Oracle® Cloud

Migrating API Platform Cloud Service Instances to Oracle Cloud Infrastructure

ORACLE®

Oracle Cloud Migrating API Platform Cloud Service Instances to Oracle Cloud Infrastructure, 19.3.3

F17023-04

Contents

Audience

This book is intended for Administrators who want to migrate their API Platform Cloud Service instances to Oracle Cloud Infrastructure.

Documentation Accessibility

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

Access to Oracle Support

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

Conventions

The following text conventions are used in this document:

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

1
Learn About Migrating to Oracle Cloud Infrastructure

These topics help you learn about the benefits to migrating your existing Oracle Java Cloud Service instances to Oracle Cloud Infrastructure, and also provide an overview of the migration process and tools.

Topics:

- Why Migrate to Oracle Cloud Infrastructure
- About the Migration Scope
- About Oracle Cloud Infrastructure
- About the Migration Task Flow
- About the Migration Tooling

Why Migrate to Oracle Cloud Infrastructure

Oracle encourages you to migrate your existing cloud resources to Oracle Cloud Infrastructure regions. You can gain several advantages by doing so.

In Oracle Cloud, you provision resources in specific regions, which are localized to geographic locations. Certain regions support the Oracle Cloud Infrastructure platform.

Oracle Cloud Infrastructure is Oracle's modern cloud platform that's based on the latest cloud technologies and standards. It provides more consistent performance and better features at lower costs. Oracle continues to invest in Oracle Cloud Infrastructure, including the addition of new regions, services, and features. See Data Regions for Platform and Infrastructure Services.

You can benefit from these additional administrative features when you migrate your cloud resources to Oracle Cloud Infrastructure:

- Provides a fully managed environment for the Mangement Server. Oracle is responsible for the uptime, reliability and any scaling requirements, thus reducing your overall service maintenance costs.
- New feature updates are automatically pushed out when they are ready. You don't need to perform any upgrades to get new features.

To learn more, see Upgrade Your Classic Services to Oracle Cloud Infrastructure.

About the Migration Scope

Before you migrate an existing Oracle API Platform Cloud Service instance to Oracle Cloud Infrastructure, ensure that the service instance meets the prerequisites for the migration.

Oracle does *not* currently support the migration of Oracle API Platform Cloud Service Classic instances that meet any of these conditions:

- The service instance includes multiple domain partitions.

- The service instance is running Oracle WebLogic Server 11g and includes Java Message Service (JMS) migratable targets.

This guide does not include detailed procedures on the configuration of basic Oracle Cloud Infrastructure security, network, and storage resources that might be required to support your Oracle API Platform Cloud Service instance on Oracle Cloud Infrastructure. Instead, this guide provides references to the Oracle Cloud Infrastructure documentation as appropriate.

This guide does not include detailed procedures for tasks done with the Oracle Identity Cloud Service graphical user interface. Instead, this guide provides references to the Oracle Identity Cloud Service documentation as appropriate.

About Oracle Cloud Infrastructure

This topic helps you get familiar with basic Oracle Cloud Infrastructure security, network, and storage concepts, and compare them to their equivalent concepts in Oracle Cloud Infrastructure Classic.

Cloud resources in Oracle Cloud Infrastructure are created in logical compartments. You also create fine-grained policies to control access to the resources within a compartment.

You create instances within an Oracle Cloud Infrastructure region. You also specify an availability domain (AD), if supported in the selected region. Oracle Cloud Infrastructure Classic does not use availability domains.

A virtual cloud network (VCN) is comprised of one or more subnets, and an instance is assigned to a specific subnet. In Oracle Cloud Infrastructure Classic, you assign instances to IP networks or the shared network. Typically, you create one subnet for the shared network, and create a separate subnet for each IP network in Oracle Cloud Infrastructure Classic. Note that unlike Oracle Cloud Infrastructure Classic, Oracle Cloud Infrastructure does not allow you to reserve IP addresses for platform services.

A subnet's security lists permit and block traffic to and from specific IP addresses and ports. In Oracle Cloud Infrastructure Classic, an instance's access rules provide similar capabilities, although security lists are configured at the subnet level.

