloud to connect to Oracle Database Classic Cloud Service deployed on Oracle Cloud Infrastructure Classic so that end users can analyze that data in visualizations, analyses, and pixel-perfect reports.

### Topics
- **Typical Workflow to Connect to a Database Deployed on Oracle Cloud Infrastructure Classic**
- **Prerequisites**
- **Record Database Information**
- **Enable Database Access Through Port 1521**
- **Connect to Your Database from Oracle Analytics Cloud**
Typical Workflow to Connect to a Database Deployed on Oracle Cloud Infrastructure Classic

If you’re connecting Oracle Analytics Cloud to a database deployed on Oracle Cloud Infrastructure 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>Verify the prerequisites</td>
<td>Verify that your environment satisfies the prerequisites required for this configuration.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>Record database information</td>
<td>Record connection information for Oracle Database Classic Cloud Service.</td>
<td>Record Database Information</td>
</tr>
<tr>
<td>Enable database access</td>
<td>Add access rules to enable Oracle Analytics Cloud access to the database.</td>
<td>Enable Database Access Through Port 1521</td>
</tr>
<tr>
<td>Connect to the database</td>
<td>Create and test your connections.</td>
<td>Connect to Your Database from Oracle Analytics Cloud</td>
</tr>
</tbody>
</table>

Prerequisites

Before you start, make sure you have the required environment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Note Important Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up Oracle Analytics Cloud</td>
<td>Deploy Oracle Analytics Cloud.</td>
<td>Region</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Availability Domain</td>
</tr>
<tr>
<td>Deploy Oracle Database Classic Cloud Service</td>
<td>Deploy Oracle Database Classic Cloud Service on the Virtual Cloud Network in Oracle Cloud Infrastructure Classic.</td>
<td>Public IP</td>
</tr>
<tr>
<td></td>
<td>· Populating Oracle Database Classic Cloud Service with data.</td>
<td>Service Name</td>
</tr>
<tr>
<td></td>
<td>· Setting up a database user with permissions to read database tables.</td>
<td>Host Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database User/Password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Same: Region</td>
</tr>
</tbody>
</table>

Record Database Information

All the information you need to connect to Oracle Database Classic Cloud Service is available in Oracle Cloud Infrastructure Console. Record the information now, so you have the required details when you set up the connection in Oracle Analytics Cloud.

1. In Oracle Cloud Infrastructure Console, click ☑️ in the top left corner.
2. Under More Oracle Cloud Services, go to Classic Data Management Services, and click Database Classic.
3. Click the name of the database you want to connect to and from the Instance Overview section, record the Service Name from the Connect String. For example, ucmdb906:1521/PDB1.504988564.oraclecloud.internal.
4. Extract and record the Service Name of the database from the connect string value. For example, PDB1.504988564.oraclecloud.internal.

5. Record the IP address of the database displayed in the Resources section.

6. Find out the user name and password of a database user with permissions to read from this database, and write them down. For example, the user SYSTEM.

Enable Database Access Through Port 1521

Add an access rule that enables Oracle Analytics Cloud to access the database through port 1521.

1. In Oracle Cloud Infrastructure Console, click the icon in the top left corner.

2. Under More Oracle Cloud Services, go to Classic Data Management Services, and click Database Classic.

3. Select the database you want to connect to.

4. Click the Manage service icon and select Access Rules.

5. For port 1521, click Actions and select Enable to enable the port for the default Oracle listener.

Connect to Your Database from Oracle Analytics Cloud

After enabling access to the database, use the database connection information you recorded earlier to connect Oracle Analytics Cloud to the database deployed in Oracle Cloud Infrastructure Classic. The way you connect to the database depends on what you want to do with the data.

- Visualize the data.
- Model the data using Data Modeler, then generate analyses and dashboards.
- Model the data with Oracle Analytics Cloud Developer Client Tool, then generate analyses and dashboards.

Connect to Your Database for Data Visualization

In Oracle Analytics Cloud, create an Oracle Database connection for data visualizations in the usual way. See Create Database Connections.
Use the database details you recorded earlier to fill in the Create Connection dialog.
Specify these values:

- **Connection Name**: The name of the Oracle Database Classic Cloud Service you want to connect to.
- **Host**: The **Public IP** address for Oracle Database Classic Cloud Service. For example, 123.213.85.123.
- **Port**: The port number that enables access to Oracle Database Classic Cloud Service. For example, 1521.
- **Username**: The name of a user with read access to Oracle Database Classic Cloud Service.
- **Password**: The password for the specified database user.
- **Service Name**: The service name on the Database Classic page. For example, PDB1.587075508.oraclecloud.internal.

**Connect to Your Database for Data Modeler**

In Oracle Analytics Cloud Console, create a connection in the usual way. See Connect to Data in an Oracle Cloud Database.

Use the database details you recorded earlier to fill in the Create Connection dialog.
Specify these values:

- **Name and Description**: The name of the Oracle Database Classic Cloud Service you want to connect to.
- **Connect Using**: Select **Host, Port, and Service Name**.
- **Host**: The **Public IP** address for Oracle Database Classic Cloud Service. For example, 123.213.85.123.
- **Port**: The port number that enables access to Oracle Database Classic Cloud Service. For example, 1521.
- **Service Name**: The service name from the Database Classic page. For example, PDB1.123456789.oraclecloud.internal.
- **Connect as**: The name of a user with read access to Oracle Database Classic Cloud Service.
- **Password**: The password for the specified database user.

**Connect to Your Database in Oracle Analytics Cloud Developer Client Tool**

In Oracle Analytics Cloud Developer Client tool, click **File, Open**, and then **In the Cloud** to open your data model in the usual way. See Edit a Data Model in the Cloud.
When you sign in, use connection information for your Oracle Analytics Cloud to fill in the Open in the Cloud dialog.

Create a connection pool for your database. In the Physical pane, expand the database node, right-click the database icon, and click Properties to display the Connection Pool dialog. Use the database details you recorded earlier to specify Call Interface, Data Source Name, User Name, and Password.

