Oracle® Cloud

Migrating Oracle MFT Cloud Service Instances to Oracle Cloud Infrastructure

Release 19.1.5
F16657-02
April 2019

Oracle Cloud Migrating Oracle MFT Cloud Service Instances to Oracle Cloud Infrastructure, Release 19.1.5

F16657-02

Primary Author: Oracle Corporation

Contents

4 Perform Oracle Cloud Infrastructure Prerequisites

5 Complete the Post-Migration Tasks

Preface

Migrating Oracle Managed File Transfer Cloud Service Instances to Oracle Cloud Infrastructure describes how to migrate an existing Oracle Managed File Transfer Cloud Service instance from an Oracle Cloud Infrastructure Classic region to an Oracle Cloud Infrastructure region.

Topics:

Audience

Migrating Oracle Managed File Transfer Cloud Service Instances to Oracle Cloud Infrastructure is intended for users who need to migrate existing Oracle Managed File Transfer 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.

Related Resources

For more information, see these Oracle resources:

- Oracle Managed File Transfer Cloud Service documentation in the Oracle Cloud Library on the Oracle Help Center.
- Oracle Cloud at `http://cloud.oracle.com`.

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

Learn about the benefits of migrating your existing Oracle Managed File Transfer Cloud Service to Oracle Cloud Infrastructure.

Topics:

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. A region supports either the Oracle Cloud Infrastructure Classic or Oracle Cloud Infrastructure platform.

Oracle Cloud Infrastructure is Oracle's more modern infrastructure platform that's based on the latest cloud technologies and standards. It typically provides better performance than Oracle Cloud Infrastructure Classic. Oracle Cloud Infrastructure also has more predictable pricing and lower costs in terms of Oracle Compute Units (OCPUs) per hour. Most importantly, 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 in Oracle Cloud Infrastructure when you migrate your cloud resources from Oracle Cloud Infrastructure Classic:

- Organize cloud resources into a hierarchy of logical compartments.
- Create fine-grained access policies for each compartment.

Compare Oracle Cloud Infrastructure to Classic

Get familiar with basic Oracle Cloud Infrastructure security, network, and storage concepts, and 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 Oracle Cloud Infrastructure Users and Groups

Use the Identity and Access Management (IAM) system in Oracle Cloud Infrastructure to manage users, groups, and policies.

For example, the following Oracle Cloud Infrastructure policy grants members of the group `MyGroup` all privileges to all resources in the compartment `MyCompartment`:

```
Allow group MyGroup to manage all-resources in compartment MyCompartment
```

By default, this system is also configured to use Oracle Identity Cloud Service as a federated identity provider. Therefore, when you define policies in Oracle Cloud Infrastructure, you can reuse existing users and groups in Oracle Identity Cloud Service. You can either add users to a new group in Oracle Cloud Infrastructure, or map an existing Oracle Identity Cloud Service group to an Oracle Cloud Infrastructure group.

While policies control access to services in Oracle Cloud Infrastructure, administrator roles control access to platform services that are found only on the My Services Dashboard. Assign Oracle Identity Cloud Service users and groups to administrator roles in order to grant them access to services that are not found in Oracle Cloud Infrastructure.

- Common Policies in the Oracle Cloud Infrastructure documentation
- Federating with Oracle Identity Cloud Service in the Oracle Cloud Infrastructure documentation
- Create a Service Administrator in *Getting Started with Oracle Cloud*

About the Migration Scope

There are certain pre-requisites that you should be aware of before you begin migration to Oracle Cloud Infrastructure.

Before migration, ensure the following:

- The source version for migration in the cloud is 12.1.3 or later.
- It is assumed that disaster recovery is not configured for the source environment. Note that appropriate changes have to be made to the instructions if disaster recovery is configured.
- It is assumed that the production environment has a load balancer. Otherwise, the steps have to be modified and adapted accordingly.