Instances can communicate with resources outside of Oracle Cloud by using Oracle Cloud Infrastructure FastConnect, which provides a fast, dedicated connection to your on-premises network. This service is equivalent to Oracle Cloud Infrastructure FastConnect Classic. Alternatively, use IPSec VPN in Oracle Cloud Infrastructure as a replacement for VPN as a Service (VPNaaS) or Corente in Oracle Cloud Infrastructure Classic.

A bucket in Oracle Cloud Infrastructure Object Storage can be used to store files and share them with multiple instances. A user's generated authentication token (auth token) is required to access the bucket. Oracle Cloud Infrastructure Object Storage Classic provides the same service in Oracle Cloud Infrastructure Classic, but does not use auth tokens.

To learn more, see Key Concepts and Terminology in the Oracle Cloud Infrastructure documentation.

About the Migration Task Flow

Get an overview of the process that you use to migrate your existing Oracle API Platform Cloud Service instances to Oracle Cloud Infrastructure.

The following diagram shows the migration topology for a typical Oracle API Platform Cloud Service instance.
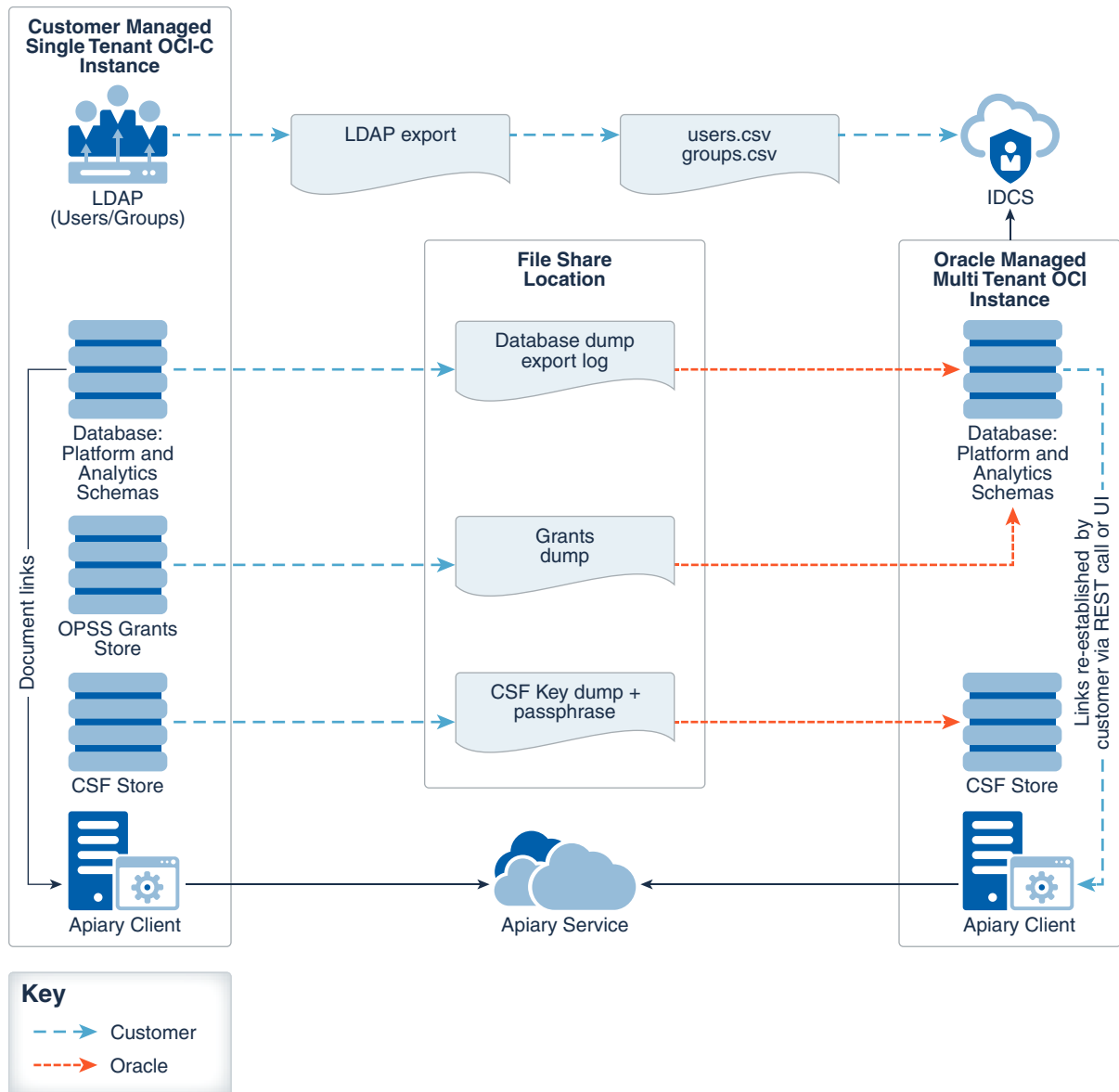
There are three levels of migration:

