

Oracle® Cloud

Migrating Oracle SOA Cloud Service Instances to Oracle Cloud Infrastructure



F15009-11
March 2024



Oracle Cloud Migrating Oracle SOA Cloud Service Instances to Oracle Cloud Infrastructure,

F15009-11

Copyright © 2019, 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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>.

Contents

Preface

Audience	v
Documentation Accessibility	v
Related Resources	v
Conventions	v

1 About Migrating to Oracle Cloud Infrastructure

Why Migrate to Oracle Cloud Infrastructure	1-1
About the Migration Scope	1-1
Compare Oracle Cloud Infrastructure to Classic	1-2
About the Migration Task Flow	1-2
About Migrating an Oracle SOA Cloud Service Classic Instance	1-3

2 Prepare to Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure

About Downtime Requirements	2-1
Select Oracle Cloud Infrastructure Shapes	2-1
Design the Oracle Cloud Infrastructure Network	2-2
Create Infrastructure and Database Resources	2-2
Provision a New Target Instance	2-3
Prepare Clients for Migration	2-3

3 Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure Manually

Migrate to Your Target Environment Manually	3-1
Migrate Data Components Manually	3-3
Move LDAP Data	3-3
Move OPSS Data	3-4
Move OWSM Data	3-5
Move ESS Metadata	3-5

Move B2B Metadata	3-5
Move Oracle Service Bus Projects	3-6
Move SOA Projects	3-6

4 Complete the Post-Migration Tasks

Transition from Old Deployment to New Deployment	4-1
Reconfigure Tuning and Configuration Parameters	4-2
Transition Inbound Adapters/Transports	4-3
Test Your Target Environment	4-3
Migrate FastConnect and VPN Connections to Oracle Cloud Infrastructure	4-3
Configure the Load Balancer	4-4
Clean Up Resources in Oracle Cloud Infrastructure Classic	4-4

Preface

Migrating Oracle SOA Cloud Service Instances to Oracle Cloud Infrastructure describes how to migrate an existing Oracle SOA Cloud Service instance from an Oracle Cloud Infrastructure Classic region to an Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service instance in an Oracle Cloud Infrastructure region.

Topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Resources](#)
- [Conventions](#)

Audience

Migrating Oracle SOA Cloud Service Instances to Oracle Cloud Infrastructure is intended for users who need to migrate existing Oracle SOA 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 SOA 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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Videos and Images

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

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

1

About Migrating to Oracle Cloud Infrastructure

Learn about the benefits of migrating your existing Oracle SOA Cloud Service Classic instances to Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service instances in Oracle Cloud Infrastructure, and get an overview of the migration process and tools.

Topics:

- [Why Migrate to Oracle Cloud Infrastructure](#)
- [About the Migration Scope](#)
- [Compare Oracle Cloud Infrastructure to Classic](#)
- [About the Migration Task Flow](#)
- [About Migrating an Oracle SOA Cloud Service Classic Instance](#)

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:

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

To learn more, see [Upgrade Your Classic Services to Oracle Cloud Infrastructure](#).

About the Migration Scope

Before you migrate your existing Oracle SOA Cloud Service Classic instances to Oracle Cloud Infrastructure, ensure that the instance meets the prerequisites for the migration.

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 new WebLogic Server domain. Instead, this guide provides references to the Oracle Cloud Infrastructure documentation as appropriate.

This guide also does not include steps for migrating SOA schemas from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. One option is the Oracle Cloud

Infrastructure Classic Database Backup Migration Tool, which uses Recovery Manager (RMAN). Another option is Oracle Data Guard. See [Select a Method to Migrate Database Instances](#) in *Migrating Infrastructure Classic Workloads to Oracle Cloud Infrastructure*.

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 CoreNet 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 SOA Cloud Service Classic instances to Oracle Cloud Infrastructure.