Specify these values:

- **Call interface**: Select Default (Oracle Call Interface (OCI)).
- **Data Source Name**: Specify the connection details. For example:
  
  ```
  (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
  (HOST=123.213.85.123) (PORT=1521)))
  (CONNECT_DATA=(SERVICE_NAME=PDB1.587075508.oraclecloud.internal))
  
  For SERVICE_NAME, use the Database Classic page to locate the service name. For example, PDB1.587075508.oraclecloud.internal.
  
  You’re now ready to model the data in Oracle Analytics Cloud Developer Client Tool, publish the data model to Oracle Analytics Cloud, and create analyses and data visualizations using data from Oracle Database Classic Cloud Service.

**Federate with Oracle Identity Cloud Service Manually**

In most cases, Oracle Analytics Cloud is automatically federated with the primary Oracle Identity Cloud Service instance associated with your tenancy. If you want to federate Oracle Analytics Cloud with a secondary Oracle Identity Cloud Service
instance or your tenancy is a government region where federation isn’t set up automatically, you must federate with Oracle Identity Cloud Service manually.

The way you do this depends whether your Oracle Identity Cloud Service includes the COMPUTEBAREMETAL application. If a COMPUTEBAREMETAL application doesn’t exist in your tenancy, you must perform some additional steps to set up a trusted application that you can use.

Once set up, select the new Oracle Identity Cloud Service provider before you sign-in to Oracle Cloud and then create your Oracle Analytics Cloud instance. The new Oracle Analytics Cloud instance will use the federated Oracle Identity Cloud Service that you're signed-in with. You can't reconfigure Oracle Analytics Cloud to use a different Oracle Identity Cloud Service later on.

1. Sign-in to your Oracle Identity Cloud Service console with administrator privileges.

2. In the Oracle Identity Cloud Service console, click Applications.

3. Determine whether the COMPUTEBAREMETAL application is available.
   - COMPUTEBAREMETAL application in the list
     a. Open the application, and click the Configuration tab.
     b. Expand General Information and make a note of the Client ID.
     c. Click Show Secret to display and then copy the Client Secret.
     d. Skip Step 4 and go to Step 5.
   - No COMPUTEBAREMETAL application in the list
     Continue with Step 4 to set up a trusted application.

4. Set up a trusted application.
   a. In the Applications tab, click Add Application.
   b. Click Confidential Application.
   c. Enter a suitable Name (for example, OCI_Federation) and Description (for example, Confidential application to enable federation with OCI), and then click Next.
   d. In Allowed Grant Types, select Resource Owner, Client Credentials, and JWT Assertion.
   e. In the App Roles table, add the role Security Administrator.
   f. Click Next, and then click Finish.
   g. When the Application Added dialog is displayed, make a note of the Client ID and Client Secret.
   h. Click Activate and then OK to confirm that you want to activate the application.

5. Create a group named OCI_Administrators.
   a. Click the Groups tab.
   b. Create a group called OCI_Administrators, and add one or more users to the group.

6. Federate your Oracle Identity Cloud Service in Oracle Cloud Infrastructure.
   a. Sign-in to your Oracle Cloud Infrastructure Console.
b. Under **Governance and Administration**, click **Identity**, then **Federation**.

c. Click **Add identity provider**.

d. Enter details about the Oracle Identity Cloud Service instance you want to use.
   Enter a **Name** (for example, *MyOracleIdentityCloudProvider*), **Description**, and for Type select **Oracle Identity Cloud Service**.

   Enter the Base URL for the Oracle Identity Cloud Service instance you want to use (primary or secondary), and then enter the **Client ID** and **Client Secret** values that you recorded earlier.

   e. Click **Continue**.

   f. Map the Oracle Identity Cloud Service group you created in Step 5 (*OCI_Administrators*) to the **Administrators** group in Oracle Cloud Infrastructure.

   g. Click **Add Provider**.

   The identity provider is displayed with the status **Active**.

7. Sign out of your tenancy.

   The Sign In page displays the new federated identity provider. For example *myoracleidentitycloudprovider*.

   Oracle Identity Cloud Service users who sign in through the federated identity provider inherit permissions based on their Oracle Identity Cloud Service to Oracle Cloud Infrastructure group mappings. This means that users who belong to the Oracle Identity Cloud Service group *OCI_Administrators* have all the permissions granted to the Oracle Cloud Infrastructure group *Administrators*.

8. In the Sign-in page, select the new federated identity provider, click **Continue**, and sign in.

   Any new Oracle Analytics Cloud instances that you create will use the federated Oracle Identity Cloud Service you signed-in with.

---

### Set Up a Custom Vanity URL

You can configure a custom vanity URL for your Oracle Analytics Cloud instance.

**Topics:**

- About Vanity URLs
- Prerequisites for a Vanity URL
- Typical Workflow to Set Up a Vanity URL
- Configure a Vanity URL
- Update Certificates for a Vanity URL
- Delete a Vanity URL

### About Vanity URLs

A vanity URL is a unique, customized web address that's branded for marketing purposes and helps users remember and find your web site. If you want to customize
the user login experience for Oracle Analytics Cloud, you can use your own vanity URL instead of the default URL that Oracle provides.

These examples show the standard URL for Oracle Analytics Cloud and a sample vanity URL that you might use instead:

- **Standard URL:** https://example-mytenancy.analytics.ocp.oraclecloud.com/ui
- **Vanity URL:** https://mycoolanalytics.com/ui

Typical Workflow to Set Up a Vanity URL

If you want to set up a vanity URL for an Oracle Analytics Cloud instance 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>Understand prerequisites for a vanity URL</td>
<td>Obtain the custom domain name and the required security certificates before you start.</td>
<td>Prerequisites for a Vanity URL</td>
</tr>
<tr>
<td>Deploy Oracle Analytics Cloud</td>
<td>Deploy Oracle Analytics Cloud with a public or private endpoint.</td>
<td>Create a Service</td>
</tr>
<tr>
<td>Configure a vanity URL</td>
<td>Use Oracle Cloud Infrastructure Console to configure a vanity URL.</td>
<td>Configure a Vanity URL</td>
</tr>
<tr>
<td>Update security certificates for the vanity domain</td>
<td>If the security certificate, private key file, or certificate chain associated with your vanity domain expires or changes you can upload new details.</td>
<td>Update Certificates for a Vanity URL</td>
</tr>
<tr>
<td>Delete a vanity URL</td>
<td>Delete a vanity URL that you configured for Oracle Analytics Cloud but don't need anymore.</td>
<td>Delete a Vanity URL</td>
</tr>
</tbody>
</table>

Prerequisites for a Vanity URL

Before you configure a vanity URL for an Oracle Analytics Cloud instance you need to know the custom domain name and valid certificate for the domain.

1. Obtain the custom domain name you want to use from a web service provider or use the domain name of your company.

2. Add a DNS entry that maps your custom domain name to the **IP address** of your Oracle Analytics Cloud instance.

   See [Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance](#).
3. Obtain a public digital X.509 certificate (.pem) for your vanity domain name from a Certificate Authority.
4. Obtain a private key file (.pem) that matches the certificate’s public key.
5. Obtain a certificate chain for multiple certificates (.pem).

Configure a Vanity URL

You can configure a vanity URL using the Console, API, or command line.

Note:

Required IAM Policy
Verb: manage
Resource Type: analytics-instance, analytics-instances
Custom Permission: ANALYTICS_INSTANCE_MANAGE
See About Permissions to Manage Oracle Analytics Cloud Instances.

Topics
• Configure a Vanity URL using the Console
• Configure a Vanity URL using the REST API
• Configure a Vanity URL using the Command Line

Configure a Vanity URL using the Console