Understand Migration for Oracle Managed File Transfer Cloud Service

For the migration of Oracle Managed File Transfer Cloud Service to Oracle Cloud Infrastructure, you'll provision a new cloud instance of Oracle Managed File Transfer Cloud Service, migrate or recreate configurations from the old source environment and then transition to the newly provisioned cloud instance.

You have to keep the following details in mind for a migration to Oracle Cloud Infrastructure:

- The source version of the cloud instance that you want to migrate can be 12.1.3 or later.
- SOA Cloud Service/MFT Cloud Service uses internal LDAP.
- SOA Cloud Service/MFT Cloud Service uses OTD.
- SOA Cloud Service/MFT Cloud Service uses KSS.
- You can directly copy and import security information between the source and the target Oracle Managed File Transfer Cloud Service instances.

About the Migration Task Flow

Get an overview of the process that you use to migrate your existing Oracle Managed File Transfer Cloud Service instances to Oracle Cloud Infrastructure.

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

1. Prepare for the migration and perform any prerequisite tasks in Oracle Cloud Infrastructure.
2. Create the target Oracle Managed File Transfer Cloud Service in an Oracle Cloud Infrastructure region.

3. Use Oracle Data Guard to migrate any application databases in Oracle Cloud Infrastructure Classic regions to Oracle Cloud Infrastructure Database.
4. Use the Oracle WebLogic Server Deploy Tooling to discover and export the domain configuration, applications and other supporting files from your source Oracle Managed File Transfer Cloud Service instance.
5. Use the Oracle WebLogic Server Deploy Tooling to update the domain configuration on your target Oracle Managed File Transfer Cloud Service instance and to deploy your applications.
6. Test your applications on the target instance, and perform any other post-migration tasks.

2

Prepare to Migrate Oracle MFT Cloud Service to Oracle Cloud Infrastructure

Before you migrate your service instances from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure, understand how the migration affects your existing instances, identify the necessary compute shapes, and create the network to support your migrated service instances.

Topics:

About Downtime Requirements

The migration process does not affect the availability of your existing Oracle Managed File Transfer Cloud Service instance in Oracle Cloud Infrastructure Classic. This instance continues to run and can serve client requests during this process.

After a service instance is migrated successfully, you can reroute clients to the new instance in Oracle Cloud Infrastructure.

Design the Oracle Cloud Infrastructure Network

Before you migrate your service instances from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure, you must design and implement a virtual cloud network (VCN) to support your migrated service instances.

You can create new Oracle Cloud Infrastructure compartments, VCNs, and subnets for your service instances, or you can use existing ones. See these topics in the Oracle Cloud Infrastructure documentation:

- Managing Compartments
- VCNs and Subnets
- Security Lists

Consider the following guidelines when you create or select a network for your service instances:

- If instances communicate using the default shared network in Oracle Cloud Infrastructure Classic, then use a single subnet for these instances.
- If instances are on separate IP networks in Oracle Cloud Infrastructure Classic, then use separate subnets for these instances.

- A VCN should have an address range that includes all of the IP networks in Oracle Cloud Infrastructure Classic that need to communicate. Alternatively, configure peering between multiple VCNs.
- A subnet should have at least the same number of addresses as the corresponding IP network in Oracle Cloud Infrastructure Classic.
- If an instance was created in Oracle Cloud Infrastructure Classic without public IP addresses, then use a private subnet for this instance.
- If custom access rules were created for an instance in Oracle Cloud Infrastructure Classic to control communication to or from the instance, then create a security list in Oracle Cloud Infrastructure and assign the security list to the appropriate subnets. To use custom security lists, you must assign the instance to a custom subnet, and not the default subnet.

Before you create service instances in Oracle Cloud Infrastructure that use your new network resources, you must create policies that grant your service access to these resources. See Prerequisites for Oracle Platform Services in the Oracle Cloud Infrastructure documentation.