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

Step	Refer to
Plan and prepare for the migration and perform any prerequisite tasks in Oracle Cloud Infrastructure, which include creating resources, preparing clients and the target environment, and provisioning a target instance.	Prepare to Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure
Migrate the Oracle SOA Cloud Service Classic instance to Oracle Cloud Infrastructure.	Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure Manually
Perform post-migration tasks, including testing your applications on the target instance.	Complete the Post-Migration Tasks

About Migrating an Oracle SOA Cloud Service Classic Instance

Migrating an Oracle SOA Cloud Service Classic instance to Oracle Cloud Infrastructure includes provisioning a new Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service instance, migrating or re-creating configurations from the old source environment, and then transitioning to the newly provisioned instance.



Note:

If you want to upgrade an instance from one version to another in Oracle Cloud Infrastructure, or from an older to a newer instance in the same version, you can perform a side-by-side upgrade by following the manual migration steps in [Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure Manually](#).

Keep the following details in mind for migrating an Oracle SOA Cloud Service Classic instance to Oracle SOA Suite on Marketplace instance versus an Oracle SOA Cloud Service target on Oracle Cloud Infrastructure:

Oracle SOA Suite on Marketplace Target	Oracle SOA Cloud Service Target
To migrate an Oracle SOA Cloud Service Classic instance to Oracle SOA Suite on Marketplace on Oracle Cloud Infrastructure: <ul style="list-style-type: none"> using manual steps, the source Oracle SOA Cloud Service instance version must be 12.1.3 or later. 	To migrate an Oracle SOA Cloud Service Classic instance to Oracle SOA Cloud Service on Oracle Cloud Infrastructure: <ul style="list-style-type: none"> using manual steps, the source Oracle SOA Cloud Service instance version must be 12.1.3 or later.
The target Oracle SOA Suite on Marketplace instance is 12.2.1.4, which is the only version for Oracle SOA Suite on Marketplace.	<ul style="list-style-type: none"> When using manual steps, the target Oracle SOA Cloud Service instance can be 12.2.1.4 or earlier.
Oracle SOA Cloud Service uses internal Lightweight Directory Access Protocol (LDAP).	Oracle SOA Cloud Service uses internal Lightweight Directory Access Protocol (LDAP).
Oracle SOA Suite on Marketplace uses the Oracle Cloud Infrastructure load balancer in both private and public subnets. The load balancer can be configured during provisioning or post-provisioning.	Oracle SOA Cloud Service uses Oracle Traffic Director (OTD) as a load balancer. On Oracle Cloud Infrastructure, also supports the Oracle Cloud Infrastructure load balancer, which must be configured manually post-provisioning.
Oracle SOA Suite on Marketplace uses Keystore Services (KSS).	Oracle SOA Cloud Service uses Keystore Services (KSS).

Oracle SOA Suite on Marketplace Target	Oracle SOA Cloud Service Target
You can directly copy and import security information between the source and the target Oracle SOA Suite on Marketplace instances.	You can directly copy and import security information between the source and the target Oracle SOA Cloud Service instances.
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 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.

2

Prepare to Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure

Before you migrate an Oracle SOA Cloud Service Classic instance 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 instances.

Topics:

- [About Downtime Requirements](#)
- [Select Oracle Cloud Infrastructure Shapes](#)
- [Design the Oracle Cloud Infrastructure Network](#)
- [Create Infrastructure and Database Resources](#)
- [Provision a New Target Instance](#)
- [Prepare Clients for Migration](#)

About Downtime Requirements

The migration process does not affect the availability of your existing Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure Classic. The 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.

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.

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.

Create Infrastructure and Database Resources

Before you migrate an Oracle SOA Cloud Service Classic instance to 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:

Resources for Oracle SOA Suite on Marketplace	Resources for Oracle SOA Cloud Service
<ul style="list-style-type: none"> • A compartment • A virtual cloud network (VCN) and at least one subnet 	<ul style="list-style-type: none"> • A compartment • A virtual cloud network (VCN) and at least one subnet • A storage bucket for backups • A user authentication token (auth token) • Policies that allow Oracle SOA Cloud Service to access the resources in your compartment

2. Create a database in Oracle Cloud Infrastructure if one doesn't already exist.

Oracle SOA Cloud Service will provision the required infrastructure schema to this database.