You can use Oracle Cloud Infrastructure Console to configure a vanity URL for your Oracle Analytics Cloud instance.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to configure a vanity URL for.
5. On the Instance Details page, click Create Vanity URL.
6. For Hostname, enter the fully qualified, custom domain name that you want to appear in the URL.
   For example, enter mycoolanalytics.com.
   A preview of the HTTPS URL is displayed. For example: https://mycoolanalytics.com/ui/

7. Specify the digital X.509 (public key) certificate for your vanity domain.
   - Upload a valid certificate file in PEM format (.pem .cer .cn).
   - Paste the valid X.509 certificate text.

8. Enter the private key for this certificate.
   - Upload the private key file (.pem).
   - Paste the private key text.

9. Optional: In Private Key Passphrase, enter the password for the private key.

10. Optional: If your certificate requires a certificate authority chain:
    a. Select Custom Certificate Authority Chain.
    b. Enter the authority chain.
       - Upload the certificate authority chain file (.pem .cer .cn).
       - Paste the authority chain text.

11. Click Create.
    You'll know when the vanity URL is ready to use because the URL becomes a live link in the Access Information section.

12. Click the link or enter the vanity URL in a browser to test you can access Oracle Analytics Cloud.
Configure a Vanity URL using the REST API

You can use the CreateVanityUrl operation to set up a vanity URL for an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:

• CreateVanityUrl

Configure a Vanity URL using the Command Line

You can use the analytics-instance create-vanity-url command to set up a vanity URL for an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure CLI Command Reference for information about how to use this command:

• analytics-instance create-vanity-url

Update Certificates for a Vanity URL

You can update the security certificates associated with your vanity URL using the Console, API, or command line.

Note:

Required IAM Policy
Verb: manage
Resource Type: analytics-instance, analytics-instances
Custom Permission: ANALYTICS_INSTANCE_MANAGE
See About Permissions to Manage Oracle Analytics Cloud Instances.

Topics

• Update Certificates for a Vanity URL using the Console
• Update Certificates for a Vanity URL using the REST API
• Update Certificates for a Vanity URL using the Command Line

Update Certificates for a Vanity URL using the Console

If the security certificate, private key file, or certificate chain associated with your vanity domain expires or changes you can upload new details using the Console.

1. In Console, click in the top left corner.
2. Under Solutions and Platform, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.

4. Click the name of the instance you want to configure a vanity URL for.

5. On the Instance Details page, click **More Actions** and then select **Update Vanity URL Certificate**.

6. Update the digital X.509 (public key) certificate for your vanity domain.
   - Upload a valid certificate file in PEM format (.pem .cer .crt).
   - Paste the valid X.509 certificate text.

7. Update the private key for this certificate.
   - Upload the private key file (.pem .key).
   - Paste the private key text.

8. Optional: In **Private Key Passphrase**, enter the password for the private key.

9. Optional: If your certificate requires a new certificate authority chain:
   a. Select **Custom Certificate Authority Chain**.
   b. Update the authority chain.
      - Upload the certificate authority chain file (.pem .cer .crt).
      - Paste the authority chain text.

10. Click **Update**.

11. Wait a few moments for the update to complete and then click the vanity URL link that displays in the **Access Information** section to verify you can access Oracle Analytics Cloud.

**Update Certificates for a Vanity URL using the REST API**

You can use the **UpdateVanityUrl** operation to update security certificates for the vanity URL that you configured for an Oracle Analytics Cloud instance.

Refer to the **Oracle Cloud Infrastructure REST API Reference** for information about how to use this operation:

- **UpdateVanityUrl**

**Update Certificates for a Vanity URL using the Command Line**

You can use the **analytics-instance update-vanity-url** command to update security certificates for the vanity URL that you configured for an Oracle Analytics Cloud instance.

Refer to the **Oracle Cloud Infrastructure CLI Command Reference** for information about how to use this command:

- **analytics-instance update-vanity-url**
Delete a Vanity URL

You can delete a vanity URL using the Console, API, or command line.

**Note:**
- **Required IAM Policy**
  - Verb: manage
  - **Resource Type:** analytics-instance, analytics-instances
  - **Custom Permission:** ANALYTICS_INSTANCE_MANAGE

See About Permissions to Manage Oracle Analytics Cloud Instances.

Topics
- Delete a Vanity URL using the Console
- Delete a Vanity URL using the REST API
- Delete a Vanity URL using the Command Line

Delete a Vanity URL using the Console

You can delete a vanity URL that you configured for Oracle Analytics Cloud but don’t need anymore.

1. In Console, click ☐ in the top left corner.
2. Under **Solutions and Platform**, select Analytics, then Analytics Cloud.
3. Select the compartment that contains the Oracle Analytics Cloud instance you're looking for.
4. Click the name of the instance you want to edit.
5. On the Instance Details page, click **More Actions** and then select **Remove Vanity URL**.
6. Click **Remove** to confirm.

Delete a Vanity URL using the REST API

You can use the `DeleteVanityUrl` operation to delete the vanity URL configured for an Oracle Analytics Cloud instance.

Refer to the Oracle Cloud Infrastructure REST API Reference for information about how to use this operation:
- `DeleteVanityUrl`
Delete a Vanity URL using the Command Line

You can use the `analytics-instance delete-vanity-url` command to delete the vanity URL configured for an Oracle Analytics Cloud instance.

Refer to the *Oracle Cloud Infrastructure CLI Command Reference* for information about how to use this command:

- `analytics-instance delete-vanity-url`

Query Data Models Remotely Using JDBC

You can query Oracle Analytics Cloud data models from an external client tool using a JDBC connection.

Topics

- Overview to Querying Oracle Analytics Cloud Data Models Remotely
- Choosing an Assertion Type for Your JDBC Connection
- Typical Workflow to Query Oracle Analytics Cloud Data Models Remotely
- Register the BIJDBC Application Using Resource Owner Assertion
- Generate the Client Private Key and Client Certificate File
- Register the BIJDBC Application using JWT Assertion
- Set Up Refresh Security Token Generation
- Download the JDBC Driver
- Connect to Oracle Analytics Cloud Using a JDBC URL

Overview to Querying Oracle Analytics Cloud Data Models Remotely

Java Data Base Connectivity (JDBC) is an industry standard API for accessing data sources. Use JDBC-compliant client tools to access data models defined in Oracle Analytics Cloud so that you can take advantage of its analytics engine and data abstraction features.

This feature requires Oracle Analytics Cloud 5.6 or later. Before you start, verify that the Oracle Analytics Cloud instance you're connecting to is version 5.6 or later. If you're not sure, contact your Oracle representative.

JDBC uses OAuth to secure access to Oracle Analytics Cloud. OAuth 2.0 is an authorization framework that enables an application to obtain limited access to a protected HTTP resource. Using OAuth, the applications are called clients; they access protected resources by presenting an access token to the HTTP resource.

To learn more about how Oracle Cloud services use OAuth, see Introduction to OAuth in Oracle Cloud.
Typical Workflow to Query Oracle Analytics Cloud Data Models Remotely

If you’re querying Oracle Analytics Cloud data models remotely 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>Decide how you want to secure your JDBC connection</td>
<td>Depending on your security requirements, choose either Resource Owner (recommended) or JSON Web Tokens (JWT) as the assertion type.</td>
<td>Choosing an Assertion Type for Your JDBC Connection</td>
</tr>
</tbody>
</table>