- You prepare data for migration.
- Oracle performs the migration.
- You perform post-migration tasks.

At a high level, the pre-migration process is comprised of these tasks:

- Submit a service request (SR) asking for Oracle to migrate your API Platform Cloud Service instance to Oracle Cloud Infrastructure, and then download the `ldap-to-idcs-csv.sh` script and Migration Application that Oracle will provide in the SR.

- Provision an Oracle API Platform Cloud Service instance, which Oracle uses as the final destination for the migrated artifacts.

- Export users from LDAP, then use a script to convert the output to the `users.csv` and `groups.csv` CSV files that Oracle Identity Cloud Service needs.

- Import the CSV files into Oracle Identity Cloud Service.

- Because LDAP export does not preserve user and group assignments to application roles, you must assign roles manually.

- Export the data from the database schema so that Oracle can import it into the Oracle-managed database in the Oracle Cloud Infrastructure environment.

- Install the Migration Application that you downloaded from your service request.

- Export CSF data to extract the credential information for services and service accounts from the original service instance's secure storage.

- Export your grants.

- Send your information to Oracle by uploading it to your service request.

After receiving all your data, Oracle performs the migration for you.

At a high level, the post-migration process is comprised of these tasks:

- Re-establish links between the APIs and Apiary projects.

- Register a gateway.

- Test the migrated instance.

About the Migration Tooling

Learn about the migration tooling provided by Oracle for the pre-migration process.

Oracle provides two tools that help you complete the pre-migration tasks.

- LDAP data conversion script (`ldap-to-idcs-csv.sh`)
  This is a Bash Shell script that converts your instance's exported LDAP data from your API Platform Cloud Service instance on Oracle Cloud Infrastructure Classic into `.csv` files. Bash v4.x is required. When migrating your instance, Oracle imports the `.csv` files into your Oracle Identity Cloud Service identity domain. You can find a detailed description on how the script works inside the script as code comments.

- Migration Application
  This application retrieves certain data from the API Platform Cloud Service instance on Oracle Cloud Infrastructure Classic so that Oracle can import it into your new service instance. You must install the application on your API Platform Cloud Service instance on Oracle Cloud Infrastructure Classic. The application exposes some REST endpoints (`<server>/apiplatform/mtmigration/*`) that implement the retrieval logic for the data.

2
Prepare for Migration

Summarizes what you need to do to prepare for migration.

Topics:

- Create a Service Request for Migration
- #unique_19
- Create an Oracle API Platform Service Instance
- Transfer Identity Data
- Export the Data from the Database Schema
- Install the Migration Application
- Export CSF Data
- Export Grants
- Send the Information to Oracle

Create a Service Request for Migration

Initiating a Service Request (SR) with Oracle customer support starts the process of migrating your API Platform Cloud Service instance to Oracle Cloud Infrastructure.

Oracle performs migration for you, so you must create a Service Request (SR) to request this service. After you create the SR, Oracle provides two tools you download and use for completing the pre-migration steps.

1. Open the My Oracle Support portal at support.oracle.com.

2. Create a Service Request (SR) for Oracle to migrate your instance to Oracle Cloud Infrastructure.

   Oracle will provide access to tooling you will use for the pre-migration process.

3. Given directions from the SR, download the LDAP data conversion script (`ldap-to-idcs-csv.sh`) and Migration Application.

After you have completed the pre-migration steps, you then upload your data to the SR.