For information about creating these resources, see:

- For an Oracle SOA Suite on Marketplace target environment: Prerequisites in Oracle SOA Suite on Marketplace.
- For an Oracle SOA Cloud Service target environment: Prerequisites for Oracle Cloud Infrastructure in *Administering Oracle SOA Cloud Service*.

Provision a New Target Instance

Provision a new Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service instance before starting the other migration tasks. You'll migrate or re-create configurations from your old source environment into the newly provisioned instance.

Create a simple hello world application (SOA composite/OSB proxy service/B2B agreement) and test to check that it works.

See:

- Provision an Oracle SOA Suite on Marketplace Instance in *Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure*.
- Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure of *Administering Oracle SOA Cloud Service*.

Prepare Clients for Migration

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 Domain Name System (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.

2. Create a new port in the source environment load balancer that matches the target port number. Add routing rule to this new port to route to the original load balancer port in the source environment.
3. Change all clients to use the DNS name and new port.

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.

4. If you were already set up to use a global DNS name, ensure that the Oracle WebLogic Server front end host points to the load balancer and not the DNS name.

Ensure that the loopback HTTP invokes point to the Oracle WebLogic Server front end host/port. For SOA, also ensure that the loopback abstract WSDL/Schema references point to the WebLogic FE host/port.

These changes ensure that:

- Callbacks come back to the source domain that issued the request, after transitioning to the target.
- Loopbacks in the source domain come back to the source domain after transitioning to the target.

3

Migrate an Oracle SOA Cloud Service Classic Instance to Oracle Cloud Infrastructure Manually

After you have completed the [migration preparation steps](#), you can migrate an Oracle SOA Cloud Service Classic instance to Oracle Cloud Infrastructure.

Use the steps in this chapter in the following circumstances:

- You want to upgrade an instance from one version to another in Oracle Cloud Infrastructure (side-by-side upgrade).
- You want to upgrade from an older to a newer instance in the same version (side-by-side upgrade).

Topics:

- [Migrate to Your Target Environment Manually](#)
- [Migrate Data Components Manually](#)

Migrate to Your Target Environment Manually

After you have completed the [migration preparation steps](#), you can migrate to your target environment by manually importing or re-creating all the configurations of your source. This will ensure successful deployment of the target instance.

To migrate to your target environment:

1. Create the required WLS artifacts.

WLS artifacts can be: Java Message Service (JMS) queue, Java EE Connector Architecture (JCA) adapter configurations, data source, work managers, J2EE app deployment, JMS servers, JMS topics, and so on.

2. 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, role memberships, enterprise roles, OPSS credentials, and so on.

For more information about:

- OPSS commands to migrate keystores, see [Managing Keystores with WLST](#) in *Securing Applications with Oracle Platform Security Services*.
- OPSS commands to migrate credentials, see [Managing Credentials with WLST](#) in *Securing Applications with Oracle Platform Security Services*.
- OWSM commands to migrate custom policies, see [Migrating Policies](#) in *Administering Web Services*.

 **Note:**

The source Oracle SOA Cloud Service internal LDAP data can be migrated into the target Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service instance.

3. Test that your security configurations work.
 - a. Create a simple application comprising of SOA composite, Oracle Service Bus proxy service, B2B agreement, ESS job.
 - b. Ensure that the application uses at least one of the keys/certificates/credentials.
 - c. Test to check if the application works.
 - d. Check if you can view an imported user in LDAP.
4. Import shared artifacts in MetaData Services (MDS) schemas for SOA.
5. Deploy projects from the console for SOA/Oracle Service Bus.

Use the prepared customization file/configuration plan. Ensure loopback abstract WSDL/Schema references and loopback HTTP invokes point to the target environment load balancer and not the DNS name.