Select Oracle Cloud Infrastructure Shapes

Identify compute shapes that provide similar IaaS resources in Oracle Cloud Infrastructure to the shapes that you're currently using for your service instances on Oracle Cloud Infrastructure Classic.

A compute shape defines the IaaS resources, such as OCPUs and memory, that are available to a specific node in a service instance. Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic each has its own set of standard compute shapes. See:

- About Shapes in *Using Oracle Cloud Infrastructure Compute Classic*
- Compute Shapes in the Oracle Cloud Infrastructure documentation

To ensure that a migrated service instance has the same performance characteristics as the original instance, and can support an equivalent workload, choose Oracle Cloud Infrastructure shapes that most closely map to the Oracle Cloud Infrastructure Classic shapes that you specified when you created the instance.

You must also confirm that the chosen shapes are available in your Oracle Cloud tenancy. Oracle configures shape limits for an Oracle Cloud Infrastructure region, or for a specific availability domain within a region. You can use the console to view the current shape limits for your tenancy, and to request a limit increase if necessary. See Service Limits in the Oracle Cloud Infrastructure documentation.

3

Migrate an Oracle Managed File Transfer Cloud Service instance to Oracle Cloud Infrastructure

Create a new Oracle Managed File Transfer Cloud Service instance in Oracle Cloud Infrastructure, and then use the WebLogic Deploy Tooling to migrate your WebLogic Server domain resources and applications from your existing instance in Oracle Cloud Infrastructure Classic.

Topics:

Create Infrastructure Resources

You must create certain networking and storage resources for instances in Oracle Cloud Infrastructure.

To learn about these resources, see Prerequisites for Oracle Platform Services in the Oracle Cloud Infrastructure documentation.

For step-by-step instructions to create these resources, see Creating the Infrastructure Resources Required for Oracle Platform Services.

> **Note:**
>
> Make a note of the region, tenancy, and storage bucket from the Oracle Cloud Infrastructure console. Construct the backup storage URL in the format mentioned below.
>
> `https://swiftobjectstorage.<region>.oraclecloud.com/v1/<namespace>/<containerName>`
>
> Where,
> `<namespace>` is the tenancy, and
>
> `<container name>` is the storage bucket name.
>
> Enter the above URL in the **Storage Container Name** during provisioning of the instance in Oracle Cloud Infrastructure.

Provision MFT Cloud Service

Provision a new MFT Cloud Service instance before starting the other migration and side-by-side related tasks. You'll migrate or recreate configurations from your old source environment into this newly provisioned instance of MFT Cloud Service.

Create a simple hello world application (MFT transfer) and test to make sure it works.

Prepare Clients for Migration/Side-by-Side Upgrade (MFT)

Configure and prepare your clients such that the transition of HTTP clients from the old deployment to the new deployment is smooth and happens by switching the DNS entry.

These changes can be done gradually over time because after these changes are completed everything continues to work as before the changes. This includes some changes to the source environment.

To prepare clients:

1. Get a DNS name issued from DNS issuing authority. Point this DNS name to the source environment load balancer.

   If you are already using a DNS name in clients skip this step. This step is required only if you are using an Oracle Traffic Director (OTD) IP address.

2. Create a new port in the source environment load balancer that matches the target MFT Cloud Service port number. Add routing role to this new port to route to the original load balancer port in the source environment.

   Note that on-premises MFT applications can use a different port number than the target MFT Cloud Service environment. This makes it impossible to switch clients during transition from the old to the new deployment by switching the DNS.

3. Change all clients to use the DNS name and new port.

   Note that the DNS name will also be used by clients of the embedded FTP and SFTP server that write files.

For SSL, it might be required that the trust certificate for the target environment server has to be pre-configured at the client so that transition from the source to the target environment works smoothly.

Prepare Your Source for Migration/Side-by-Side Upgrade (MFT)

Prepare your source for migration/side-by-side upgrade by exporting or capturing the needed artifacts from the source environment.