Access Oracle API Platform Cloud Service

You access API Platform Cloud Service through the web console.

Depending on how you signed up for Oracle Cloud, you'll be directed to either the Oracle Cloud Infrastructure Console or the Oracle Cloud Infrastructure Classic Console.

Topics

Access Oracle API Platform Cloud Service from the Oracle Cloud Infrastructure Console

On most Oracle Cloud accounts, which are Universal Credits subscriptions, you access the API Platform Cloud Service console from the Oracle Cloud Infrastructure Console.

1. Sign in to Oracle Cloud.

   The Infrastructure Console is displayed.

2. From the Infrastructure Console, click the navigation menu ≡ in the top left corner, expand **Platform Services**, and then click **API Platform**.
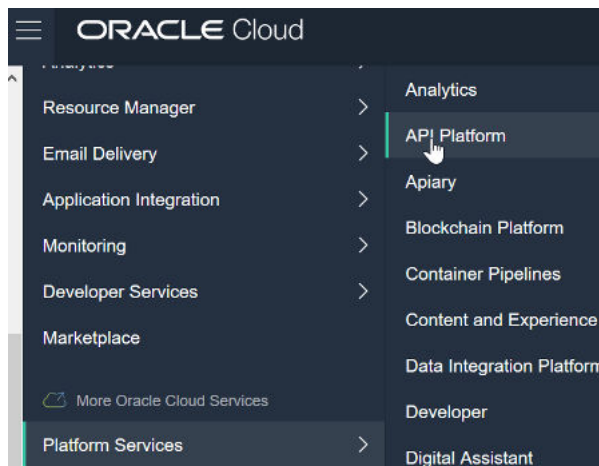
   The Instances page is displayed.

3. From the Instances page, you can create a new API Platform Cloud Service, or you can click an existing instance to view or manage it.

   To view help for the current page, click the help icon at the top of the page.

Access Oracle API Platform Cloud Service Classic from the Oracle Cloud Infrastructure Classic Console

On older Oracle Cloud accounts that are not Universal Credits subscriptions, you access the API Platform Cloud Service console from the Oracle Cloud Infrastructure Classic Console.

1. Sign in to Oracle Cloud.

   The Infrastructure Classic Console is displayed.

2. From the Infrastructure Classic Console, click the navigation menu ▤ in the top left corner, and then click **API Platform Classic**.

The Instances page is displayed.

3. From the Instances page, you can create a new API Platform Cloud Service, or you can click an existing instance to view or manage it.

Create an Oracle API Platform Service Instance

Create an Oracle API Platform Cloud Service instance to use as a target for the migration to Oracle Cloud Infrastructure.

Create a new service instance that will be the final destination for your migrated artifacts. After you create the instance, you share the region and identity domain details with Oracle. Oracle uses this information to import the artifacts from your original Oracle Cloud Infrastructure Classic instance and perform sanity checks. When the migration is complete, Oracle returns the new service instance's ownership to you.

Before you begin, ensure that you have subscribed to the required services, collected the required information for each service, and created SSH keys. See Before You Begin with Oracle API Platform Cloud Service in *Using Oracle API Platform Cloud Service*.

To create an Oracle API Platform Cloud Service instance by using the Provisioning wizard on the service console:

1. Open the service console.
   - If you have a Universal Credits subscription, see Access Oracle API Platform Cloud Service from the Oracle Cloud Infrastructure Console.
   - If you do not have a Universal Credits subscription, see Access Oracle API Platform Cloud Service Classic from the Oracle Cloud Infrastructure Classic Console .

2. Click **Create Instance**.

3. Complete the remainder of the steps documented in Create an Oracle API Platform Cloud Instance in *Using Oracle API Platform Cloud Service*.

4. Append the instance name, region, and identity domain to your Service Request.

   See Create a Service Request for Migration.

Oracle uses this service instance for the migration target.

Transfer Identity Data

The target Oracle API Platform Cloud Service instance on Oracle Cloud Infrastructure will use Oracle Identity Cloud Service for user accounts and security, while the

originating Oracle API Platform Cloud Service Classic instance uses LDAP. You must export the LDAP data.