For inbound adapters, if the address for both deployments is the same, ensure that it doesn't start processing production messages by externally blocking it from accessing inbound endpoints. Then, if possible, you can deactivate the SOA adapter.
6. Import artifacts for B2B.

The inbound channels are disabled by default. If required, add URLs in the console for the cloud and deploy all artifacts.
7. Import `/oracle/apps/ess/custom namespace` and `/oracle/as/ess/essapp/custom namespace` for Oracle Enterprise Scheduler.
8. Enter the token values noted earlier for Oracle Enterprise Scheduler.
9. Rebind work assignments to the cluster or managed server for Oracle Enterprise Scheduler.

See [Managing Work Assignments and Workshifts in Administering Oracle Enterprise Scheduler](#).
10. Add file system artifacts captured from the source environment, such as custom XPath functions, SOA token mapping file, B2B java callouts.
11. Test the endpoints.

Use the endpoints in the application (SOA composite, OSB proxy service, B2B agreement, ESS job) created for testing and check if it works. After testing, change it back to the original endpoints.
12. Add scripts scheduled with Oracle Enterprise Scheduler.
13. Set your tuning settings if they are available.
14. If the FTP adapter is used, move the contents of the `privateKeyFile` source location to the same location on the target.

15. If the MQ adapter is used, move the contents of the `KeyStoreLocation` and `TrustStoreLocation` source locations to the same locations on the target.
16. Redo all the SOA Composer customizations manually.
17. Redo any Enterprise Manager configuration steps manually.
For details, see [Reconfigure Tuning and Configuration Parameters](#).
18. If the target instance is going to access endpoints on-premises then you may need VPN.
You can set up VPN through VPNaaS.
19. Apply UMS configuration manually to the target environment.
20. Deploy other supported third-party resource adapters (for example, OracleApps Adapter, SAP Adapter) that are being used in the Oracle WebLogic Server Administration Console to both the Administration Server and the Managed Servers.

Migrate Data Components Manually

Migrate your data components such as LDAP, OPSS, OWSM, ESS, B2B, Oracle Service Bus, and SOA from the source to the target environment.

Topics:

Migrate your data components from the source to the target environment in the following order:

1. [Move LDAP Data](#)
2. [Move OPSS Data](#)
3. [Move OWSM Data](#)
4. Migrate the remaining data in any order:
 - [Move ESS Metadata](#)
 - [Move B2B Metadata](#)
 - [Move Oracle Service Bus Projects](#)
 - [Move SOA Projects](#)

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.

Keep in mind that SOA Cloud Service uses internal LDAP.

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.

Move OPSS Data

Move OPSS data by exporting from the source, and 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 overlaid 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 overlaid 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 WSLT](#) in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

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

The `exportWSMRepository` command exports all custom policies from the repository, the trust configuration, OAuth configuration, and any other configuration documents.

Move ESS Metadata

Since we need to export tip versions of metadata in MDS in a specific package, we can use the `exportMetadata WLST` command with `docs` parameter as `"/oracle/apps/ess/custom/**"` and `"/oracle/as/ess/essapp/custom/**"` to an archive. Then we can import from the archive to the target MDS repository using the `importMetadata WLST` command.

To ensure the metadata is independent of environment, we need to tokenize URLs in job definitions first. Users have to define the new token values in the target environment (if required).

For MDS `importMetadata` and `exportMetadata` commands, see [exportMetadata](#) and [importMetadata](#) in *WLST Command Reference for Infrastructure Components*.

Move B2B Metadata

Move B2B metadata from your source to your target environment.

For detail instructions, see [Importing and Exporting Data](#) in *Using Oracle B2B*.

Move Oracle Service Bus Projects

The easiest way to export and import Oracle Service Bus metadata is through the console. You can export all the projects with one export.

See [How to Export Resources to a Configuration JAR File in the Console](#) in *Developing Services with Oracle Service Bus*.