To prepare your source:

1. Export all metadata from the source environment.

   See Importing and Exporting the MFT Configuration in *Using Oracle Managed File Transfer*.

   In earlier versions of MFT, a configuration plan (that the user can edit) is not generated during export. However, you'll require a configuration plan for import. In such cases, the easiest way to generate a configuration plan is to import it into a test 12.2.1.2 deployment and generate the configuration plan from the test deployment.

2. Grab the domain file system artifacts such as Java callouts.
3. Adjust the configuration plans for deployment to MFT Cloud Service.

   Change URLs to values appropriate for MFT Cloud Service.

Prepare Your Target Environment (MFT)

Prepare your target environment by importing or recreating all the configurations of your source. This will ensure successful deployment of the target MFT Cloud Service instance.

To prepare your target environment:

1. Implement any security configurations.

   Security configurations can be: custom Oracle Web Service Manager (OWSM) policies, Credential Store Framework (CSF) keys, certificates, users, groups, custom Oracle Platform Security Service (OPSS) roles, custom OPSS permissions, group memberships, enterprise roles, OPSS credentials and so on.

   For information on OPSS commands to migrate keystores , see Managing Keystores with WLST in *Securing Applications with Oracle Platform Security Services*.

   For information on OPSS commands to migrate credentials, see Managing Credentials with WLST in *Securing Applications with Oracle Platform Security Services*.

   For information on OWSM commands to migrate custom policies, see Migrating Policies in *Administering Web Services*.

> **Note:**
>
> If the source environment is MFT Cloud Service, the internal LDAP data can be migrated into the target environment MFT Cloud Service instance. Migration is supported for MFT Cloud Service 12.1.3, 12.2.1 and 12.2.1.2.

2. Import artifacts with the configuration plan. Do not deploy yet.
3. Add file system artifacts captured from source environment – Java callouts.
4. Test by creating a simple hello world application (MFT transfer). Ensure that it works.
5. Set your tuning settings if they are available.
6. Redo any Enterprise Manager configuration steps manually.

   For details, see Reconfigure Configuration Parameters and Tuning in MFT Cloud Service.
7. If MFT Cloud Service is going to access endpoints on-premises then you may need VPN.

   You can setup VPN through VPNaaS.
8. Apply UMS configuration manually to the target environment.
9. Enable the embedded SFTP server by making any documented changes.

Transition from Old Deployment to New Deployment (MFT)

After you have prepared your source and target environments for the migration/side-by-side upgrade, you can transition your production system from old deployment to new deployment.

To transition from old to new deployment:

1. Disable inbound sources in the source environment, if the inbound address in both old and new deployment is same.

   For inbound sources which are remote FTP/SFTP servers, ensure that already processed files in the directory are not processed again after transitioning to the target environment by removing them from the directory.
2. Complete deployment and enable everything in the target environment.

   Note that for some inbound sources, the address is different and clients have to change the address in the source and switch.
3. Switch the DNS.

   The DNS switch is not instantaneous and may take a while (depending on TTL settings in routers) to propagate across the internet.
4. Note that the source environment will continue processing backlogged transfers while new messages are processed by the target environment. When all backlogged transfers are processed and there is no need to rollback, you can destroy the source environment.

   Switch external clients of the embedded FTP and SFTP server that read files to the new deployment, after all files in the old deployment have been processed.

5. If you have directories in the embedded FTP server for storing data that is not processed by MFT, it is up to you to either copy these files or deal with them as you see fit.

Reconfigure Configuration Parameters and Tuning in MFT Cloud Service

Re-configure any tuning and configuration parameters that you had previously set in the source environment or you need to change in the target environment.

You'll perform these steps as part of preparing your target environment for transitioning from the old to the new environment.

- Schedule Purge
- See Tuning Oracle Managed File Transfer in *Fusion Middleware Tuning Performance Guide*.