| Register the BIJDBC application | Register the BIJDBC application in Oracle Identity Cloud Service to authenticate your JDBC connection. | (Recommended) Use Resource Owner assertion, see Register the BIJDBC Application Using Resource Owner Assertion. Alternatively, use JWT assertion:  
  - First, generate a private key and certificate that JWT requires, see Generate the Client Private Key and Client Certificate File.  
  - Then, use JWT assertion, see Register the BIJDBC Application using JWT Assertion. |
| Enable refresh security token generation | Set up refresh security token generation in Oracle Identity Cloud Service. | Set Up Refresh Security Token Generation |
| Download the JDBC driver | Download the JDBC driver for Oracle Analytics Cloud. | Download the JDBC Driver |
| Connect to Oracle Analytics Cloud | Connect to Oracle Analytics Cloud remotely using JDBC. Refer to the example as a guide, see Example: Connect to a Data Model Remotely Using SQuirrel. | Connect to Oracle Analytics Cloud Using a JDBC URL |

Choosing an Assertion Type for Your JDBC Connection

When you register a BIJDBC application in Oracle Identity Cloud Service, you specify an assertion type that best secures your connection.

Here’s some guidance on choosing an assertion type using the Allowed Grant Types option on the Add Confidential Application dialog.

<table>
<thead>
<tr>
<th>Assertion Type</th>
<th>Use this option when:</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Recommended) Resource Owner</td>
<td>Your application has access to the user name and password of the end user connecting to Oracle Analytics Cloud. You want to create a 'gateway' connection to query data from the BI Server. Gateway accounts always use one single user name and password.</td>
<td>We recommend using this assertion type. It's simpler to configure.</td>
</tr>
</tbody>
</table>
### Assertion Type

<table>
<thead>
<tr>
<th>Assertion Type</th>
<th>Use this option when:</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>JWT</td>
<td>You don’t have the password and you need to connect to Oracle Analytics Cloud as different users.</td>
<td>This assertion type is more complex to configure. It also allows you to impersonate any BI user in the system, therefore you must ensure that the keys you generate are secured appropriately.</td>
</tr>
</tbody>
</table>

### Register the BIJDBC Application Using Resource Owner Assertion

You register the BIJDBC application in Oracle Identity Cloud Service using Resource Owner assertion to authenticate your public JDBC connections.

1. Sign-in to Oracle Identity Cloud Service as an administrator.
2. Navigate to the Applications tab and click Add.
3. In the Add Application dialog, click Confidential Application.
4. Specify a Name (for example, bi-jdbc-connection), a Description, and then click Next.
5. Select Configure this application as a client now.
6. In Allowed Grant Types, click Resource Owner.

#### Add Confidential Application

- **Details**
- **Client**
- **Resources**
- **Authorization**

7. In the Token Issuance Policy section:
   a. Under Authorized Resources, select Specific.
   b. Click Add Scope.
   c. Select the Oracle Analytics Cloud instance you want to connect to (for example, select AUTOANALYTICSINST_<my_instance_ID>).
   d. Click Add.
8. Click Next and then Finish to display an Application Added window.
9. Copy the Client ID and Client Secret to use later.
10. Close the Application Added page.
11. Click **Activate**, then click **Activate Application**.

12. Click **Save** to display a confirmation message.

**Generate the Client Private Key and Client Certificate File**

If you decide to secure your JDBC connection using the JWT assertion type, you generate a private key and certificate to authenticate the connection.

**Note**: You don’t need a private key and certificate file if you’re securing your JDBC connection using the Resource Owner assertion type.

See [https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html](https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html).

1. Generate a key pair and key store.

   From a command prompt, issue a `keytool` command, using the command format:

   ```
   keytool -genkeypair -v -keystore <keystore name> -storetype <store type i.e PKCS12> -storepass <store pass> -keyalg <key algorithm> -keysize <key size> -sigalg <sig algorithm> -validity <validity days> -alias <alias name> -keypass <key pass>
   ```

   **For example:**

   ```
   keytool -genkeypair -v -keystore bijdbckeystore.jks -storetype PKCS12 -storepass password -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -validity 3600 -alias bijdbcclientalias -keypass password
   ```

2. Generate a public certificate.

   From a command prompt, issue a `keytool` command, using the command format:

   ```
   keytool -exportcert -v -alias <alias name> -keystore <keystore name> -storetype <store type, such as PKCS12> -storepass <store pass> -file <certificate file> -rfc
   ```

   **For example:**

   ```
   keytool -exportcert -v -alias bijdbcclientalias -keystore bijdbckeystore.jks -storetype PKCS12 -storepass password -file bijdbcclient.cert -rfc
   ```

3. Use OpenSSL to extract the private key, in PKCS8 format, from the keystore file.

   Use the command format:

   ```
   openssl pkcs12 -in <keystore file name> -passin pass:<keystore password> -nodes -nocerts -nomacver > <PKCS8 key file path>
   ```

   **For example:**

   ```
   openssl pkcs12 -in bijdbckeystore.jks -passin pass:password -nodes -nocerts -nomacver | sed -n '/BEGIN PRIVATE KEY/,$/p' > bijdbcclient.pem
   ```

4. Save the generated key and certificates in a location accessible to your client machine.
Register the BIJDBC Application using JWT Assertion

You register the BIJDBC application in Oracle Identity Cloud Service using JWT assertion to authenticate your public JDBC connections.

Before you start, generate a Client Private Key and Client Certificate File as specified in the previous step.

1. Sign-in to Oracle Identity Cloud Service as an administrator.
2. Navigate to the Applications tab and click Add.
3. In the Add Application dialog, click Confidential Application.
4. Specify a Name (for example, bi-jdbc-connection) , a Description, and then click Next.
5. Select Configure this application as a client now.
6. In Allowed Grant Types, click JWT Assertion.
7. For Security:
   a. Select Trusted Client.
   b. Click Import, enter a Certificate Alias, and then upload your client certificate file.
8. In the Token Issuance Policy section:
   a. Under Authorized Resources, select Specific.
   b. Click Add Scope.
   c. Select the Oracle Analytics Cloud instance you want to connect to (for example, select AUTOANALYTICSINST_<my_instance_ID>).
   d. Click Add.
9. Click Next and then Finish to display an Application Added window.
10. Copy the Client ID and Client Secret to use later.
11. Close the Application Added page.
12. Click Activate, then click Activate Application.
13. Click Save to display a confirmation message.

Set Up Refresh Security Token Generation

Configure your BIJDBC application to refresh security tokens.

1. In Oracle Identity Cloud Service, enable the Refresh Token option for the BIJDBC application that you created earlier.
   a. In Oracle Identity Cloud Service Console, navigate to Applications, and click the name of the BIJDBC application that you created earlier.
   b. Click Configuration, then Client Configuration.
   c. Select Refresh Token, and click Save.
If your Oracle Analytics Cloud instance was created after 12th May 2020, your BIJDBC application is now configured to refresh security tokens.

If your Oracle Analytics Cloud instance was created before 12th May 2020, perform the additional steps 2 to 4.

2. In Oracle Identity Cloud Service Console, navigate to the application associated with Oracle Analytics Cloud you want to connect to, and make a note of the following information:
• **Oracle Identity Cloud Service Hostname**

![Oracle Identity Cloud Service Hostname Image]

• **Application ID (IDCS application associated with Oracle Analytics Cloud)**

![Application ID Image]
3. Use the Oracle Identity Cloud Service REST API to generate the access token using client credentials.

Use this REST API command format:

```
```

Parameters:
- **Client-ID**: Client ID of the Oracle Identity Cloud Service application associated with your Oracle Analytics Cloud instance.
- **Client-Secret**: Client secret for the Oracle Identity Cloud Service application associated with your Oracle Analytics Cloud instance.
- **IDCS-Host**: Host name of your Oracle Identity Cloud Service instance.

See [Generate Access Token and Other OAuth Runtime Tokens to Access the Resource](#).

4. Use the Oracle Identity Cloud Service REST API to update the flag.

Use this REST API command format:

```
```

Parameters:
- **IDCS-Host**: Host name of your Oracle Identity Cloud Service instance.
- **Application-Id**: Application ID of the Oracle Identity Cloud Service application associated with your Oracle Analytics Cloud instance.
- **Access-token**: Access token value you generated earlier.
Download the JDBC Driver

Obtain the JDBC driver JAR file (bijdbc-all.jar) from an Oracle Analytics Cloud Client Tools installation on a Windows machine.

If you don't already have an installed version of Oracle Analytics Cloud Client Tools that matches your Oracle Analytics Cloud version, then download and install it first on a Windows machine. To connect to Oracle Analytics from an iOS machine, copy the JDBC driver file from the Windows installation folder to your iOS machine.

1. Download the Analytics Client Tools for Oracle Analytics.
   b. To start the download, click the Oracle Analytics Client Tools link for the version that matches your Oracle Analytics version.
   c. Accept the Oracle license agreement if prompted, and click the download link to download the software to your local machine.

2. Install Analytics Client Tools.
   a. From the downloaded ZIP file, extract the setup_bi_client-<version number>-win64.exe file.
   b. In the local download area, double-click the setup_bi_client-<version number>-win64.exe file to start the installer.
   c. Follow the on-screen instructions.

3. From the installation folder, copy the JDBC driver file <OH>/bi/bifoundation/jdbc/bijdbc-all.jar.
   To connect to Oracle Analytics from an iOS machine, copy the bijdbc-all.jar file to your iOS machine.

Connect to Oracle Analytics Cloud Using a JDBC URL

Determine the JDBC URL required to connect to your Oracle Analytics Cloud instance and test the connection.

1. In Oracle Identity Cloud Service Console, make a note of the following information:
   • Oracle Identity Cloud Service host name
- Client ID (BIJDBC application)

- Client Scope (BIJDBC application)
2. Create a `bijdbc.properties` file for OAuth authentication and authorization and add credentials for your Oracle Analytics Cloud instance.

   To connect using Resource Owner assertion, use the following format for your `bijdbc.properties` file:

   ```properties
   idcsEndpointUrl=https://<IDCS_hostname>
   idcsClientId=<ID string>
   idcsClientScope=<ID string>
   idcsClientSecret=<secret>
   user=<firstname.lastname@example.com>
   password=<mypassword>
   
   For example:

   idcsEndpointUrl=https://idcs-1a2bc345678901d2e34fgh56789j0ke.identity.c9abc1.oc9def.com
   idcsClientId=12a000dc9ef345678000ghij2kl8a34
   idcsClientScope=https://<host>.com:443urn:opc:resource:consumer::all
   idcsClientSecret=xyz
   user=myuser@office.com
   password=mypassword
   ```

   If you're using JWT assertion, omit the `password=` and `idcsClientSecret=` properties and add `certificateFile=` and `privateKeyFile=`. For example, add the following:

   ```properties
   certificateFile=D:\jdbc\bijdbcclient.cert
   privateKeyFile=D:\jdbc\bijdbcclient.pem
   
   3. Determine the URL required to connect to your Oracle Analytics Cloud instance. The format you use depends on when and how the instance was deployed.