Topics

- [Export Users from LDAP](#)
- [Convert the Data File to CSV](#)
- [Import the CSV Files into IDCS](#)

Export Users from LDAP

The first step is to export the users from the LDAP server.

The directory into which you export the LDAP data must exist before your perform the export. If it does not exist, the function will silently fail.

To export user data from LDAP:

1. Create a directory for the exported files, if necessary.

2. Log on to the WebLogic Server Console.

3. Click **Security Realms** and select your realm.

4. Click **Migration** and then click **Export**.

A `DefaultAuthenticator.dat` file is created in the directory you specified.

Convert the Data File to CSV

You must convert the `DefaultAuthenticator.dat` data file from LDAP into CSV files to create usernames for the Oracle API Platform Cloud Service environment.

Use the `ldap-to-idcs-csv.sh` script you imported to convert the `DefaultAuthenticator.dat` file from LDAP to the `users.csv` and `groups.csv` files.

In the target Oracle API Platform Cloud Service environment, Oracle Identity Cloud Service uses full email addresses as usernames, for example, `john.example@example.com`. The original Oracle API Platform Cloud Service Classic environment you are migrating from does not use full email addresses, for example, `john.example`. You must either use the script provided to update the usernames, or change them manually, depending on how you specified the username. In the case where the original username is of the form `john.example`, the script appends the domain name `example.com` to this name to obtain `john.example@example.com`. If you use a different format for your original usernames, you must update them manually.

To convert the data file into CSV files:

1. Copy the `ldap-to-idcs-csv.sh` script you downloaded to the `DefaultAuthenticator.dat` file location.

2. Open the `ldap-to-idcs-csv.sh` script and review the instructions on how to set environment variables that control the script's behavior.

3. Set the environment variables as directed.

4. Run `./ldap-to-idcs-csv.sh` to generate the `users.csv` and `groups.csv` files.

   The `users.csv` and `groups.csv` files are generated.

5. Review the `users.csv` and `groups.csv` files and apply fixes manually where necessary.

Import the CSV Files into IDCS

After you have created the CSV files, you can then import them into IDCS.

For prerequisites, additional information about this procedure, and troubleshooting, see Importing User Accounts and Importing Groups in *Administering Oracle Identity Cloud Service*.

To import the CSV files into IDCS:

1. Log in to the IDCS console.

2. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Users**.

3. Click **Import**.

4. In the **Import Users** dialog, click **Browse** to navigate to the location of `users.csv` and select the file.

5. Verify that the path and name of the CSV file that you selected appear in the **Select a file to import** field.

6. Click **Import**.

7. In the Identity Cloud Service console, expand the **Navigation Drawer**, and then click **Groups**.

8. Click **Import**.

9. In the **Import Groups** dialog, click **Browse** to navigate to the location of `groups.csv` and select the file.

10. Verify that the path and name of the CSV file that you selected appear in the **Select a file to import** field.

11. Click **Import**.

You can view the results. When you import either users or groups, a dialog appears with a **Job ID** link for the import job. Click the link to view the details on the Jobs page. If a **Schedule ID** appears instead, it means that the job cannot be processed immediately. You can copy the **Schedule ID** and use it to search for the on the Jobs page.

Assign Users and Groups to Application Roles

After importing users and groups into Oracle Identity Cloud Service, assign application roles to them.

Exporting users and groups from LDAP doesn't preserve assignments to application roles. You must assign roles manually.

1. Access the Oracle Identity Cloud Service console.

2. Expand the **Navigation Drawer**, and then click **Applications**.

3. Select your application.

4. Click the **Application Roles** tab.

5. Assign users to your Oracle application. See Assigning Users to Oracle Applications in *Administering Oracle Identity Cloud Service*.

6. Assign groups to your Oracle application. See Assigning Groups to Oracle Applications in *Administering Oracle Identity Cloud Service*.

7. Import the users and groups for application roles. See Import Users and Groups for Oracle Application Roles in *Administering Oracle Identity Cloud Service*.

User and group assignments to application roles are complete.

Export the Data from the Database Schema

Export the data from the database schema so that Oracle can import it into the Oracle-managed database in the Oracle Cloud Infrastructure environment.