Migrate Data Components in MFT Cloud Service

Migrate your data components such as LDAP, OPSS and OWSM from your source to the target environment.

You'll perform these tasks as part of preparing your target environment for transitioning from the old to the new environment.

> **Note:**
>
> The migration steps described here are for target version of MFT Cloud Service 12.2.1.2. If you want to do the migration for other versions, refer to the product documentation.

Move LDAP Data

The tasks for migrating LDAP data in MFT Cloud Service are similar to the tasks for migrating LDAP data in SOA Cloud Service.

See Move LDAP Data.

Move OPSS Data

The tasks for migrating OPSS data in MFT Cloud Service are similar to the tasks for migrating OPSS data in SOA Cloud Service.

See Move OPSS Data.

Move OWSM Data

The tasks for migrating OWSM data in MFT Cloud Service are similar to the tasks for migrating OWSM data in SOA Cloud Service.

See Move OWSM Data.

Move LDAP Data

LDAP data includes the Oracle WebLogic Server specified user, group, enterprise role and security policies (predefined Oracle WebLogic configurations and configurations that users have added to internal LDAP). Import and move the LDAP data from your source to your target environment.

For migrating LDAP data from your on-premises SOA instance to the cloud, refer to the WebLogic LDAP documentation or refer to your on-premises IDM documentation. Check if any migration is possible or you will need to manually re-enter everything.

If you are doing a side-by-side upgrade in the cloud, note that internal LDAP is used.

The WebLogic console has commands to export and import internal LDAP. This can be used to move users/groups/group memberships/enterprise roles etc. By default, LDAP import will not overlay users and groups, and other artifacts that are already there. This is the desired behavior. For details, see Exporting and Importing Information in the Embedded LDAP Server in *Administering Security for Oracle WebLogic Server*.

When you export the whole LDAP, information which the integration does not use such as XACML policies and default credential mapper, also gets exported. This information may get seeded by WebLogic and exporting/importing this information can have issues. So do not export/import this information.

For information on how to handle the WebLogic OOTB security provider data migration, see:

- Security Data Migration in *Developing Security Providers for Oracle WebLogic Server*.
- Migrating Security Data in *Administering Security for Oracle WebLogic Server*.

You can navigate to any security provider that supports the migration functions and invoke the import( ) and/or export ( ) MBean operation such that this security provider's data can be addressed outside of any other security provider data. See Migrating Data with WLST in *Administering Security for Oracle WebLogic Server*.

Here is an example with direct lookup vs navigation:

```
$ java weblogic.WSLT
% connect()
% serverConfig()
% realm = cmo.getSecurityConfiguration().getDefaultRealm()
% atn = realm.lookupAuthenticationProvider('DefaultAuthenticator')
% atn.exportData('DefaultAtn', 'myFile', None)
% disconnect()
```

You can use WLST if you decide that you need any data beyond the default Authenticator (Embedded LDAP users/groups). It is recommended that you also export roles.

Exporting LDAP Data

This is an example of commands to export LDAP data from 12.1.3.

Before exporting LDAP data, perform the following on the source environment, 12.1.3

```
ssh -i opc_rsa opc@source_admin_host_ip
sudo -su oracle
cd /u01/
cd /app/oracle/middleware/oracle_common/common/bin/
./wlst.sh


connect('weblogic','welcome1','t3s://<source_admin_host_ip>:<admin_port>')
currentDomainName=cmo.getName()
```

1. Export users and groups.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/AuthenticationProviders/DefaultAuthenticator')
   cmo.exportData('DefaultAtn', 'filename', Properties())
   ```

   Example: `cmo.exportData('DefaultAtn','/tmp/ldapdata/DefaultAuthenticator.dat', Properties())`

2. Export security roles.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/RoleMappers/XACMLRoleMapper')
   cmo.exportData('XACML','filename', Properties())
   ```

3. Export credential mapper.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/CredentialMappers/DefaultCredentialMapper')
   cmo.exportData('DefaultCreds','filename', Properties())
   ```

4. Export XACML Authorizer.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/Authorizers/XACMLAuthorizer')
   cmo.exportData('XACML','filename', Properties())
   ```

   Where `filename` is the file path where data needs to be exported.