<table>
<thead>
<tr>
<th>To connect to an instance deployed on</th>
<th>Create date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Cloud Infrastructure (Gen 2)</td>
<td>Any</td>
</tr>
</tbody>
</table>
To connect to an instance deployed on Oracle Cloud Infrastructure

Create date
Oracle Cloud Infrastructure 12th May 2020 or later

Use this URL format with OAuth:

```
jdbc:oraclebi:https://<host>:<port>/api/jdbc?
BIJDBC_PROPERTIES_FILE=<fully qualified location
and name of properties file>
```

For example:

```
\Workspace\bijdbc\bijdbc.properties
```

To connect to an instance deployed on Oracle Cloud Infrastructure

Create date
Oracle Cloud Infrastructure Before 12th May 2020

Use this URL format with OAuth:

```
jdbc:oraclebi:https://<host>:<port>/bimodeler/api/jdbc?
BIJDBC_PROPERTIES_FILE=<fully qualified location
and name of properties file>
```

For example:

```
jdbc:oraclebi:https://abcdefghi123-jklmnopqrs4t-je.analytics.ocp.oraclecloud.com:443/
```

4. Test the connection to the target Oracle Analytics Cloud instance.

Use your favorite SQL command tool to connect to Oracle Analytics Cloud with the appropriate JDBC URL. For example:

```
jdbc:oraclebi:https://abcdefghi123-jklmnopqrs4t-je.analytics.ocp.oraclecloud.com:443/api/jdbc?
BIJDBC_PROPERTIES_FILE=D:\\Workspace\\bijdbc\\bijdbc.properties
```

Example: Connect to a Data Model Remotely Using SQuirrel

This example shows how to connect to an Oracle Analytics Cloud data model using JDBC with SQuirrel SQL Client tool.

1. Register the JDBC driver.

   a. In SQuirrel SQL Client, under Drivers, click Create a New Driver.

   b. In the Example URL field, specify the BIJDBC application URL with a fully qualified properties file.

      For example: `jdbc:oraclebi:https://abcdefghi123-jklmnopqrs4t-je.analytics.ocp.oraclecloud.com:443/`
bimodeler/api/jdbc?BIJDBC_PROPERTIES_FILE=D:\Workspace\bijdbc\bijdbc.properties

c. In the Extra Class Path tab, select the BIJDBC driver (JAR file) you downloaded from Client Installer.

d. Click List Drivers, and under Class Name select oracle.bi.jdbc.AnaJdbcDriver, then save the details.

2. Create a connection or (alias).
   a. Under Aliases, click Create a New Alias.
   b. In the Driver option, select bijdbc.
   c. Edit the URL, specify credentials (if required), then click Test.
      If credentials are provided in the property file, you don't need to specify User Name or Password.
   d. Validate the connection by connecting to the Alias and exploring the metadata in the Objects section.
3. In the SQL tab, enter a sample logical SQL query and click the Run button. For more information, see Logical SQL Reference Guide.

If the connection is working, the Results tab shows the results of your query.

4. Check the Results tab to verify the rows returned by the query.
Frequently Asked Questions

Here are answers to common questions asked by administrators creating and managing services for Oracle Analytics Cloud.

Topics

• Top FAQs for Administration
  – What do I use the Oracle Cloud Infrastructure Console? Is this the same as the Console available in my 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's created?
  – How do I patch (or upgrade) my service?
  – I want to connect to the database where my organization's analytics data is stored. Do I do this from Oracle Cloud Infrastructure Console?
  – 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?

• Top FAQs for Backup and Restore
  – What does Oracle back up?
  – How often does Oracle back up?
  – How long does Oracle keep system-generated backups?
  – What do I need to back up?
  – How often should I take snapshots?
  – Where are my snapshots stored?
  – How long can I keep my snapshots?
  – Can I use the Oracle system-generated backup to restore user content instead of my snapshots?
  – Do I need to back up and restore the actual data associated with my data sets separately?
  – What capabilities in Oracle Analytics Cloud can I use to implement a disaster recovery plan?

• Top FAQs for Public or Private Endpoint Security
Top FAQs for Administration

The top FAQs for Oracle Analytics Cloud administration are identified in this topic.

What do I use the Oracle Cloud Infrastructure Console? Is this the same as the Console available in my service?

- **Oracle Cloud Infrastructure Console** — You use the Oracle Cloud Infrastructure Console to create your service instance and perform instance-level operations such as delete, scale, start, and stop.
• **Console in Oracle Analytics Cloud** — When you sign in to a particular service, you see a different administrative console where you can customize and 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 Oracle Compute Unit (OCPU) is the processing unit that Oracle uses to build your service. The larger the compute size, the greater the processing power. When you create a service with Oracle Analytics Cloud, you specify the number of OCPUs you want to deploy. For more information, see [What Sizing Options Are Available to You?](#).

See also, [Oracle PaaS and IaaS Universal Credits Service Descriptions](#).

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

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

If you're not sure which size to use, contact your Oracle representative to discuss sizing guidelines.

**How do I access my service once it's created?**

It's accessible from the Oracle Cloud Infrastructure Console. Navigate to **Analytics Cloud**, click the name of the service instance you want to access, and then click **Open URL**.

**How do I patch (or upgrade) my service?**

You don't need to patch your service. Oracle takes care of patching for you.

**I want to connect to the database where my organization's analytics data is stored. Do I do this from Oracle Cloud Infrastructure Console?**

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's created?](#).

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

Oracle Analytics Cloud provides options to restrict access when deployed with a public endpoint or a private endpoint. See [Restrict Access to Oracle Analytics Cloud Deployed with a Public Endpoint](#) and [Deploy Oracle Analytics Cloud with a Private Endpoint](#).

**How do I add the IP address of my Oracle Analytics Cloud instance to my database allowlist?**

See [Add the IP Address of Your Oracle Analytics Cloud Instance to Allowlists](#).

**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?
Go to My Oracle Support and create a service request.

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?
No. You can't access the file system for your service. Your service is managed by Oracle.

Top FAQs for Backup and Restore

The top FAQs for Oracle Analytics Cloud backup and restore are identified in this topic.

What does Oracle back up?
Oracle regularly backs up your entire Oracle Analytics Cloud environment, including system configuration and user content. Oracle Support Services use these system-generated backups to restore an environment that becomes corrupt. System-generated backups aren't accessible to customers and they're not intended to provide customer-requested recovery points.

How often does Oracle back up?
Daily.

How long does Oracle keep system-generated backups?
30 days.

Where does Oracle keep system-generated backups?
System-generated backups are stored in Oracle Cloud Infrastructure Object Storage. The Oracle Cloud Infrastructure Object Storage service is inherently a highly durable storage service and is governed by the resiliency and disaster recovery service level agreements offered by that service.

What do I need to back up?
You should regularly back up the content that users create to a file called a snapshot. User content includes catalog content such as reports, dashboards, data visualization projects, and pixel perfect reports, data sets, data flows, data models, security roles, service settings, and so on.