To export the database schema data:

1. In the file system of your original database server, create a data dump directory, and make the `oracle` user its owner.

```
sudo su -
mkdir/u01/apics-dump
chown oracle:dba /u01/apics-dump
```

2. From SqlPlus or SqlDeveloper, use a connection string such as the following to connect to the PDB:

```
sqlplus system/<system-user-password>@localhost:1521/pdb1
```

3. Map the database to the directory you just created.

```
-- create the mapping
create or replace directory apics_dump as '/u01/apics-dump';
-- grant permissions
grant read, write on directory apics_dump to public;
-- verify the mapping exists
select directory_name, directory_path from all_directories;
```

4. Export the data dump from the OS command prompt.

```
sudo su - oracle
# replace the placeholders with the appropriate parameters
expdp system/<system-user-password>@localhost:1521/pdb1 schemas=<schema-
prefix>_APIP, <schema-prefix>_APIA exclude=TABLE:\"= \'HISTORY\'\"
directory=apics_dump dumpfile=apiexp.dmp logfile=apiexp.log
```

Note that the `HISTORY` table is excluded from the data dump. The history will start over from scratch in your new, migrated instance. Excluding the `HISTORY` makes the dump file size much smaller.

Install the Migration Application

Install the Migration Application in order to implement the curl commands used when you export CSF data and grants.

The name of the deployment must be **API MT Migration Services**.

To install the Migration Application:

1. Copy the downloaded `oracle.apiplatform.upgrade.migration.app.ear` file to the `/u01/app/oracle/suite/apip/lib` directory on both your Managed Servers.

2. Open your WebLogic Administration Console.

3. Navigate to the **Deployments** page on the WebLogic Administration Console, click **Lock & Edit**, and then click **Install**.

4. Select the **oracle.apiplatform.upgrade.mtmigration.app.ear** file, and then click **Next**.

5. Select **Install this deployment as an application**, and then click **Next**.

6. Type `API MT Migration Services` into the **Name** field, and then click **Finish**.

7. Click **Activate Changes**.

Export CSF Data

Export CSF data to extract the credential information for services and service accounts from the secure storage used by your original service instance.

- Export the CSF keys.

```
curl -X POST -u <username>:<password> '<service-url>/apiplatform/
mtmigration/keystore' --data 'passphrase=<your-passphrase-for-
migration>' -o apicskeys.out
```

The `username` and `password` can be the credentials of any user with administrator privileges.

The resulting file is encrypted, using the passphrase you specify.

Export Grants

Export the grants.

Grants are stored in OPSS, so they are not part of the exported database dump. You must export them separately.

1. Run the following curl command that exports the grants.

```
curl -X POST -u <username>:<password> '<service-url>/apiplatform/
mtmigration/grants' -o grants.zip
```

The `username` and `password` can be the credentials of any user with administrator privileges.

2. If the user and/or group names have changed, for example, if an email domain was added, complete the following steps:

   a. Extract the `mapping.json` file from `grants.zip`.

   b. In the case where the `fromUser` and `toUser` names are both LDAP names in the `mapping.json` file, edit the `toUser` value to the correct user name for Oracle Identity Cloud Service.

      Example of when `fromUser` and `toUser` values are both LDAP:

      ```
      {
          "fromUser": "john.doe",
          "toUser": "john.doe"
      }
      ```

      Edit `toUser` as follows:

      ```
      {
          "fromUser": "john.doe",
          "toUser": "john.doe@example.com"
      }
      ```

   c. Add the `mapping.json` file back to `grants.zip`.

Send the Information to Oracle

Send your data to Oracle to complete the migration.

1. Collect the following information from previous steps:

   • Database dump file, including the export log

   • CSF keys and passphrase

   • Exported grants

2. Upload your information to the Service Request you created for Oracle to migrate your instance.

3. In your API Platform Cloud Service account, create a new user for your Oracle contact, and assign this user the Administrator role.

   Oracle needs this Administrator user to perform data import tasks and do sanity checking on the imported data.

Oracle imports your data and performs the migration for you.

3
Complete the Post-Migration Steps

Learn how to complete the migration.

Topics:

- [Fix Apiary Links](#)
- [Register Gateway Nodes](#)
- [Test the Migrated Instance](#)

Fix Apiary Links

Re-establish links between the APIs and Apiary projects.