5. Copy exported file to local box.

   Create a directory where you can copy the exported data.

   ```
   scp DefaultAuthenticator.dat <username:source_host_ip>:/<local_export_dir_path>
   ```

Example:

```
scp DefaultAuthenticator.dat myuser@myhost.us.oracle.com:/scratch/
exp_dat


scp DefaultCredentialMapper.dat <username:source_host_ip>:/<local_ex-
port_dir_path>


scp XACMLAuthorizer.dat <username:source_host_ip>:/<local_ex-
port_dir_path>


scp XACMLRoleMapper.dat <username:source_host_ip>:/<local_ex-
port_dir_path>
```

6. Copy LDAP data from the 12.1.3 host to the 12.2.1.2 host.

   Create a folder on the target environment.

   Go to the target directory folder where exported files should be copied ('.' represents current directory).

   ```
   scp <username:TARGET_SOACS_HOST_IP>:/<local_export_dir>/DefaultAuthenti-
   cator.dat
   ```

   Example:

   ```
   scp myuser@myhost.us.oracle.com:/scratch/export_data/DefaultAuthentica-
   tor.dat


   scp <username:TARGET_SOACS_HOST_IP>:/<local_export_dir>/DefaultCreden-
   tialMapper.dat


   scp <username:TARGET_SOACS_HOST_IP>:/<local_export_dir>/XACMLAuthoriz-
   er.dat


   scp <username:TARGET_SOACS_HOST_IP>:/<local_export_dir>/XACMLRoleMap-
   per.dat
   ```

Importing LDAP Data

This is an example of commands to import LDAP data into 12.2.1.2.

Before importing LDAP data, perform the following on the target 12.2.1.2 environment:

```
ssh -i opc_rsa opc@host_adminip_target
sudo -su oracle
```

```
cd /u01/app/oracle/middleware/oracle_common/common/bin/
./wlst.sh


connect('weblogic','welcome1','t3s://<target_host_ip>:<target_host_port>')
currentDomainName=cmo.getName()
```

1. Import users and groups.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/AuthenticationProviders/DefaultAuthenticator')
   cmo.importData('DefaultAtn','filename', Properties())


   cmo.importData('DefaultAtn','/tmp/temp_usera/DefaultAuthenticator.dat',
   Properties())
   ```

2. Import security RoleMapper.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/RoleMappers/XACMLRoleMapper')
   cmo.importData('XACML','filename', Properties())
   ```