If something goes wrong with your content or service, 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.

**How often should I take snapshots?**

Oracle recommends that you take snapshots at significant checkpoints, for example, before you make a major change to your content or environment. In addition, Oracle recommends that you take regular weekly snapshots or at your own defined frequency based on the rate of change of your environment and rollback requirements.

**Where are my snapshots stored?**

Snapshots are saved in Oracle Cloud storage. Optionally, you can download snapshots to your own file system and store them locally.

**How long can I keep my snapshots?**

Snapshots are retained in Oracle Cloud storage forever. You can delete snapshots that you don't need.

**Can I use the Oracle system-generated backup to restore user content instead of my snapshots?**

No. System-generated backups aren't available to customers. You must use the snapshot feature to back up and restore user content.

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

Yes.

**What capabilities in Oracle Analytics Cloud can I use to implement a disaster recovery plan?**

*Target Service Uptime* information for Oracle Analytics Cloud is available at: Oracle PaaS and IaaS Public Cloud Services - Pillar document

If an unforeseen disaster happens, a well-architected business continuity plan will enable you to recover as quickly as possible and continue to provide services to Oracle Analytics Cloud users.

Oracle Analytics Cloud offers several features that you can implement to minimize disruption for users:

- **Snapshots**: Oracle recommends that you back up user content regularly to a snapshot. If required, you can restore the content in your snapshot to a redundant Oracle Analytics Cloud environment. See Take Snapshots and Restore.

- **Pause and resume**: You can deploy a passive backup Oracle Analytics Cloud environment, and use the pause and resume feature to control metering and minimize costs. See Pause and Resume a Service.

- **Diverse regional availability**: Oracle Analytics Cloud is available in several global regions. You can deploy a redundant Oracle Analytics Cloud environment in a different region to mitigate the risk of region-wide events. See Data Regions for Platform and Infrastructure Services.
Top FAQs for Public or Private Endpoint Security

The top FAQs for securing access to Oracle Analytics Cloud through a public or private endpoint are identified in this topic.

In which regions is this feature available?
All regions.

Can I use REST API or Command Line Interface (CLI) to create my Oracle Analytics Cloud instance with a public or private endpoint?
Yes. You can use the Console, REST API or CLI commands. See Create a Service.

Why can't I see the VCN I want to use in the Create Instance dialog?
You must select the compartment in which the VCN was created and you must have the required permissions. See Prerequisites for a Public Endpoint and Prerequisites for a Private Endpoint.

My Oracle Analytics Cloud instance has a public endpoint. Can I change this to a private endpoint?
No. You can create an instance with a public endpoint or a private endpoint. You can't switch between the two.

If you want to protect your public endpoint, you can add your own, very specific access control rules. See Manage Access Rules for a Public Endpoint using the Console.

I created an Oracle Analytics Cloud instance with a private endpoint but I'm unable to access the Oracle Analytics Cloud URL from my browser?
After creating your Oracle Analytics Cloud instance, you must configure Domain Name Server (DNS) resolution on your private network to access the private endpoint. See Typical Workflow to Deploy Oracle Analytics Cloud with a Private Endpoint.

I created an Oracle Analytics Cloud instance with a public endpoint and defined access rules but I'm unable to access the Oracle Analytics Cloud URL from my browser?
Check that the machine from which you're trying to access Oracle Analytics Cloud is included in the access control list. You can review the current access rules to check whether it's missing using the console. See Manage Access Rules for a Public Endpoint using the Console.

Where can I find the IP address for my Oracle Analytics Cloud instance?
You can find the IP address, Gateway IP address, and other useful information on the Additional Details tab in the Oracle Cloud Infrastructure. See Find the IP Address or Host Name of Your Oracle Analytics Cloud Instance.
Do I have any tools to test or debug network issues from my corporate network?

You can use \texttt{nslookup} to find IP address information for your Oracle Analytics Cloud instance.

\begin{verbatim}
# Use nslookup
nslookup analytics.ocp.oraclecloud.com <DNS server IP address>
\end{verbatim}

You can use \texttt{netcat} or \texttt{cURL} to check whether your Oracle Analytics Cloud instance is accessible:

\begin{verbatim}
# Use Netcat
nc -zv analytics.ocp.oraclecloud.com 443
# Use cURL
curl -v https://analytics.ocp.oraclecloud.com/public/dv/ping
\end{verbatim}

### Top FAQs for Private Data Sources

The top FAQs when setting up a private access channel for Oracle Analytics Cloud are identified in this topic.

**What data sources can I connect to over a private access channel?**

To find out which data sources you can connect to through a private access channel, see Supported Data Sources. Look for the data sources with the connectivity option \textit{private access channel} in the "Use in Data Sets" and "Use in Data Models" columns.

\begin{note}
Private access channels enable you to connect to private data source hosts. You can't use a private access channel to access any other types of private host, such as a private FTP or SMTP host.
\end{note}

**Can I use a private access channel to access Oracle-specific DNS zones?**

In most cases, no. Access to most Oracle-specific DNS zones is restricted, for example \texttt{oracle.com} and \texttt{oraclecloud.com}. You can't register these DNS zones as private sources and connect to them over a private access channel.

The only Oracle-specific DNS zone you can register as a private source in a private access channel is \texttt{adb.<region>.oraclecloud.com}. For example, \texttt{adb.us-ashburn-1.oraclecloud.com}. You can use this format to access private Oracle Autonomous Data Warehouse and Oracle Autonomous Transaction Processing databases.

**How do I connect to a private Oracle Autonomous Data Warehouse in a customer VCN?**

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the
private Oracle Autonomous Data Warehouse is deployed. See Configure a Private Access Channel using the Console.

2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private Oracle Autonomous Data Warehouse on port 1522. See Working with Security Lists.

3. Register Oracle Autonomous Data Warehouse as a private source in the private access channel using the DNS zone format adb.<region>.oraclecloud.com. For example, adb.us-ashburn-1.oraclecloud.com. See Manage the DNS Zones You Can Access on a Private Access Channel using the Console.

4. Obtain the regional wallet for the private Oracle Autonomous Data Warehouse. See Download Client Credentials (Wallets).

5. In Oracle Analytics Cloud, create a connection to Oracle Autonomous Data Warehouse that uses the regional wallet and select the service name of the private Oracle Autonomous Data Warehouse instance you want to connect to from the list. See Connect to Oracle Autonomous Data Warehouse.

How do I connect to a private data source in my Oracle Cloud Infrastructure VCN?

1. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses a subnet in the virtual cloud network (VCN) where the private data source is deployed. See Configure a Private Access Channel using the Console.

   In the Configure Private Access Channel page, select the checkbox VIRTUAL CLOUD NETWORK's DOMAIN NAME as DNS ZONE.

2. Ensure that the subnet the private access channel uses has an egress rule to communicate with the private data source on its port. See Working with Security Lists.

3. If you didn't select the checkbox in step 1, register the DNS zone of your VCN in the format <VCN DNS label>.oraclevcn.com. For example, companyabc.oraclevcn.com. See Manage the DNS Zones You Can Access on a Private Access Channel using the Console.

4. In Oracle Analytics Cloud, create a connection that specifies the hostname of the VCN where the private data source is deployed. See Connect to Data for Visualizations and Analyses and Manage Database Connections for Data Models.

How do I connect to a private data source in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See Access to Your On-Premises Network.

2. Set up a private DNS resolver in the Oracle Cloud Infrastructure VCN. Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See Private DNS and Private DNS Implementation (A-Team Blog).

3. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network. See Configure a Private Access Channel using the Console.
4. Ensure that the subnet the private access channel uses has an egress rule to communicate with IP address and port of the private data source. See Working with Security Lists.

5. Register the DNS zone of the data source in the format <domain name>. For example, if the data source FQDN hostname is data-source-ds01.companyabc.com, add the DNS zone as companyabc.com. See Manage the DNS Zones You Can Access on a Private Access Channel using the Console.

6. In Oracle Analytics Cloud, create a data source connection using the FQDN hostname data-source-ds01.companyabc.com. See Connect to Data for Visualizations and Analyses and Manage Database Connections for Data Models.

How do I connect to a private data source using an IP address in my corporate network peered to an Oracle Cloud Infrastructure VCN?

1. Set up a direct connection between your corporate network and Oracle Cloud Infrastructure VCN. See Access to Your On-Premises Network.

2. Create a private DNS view and then add a zone (in the view) for your custom domain. For example, ocivcn.companyabc.com. See Private DNS.

3. In the zone you just created, add a DNS record type A, and map the IP address to the fully qualified hostname. For example, datasource-ds-01.ocivcn.companyabc.com.

4. Navigate to the DNS Resolver option for your VCN and associate the private DNS VCN you created in step 2. See Private DNS Resolver. Configure one of the following:
   - DNS forwarder: Configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server. See Private DNS and Private DNS Implementation (A-Team Blog).
   - Hostname to IP address mapping: Add a custom record type A entry for the data source IP address mapping to an FQDN hostname under a unique DNS domain. For example, if the data source IP address in your corporate network is 10.40.100.55 and your corporate DNS Zone domain is companyabc.com, add a DNS record type A that maps datasource-ds-01.ocivcn.company.com to 10.40.100.55.

5. In Oracle Cloud Infrastructure Console, configure a private access channel for the Analytics instance that uses the subnet in the virtual cloud network (VCN) that is connected to the corporate network. See Configure a Private Access Channel using the Console.

6. Register the DNS zone of the data source in the format ocivcn.<domain name>. For example, if the data source DNS record is datasource-ds-01.ocivcn.companyabc.com, add the DNS Zone as ocivcn.companyabc.com. See Manage the DNS Zones You Can Access on a Private Access Channel using the Console.

7. In Oracle Analytics Cloud, create a data source connection using the hostname datasource-ds-01.ocivcn.companyabc.com. See Connect to Data for Visualizations and Analyses and Manage Database Connections for Data Models.
Top FAQs for Vanity URLs

The top FAQs when setting up a vanity URL for Oracle Analytics Cloud are identified in this topic.

**How many vanity URLs can I create for my Oracle Analytics Cloud instance?**

One. See [Set Up a Custom Vanity URL](#).

**Does the standard URL continue to work?**

Yes.

**Can I use a self-signed certificate when defining a vanity URL?**

No. Self-signed certificates aren’t supported. However, you can create your own root signing certificate and use that to sign a certificate that you generate yourself. See [Prerequisites for a Vanity URL](#).

**Are wildcard certificates supported?**

Yes.

**Can I try this feature without registering a public DNS entry?**

Yes. In the `/etc/hosts` file on your client machine, add an entry for the vanity host name you plan to use that points to the IP address of your Oracle Analytics Cloud instance. The vanity URL works on that machine.
Troubleshoot

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

Topics

• I see an error message when I try to create a service
• I see an entitlement error message in the Create Instance dialog
• I’m having problems creating a service
• How do I diagnose other issues?
• Where do I find the OCID for my service?
• When do I contact Oracle Support?

I see an error message when I try to create a service

You must sign in to your Cloud Account through Oracle Identity Cloud Service. If you don’t, you see this error message when you try to create a service with Oracle Analytics Cloud:

Please ensure that you are logged into the console with an IDCS identity provider when creating an Analytics Instance

Sign out, and sign back in through Oracle Identity Cloud Service.
I see an entitlement error message in the Create Instance dialog

If you activated your Cloud Account in North America, EMEA, Asia Pacific (APAC) or Latin America (LAD) before Oracle Analytics Cloud is available on Oracle Cloud Infrastructure (Gen 2) in these regions, you might see this message:

Error: OAC-DAL-001031: Analytics Cloud entitlement is not available in your account.

Initially, only new Universal Credit customers, who activate their accounts in North America, EMEA, APAC or LAD after the official Oracle Analytics Cloud launch date, can create Analytics instances. Existing customers with accounts in North America, EMEA, APAC, or LAD will have access to Oracle Analytics Cloud soon.

If you’re an existing customer with an account in North America or EMEA, see I followed the instructions to create a service on Oracle Cloud Infrastructure Gen 2. Why do I see the error “Analytics entitlement is not available in your account”?

I’m having problems creating a service

In the Oracle Cloud Infrastructure Console, navigate to the Analytics Cloud page. Check the Status to see why provisioning failed. If you’re not sure what to do, contact Oracle Support for assistance.

How do I diagnose other issues?

If you experience issues with your service, make a note of the Oracle Cloud ID (OCID) allocated to the service and contact Oracle Support for assistance.

Where do I find the OCID for my service?

In the Oracle Cloud Infrastructure Console, navigate to the Analytics Cloud page. Click Show or Copy next to the OCID value for your service.

When do I contact Oracle Support?

If you encounter a problem creating a service, record any error messages you see in the user interface, and contact Oracle Support for assistance.

Contact Oracle Support if you want help with your service:

- You experience performance issues.
• Your service isn't available.