The Oracle API Platform Cloud Service instance on Oracle Cloud Infrastructure uses a different Apiary OAuth client than the original Oracle API Platform Cloud Service Classic instance on Oracle Cloud Infrastructure Classic. You must re-establish links between APIs to Apiary projects in the new instance, through a REST API call. You can use the REST API to look up the credentials in the database and change them to the correct credentials.
As an alternative, you can use the API Platform Cloud Service console. See Link an Oracle Apiary Specification in *Using Oracle API Platform Cloud Service*.

To fix the Apiary links:

1. If you don't have `jq`, enter the following command as the command prompt.

   ```
   sudo yum install jq
   ```

2. Identify your `client_id`, `client_secret`, `account_id`, and `instance_id`.

   See Find Your Client ID and Client Secret in *Using Oracle API Platform Cloud Service*.

3. Obtain an access token from Oracle Identity Cloud Service.

   ```
   export TOKEN=(curl -u <client_id>:<client_secret> -X POST https://idcs-
   <account_id>.identity.oraclecloud.com/oauth2/v1/token -H 'cache-
   control: no-cache' -d 'grant_type=password&scope=https://
   <instance_id>.apiplatform.ocp.oraclecloud.com:
   443.apiplatform&username=<username>&password=<password>'| jq -r
   ".access_token")
   ```

4. Use the following REST endpoint to fix the Apiary links.

   Use the same Apiary credentials you use when you connect to Apiary from the Management Portal.

   ```
   curl -k -i -X POST -H "Authorization: Bearer ${TOKEN}"-H "Content-Type:
   application/json" -d
   ```

```
'{"username":"<username>","password":"<password>"}' <service-url>/
apiplatform/mtmigration/apiary
```

Register Gateway Nodes

Create a new gateway node and register it with the logical gateway created during migration.

Logical gateways are created for the Oracle API Platform Cloud Service instance on Oracle Cloud Infrastructure as part of the data migration process, but it's not possible to migrate attached gateway nodes. You must create new gateway nodes and register them with the new logical gateways. You can't attach an existing node that was attached to a logical gateway on Oracle API Platform Cloud Service Classic to a new logical gateway for an Oracle API Platform Cloud Service instance.

Complete the following general steps:

1. Open the Management Portal and locate the logical gateways created during the migration process.

2. Create new gateway nodes.

    See Install a Gateway Node in *Using Oracle API Platform Cloud Service*.

3. Register the new gateway nodes with the logical gateways created during the migration process.

    See Register a Node to a Logical Gateway in *Using Oracle API Platform Cloud Service*.

4. Change each gateway node's network routing so that API invocations go to the new nodes.

    See Manage Gateways in *Using Oracle API Platform Cloud Service*.

For more information on gateway management, see Manage Gateways in *Using Oracle API Platform Cloud Service*.

Test the Migrated Instance

After you have fixed Apiary links and registered new gateway nodes, test the migrated instance.

To test your migrated API Platform Cloud Service instance, use the following guidelines:

1. In the Management Portal, perform the following tasks:

    a. Log in as the Administrator user, step through all main pages (APIs, Applications, Plans, Services, Service Accounts, Gateways), and check whether the object lists you see are correct.

    b. Log in from a restricted user account to ensure that grants have been transferred correctly, and that the restricted user can view *only* what is allowed to a restricted user.

    c. From each main page, open an object and check the validity of the details. Preform the following specific checks on the individual pages:

        APIs

- If you have APIs with Apiary specification, open those APIs and verify the Apiary information.

- Check if API analytics data appears correctly. You will see only analytics data that was collected in your your original system before you exported your database dump.

Services, Service Accounts

- If you have associated credentials, use the REST API to check that the credentials are correct. Do this in order to verify that the CSF key transfer was successful.

Gateways

- Check that gateway analytics data appear correctly.

- Verify that the gateway nodes you created and registered are alive, they are polling as expected, and new analytics data are flowing in from them.

2. In the Developer Portal perform the following tasks:

   a. Perform the same checks you performed in the Management Portal for APIs, Applications, and Plans.

   b. For applications, review the application analytics and verify the content is accurate.

The migration process is complete.