3. Import credential mapper.

   The WebLogic credential mapper is not used. In general, it is recommended not to import data that is not used. This is because this data may have WebLogic seeded data which might conflict with seeded data in the target environment. However it is provided for completeness.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/CredentialMappers/DefaultCredentialMapper')
   cmo.importData('DefaultCreds','filename', Properties())
   ```

4. Import XACML Authorizer.

   WebLogic XACML authorization is not used. In general, it is recommended not to import data that is not used. This is because this data may have WebLogic seeded data which might conflict with seeded data in the target environment. However it is provided for completeness.

   ```
   cd('serverConfig:/SecurityConfiguration/' + currentDomainName +
   '/Realms/myrealm/Authorizers/XACMLAuthorizer')
   cmo.importData('XACML','filename', Properties())
   ```

   Where `filename` is the directory in which the imported data needs to be placed.

Move OPSS Data

Move OPSS data by exporting from the source (on-premises applications in case of migration to the cloud and Oracle Managed File Transfer Cloud Service in case of side-by-side upgrade). Then copy the exported file to the newly provisioned target environment and import.

OPSS consists of the following:

- OPSS policies application roles and permissions

  These are mostly seeded automatically but in some cases customers can create their own roles and policies. Also, customers will define role memberships.

- Keys, certificates and trust certificates

  These are used for authentication, signing, encryption and SSL. Trust certificates are public certificates of certificate issuing authorities to establish the trust chain.

- Credentials

Note the following when you move OPSS data:

- Bootstrap credentials and bootstrap keys must be preserved in the target environment domain and should not be overlayed with import and export.

  If nothing was done to specifically import/export keys into the system keystore in the source system, it is recommended that you do not migrate the source system keystore since the same contents will get seeded when the destination domain is created.

- Migration of the OPSS audit service is not required.
- Server SSL key must be preserved in the target environment domain and should not be overlayed with import and export.

> **Note:**
>
> Source environment deployment server certificates with host names in the certificates cannot be reused.

Move OWSM Data

Move OWSM data by exporting it from the source and importing it to the target environment.

OWSM has the following artifacts of interest:

- CSF keys: There are references to CSF keys in OWSM policies/policy overrides. There is no change required as long as actual values are available in the credential store owned by OPSS. CSF keys must be available in the target environment.
- certs and keys: OWSM supports two types of keystores: JKS (file based) and KSS (owned by OPSS). The certificates/aliases in the source environment should be made available in the target environment. There are references to keys/certificates in OWSM policies/policy overrides.
- Custom OWSM authorization policies: These are same as custom policies.
- Custom OWSM policies

  See Exporting Documents from the Repository Using WLST in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

  See Importing Documents into the Repository Using WLST in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

- Additional configurations that may be required: trust config and OAuth config

In 12c, `exportWSMRepository` exports all custom policies from the repository, the trust configuration, OAuth configuration, and any other configuration documents.

In 11g, the specific custom policies have to be enumerated to export them. Note that it may not be as simple as moving the documents from 11g to 12c because as part of upgrade, the OWSM upgrade plugin takes care of adding/updating 12c specific changes in the artifacts. There may be no easy way to automate policy movement from 11g to 12c as part of migration.

Transition Inbound Adapters/Transports

For successful migration/side-by-side upgrade, you need to transition inbound adapters/transports.

There are two use cases to consider for transitioning inbound adapters/transports. During transition, you disable the inbound adapters/transport at the source and enable it on the target environment. Also, when you first deploy the projects to the target environment, you do not want inbound adapters/transports to process production messages right away until you are ready for the transition. To solve both the use cases, you can do any of the following:

- Change the etc/host file or add/remove permissions for the file directory.
- Change to composite or adapter activate/deactivate.

  SOA supports adapter activate/deactivate only in 12.1.3. In B2B, the inbound channel is disabled by default on import. OSB does not support this.
- Change the inbound endpoints to test or true endpoints.

  This requires a redeployment.

4

Perform Oracle Cloud Infrastructure Prerequisites

Before you create an Oracle Managed File Transfer Cloud Service instance in an Oracle Cloud Infrastructure region, you must create the required infrastructure and database resources.

1. Create the following Oracle Cloud Infrastructure resources if they don't already exist:
   - Compartment
   - Virtual cloud network (VCN) and at least one subnet
   - Storage bucket for backups
   - User authentication token (auth token)
   - Policies that allow the Cloud Service to access the resources in your compartment

   See Prerequisites for Oracle Platform Services in the Oracle Cloud Infrastructure documentation.
2. Create a database in Oracle Cloud Infrastructure Database if one doesn't already exist.

   Oracle Managed File Transfer Cloud Service will provision the required infrastructure schema to this database. See Managing Bare Metal and Virtual Machine DB Systems in the Oracle Cloud Infrastructure documentation.

5

Complete the Post-Migration Tasks

After successfully migrating your Oracle Managed File Transfer Cloud Service instances from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure, test your applications thoroughly, and then perform cleanup and other optional configuration tasks

Topics:

Test Your Target Environment

You can test your target environment at this point to check if everything is working as expected after the migration. It is assumed that you have already tested in a stage system (test environment).

To test your target environment:

1. Use endpoints to test in the configuration plans of the steps that you have completed till now.
2. Test and check if everything is working as expected.
3. Switch to production endpoints.

   This may require projects to be redeployed with appropriate configuration plans.

Migrate FastConnect and VPN Connections to Oracle Cloud Infrastructure

Use Oracle Cloud Infrastructure to create a connection between your private, on-premises network and a network in Oracle Cloud.

A Virtual Private Network (VPN) uses a public network to create a secure connection between two private networks. Oracle supports two connectivity solutions for a Virtual Cloud Network (VCN) in Oracle Cloud Infrastructure:

- Oracle Cloud Infrastructure FastConnect - Create dedicated, high-speed, virtual circuits for production systems that communicate with your on-premises network using the Border Gateway Protocol (BGP). This service is equivalent to Oracle Cloud Infrastructure FastConnect Classic.
- IPSec VPN - Create secure connections with your on-premises network using the IPSec protocol. This solution replaces VPN as a Service (VPNaaS) and Corente in Oracle Cloud Infrastructure Classic.

When migrating from Oracle Cloud Infrastructure Classic, update the existing BGP or VPN configuration in your on-premises network to use either Oracle Cloud Infrastructure FastConnect or IPSec VPN. Alternatively, if you require connectivity to instances

in both Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic during the migration process, create a separate BGP or VPN configuration in your on-premises network.

In Oracle Cloud Infrastructure, creating a connection to your on-premises network includes these tasks:

- Create a Dynamic Routing Gateway (DRG) in the VCN.
- Create a route table in the VCN that directs external traffic to the DRG.
- Assign the route table to a subnet in the VCN.

Refer to these topics in the Oracle Cloud Infrastructure documentation:

- FastConnect
- IPSec VPN

Configure Load Balancer

Register your domain name, import a CA- issued SSL certificate, and associate the SSL certificate with the load balancer.

Configure the load balancer as follows:

1. Register your domain name by using verisign.com or register.com.
2. Resolve the domain name to the IP address of the SOA load balancer.
3. Import a CA-issue SSL certificate to the load balancer.
4. Associate the SSL certificate with the load balancer.

Clean Up Resources in Oracle Cloud Infrastructure Classic

After testing your target Oracle Managed File Transfer Cloud Service instance, you can delete the source instance and supporting cloud resources in Oracle Cloud Infrastructure Classic.

Delete these Oracle Cloud Infrastructure Classic resources to avoid costs for services that you no longer use.

1. Access the console and select the MFT Cloud Service instance.
2. Delete the source Oracle Managed File Transfer Cloud Service instances that you created in Oracle Cloud Infrastructure Classic.
    a. Click **Manage this instance** for the service instance, and then select **Delete**.
    b. Enter the **Database Administrator User Name** and **Database Administrator User Password** for the infrastructure schema database.

       Alternatively, select **Force Delete** if you plan to delete this database as well.
    c. Click **Delete**.
3. Click **IP Reservations**.
4. Delete any IP reservations that you created for your source Oracle Managed File Transfer Cloud Service instances.

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

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

5. Access the Oracle Database Cloud Service console (Database Classic).
6. Delete the Oracle Database Cloud Service instances that you created in Oracle Cloud Infrastructure Classic to support your source instances.

   Do not delete a database if it is still in use by other services.

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

   b. When prompted for confirmation, click **Delete**.
7. Click **IP Reservations**.
8. Delete any IP reservations that you created for your Oracle Database Cloud Service instances.

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

   b. When prompted for confirmation, click **OK**.
9. Access the Oracle Cloud Infrastructure Object Storage Classic console (Storage Classic).
10. Delete the object storage containers that you created in Oracle Cloud Infrastructure Classic to support your source instances.

    Do not delete a container if it is still in use by other services.

    a. Click the delete icon  for the container.

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