Move SOA Projects

The SOA composite SAR archive can be generated easily in JDeveloper by generating a SAR archive (instead of deploying to the server). This can be deployed to the target Oracle SOA Suite on Marketplace or Oracle SOA Cloud Service server from the console, ant script, or WLST script.

See [Deploying SOA Composite Applications or Projects in Oracle JDeveloper](#) in *Developing SOA Applications with Oracle SOA Suite*.

4

Complete the Post-Migration Tasks

After successfully migrating your Oracle SOA Cloud Service Classic instances to Oracle Cloud Infrastructure, test your applications thoroughly, and then perform cleanup and other optional configuration tasks.

Topics:

- [Transition from Old Deployment to New Deployment](#)
- [Reconfigure Tuning and Configuration Parameters](#)
- [Transition Inbound Adapters/Transports](#)
- [Test Your Target Environment](#)
- [Migrate FastConnect and VPN Connections to Oracle Cloud Infrastructure](#)
- [Configure the Load Balancer](#)
- [Clean Up Resources in Oracle Cloud Infrastructure Classic](#)

Transition from Old Deployment to New Deployment

After migration, you can transition your production system from old deployment to new deployment. You can do this by transitioning: HTTP Clients, inbound adapters where the address is the same for old and new, clients of inbound adapters where the address is different for old and new, and clients who are reading from the old environment (such as a JMS queue) but now need to read from the target environment.

Note that the transition from old to new deployment will not work if the following are used:

- BPEL correlation sets or message ordering.
- Mid-process receives from clients in BPEL.
- If SOA composites have human workflow elements.

To transition from old to new deployment:

1. Deactivate the inbound composite/adaptor/channel/transport in the old deployment if the inbound address in both old and new deployment is same.

For FTP inbound, delete any processed file left behind after processing.

2. 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.

3. Enable inbound composite/adaptor/channel/transport in the target environment system.

For some inbound adapters like WLS Java Messaging Service (JMS), the address is different and clients have to change the address and switch.

4. Terminate all ESS jobs in the source environment and schedule them in the target environment.

5. Ensure that callback and loopback invokes in SOA must come to the domain that initiated it. So the old deployment continues processing callbacks/loopbacks while new requests are processed by the new deployment.

When all callbacks/loopbacks are processed and all backlog messages are processed and there is no need for a rollback, then you can destroy the old deployment. External clients who read from, for example, local weblogic JMS queues in the source deployment will switch to the target deployment after all messages are processed.

Reconfigure Tuning and Configuration Parameters

Reconfigure any Enterprise Manager tuning and configuration parameters that you had previously set in the source environment or you need to change in the target environment.

SOA

- Lazy loading
- Modularity profile
- Autopurge
- Timeouts (transaction, Enterprise JavaBeans, HTTP)
- Work managers
- SOA data source connection pool
- Resiliency
- In-memory
- EDN
- Instance tracking

ESS

- Dispatcher
- Processor thread pool
- Attach ESS web service OWSM policy
- Scheduled purge

Oracle Service Bus

- Results cache
- Work managers

B2B

Refer to the following topics in *Using Oracle B2B*:

- For information about Enterprise Manager Parameters, see [Setting B2B Configuration Properties in Fusion Middleware Control](#).
- For information about B2B interface parameters, see [Configuring B2B System Parameters](#).

Transition Inbound Adapters/Transports

For successful migration, 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.

Oracle SOA Cloud Service supports adapter activate/deactivate only in 12.1.3. In B2B, the inbound channel is disabled by default on import. Oracle Service Bus does not support this.

- Change the inbound endpoints to test or true endpoints.

This requires a redeployment.

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.

Note:

This topic is not applicable, if you are migrating Oracle Java Cloud Service on Oracle Cloud Infrastructure to Oracle WebLogic Server for Oracle Cloud Infrastructure. As the instance can be created in the existing VCN, where FastConnect or IPSec is already configured.

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 CoreNet 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 the 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 using [verisign.com](https://www.verisign.com) or [register.com](https://www.register.com).
2. Resolve the domain name to the IP address of the SOA load balancer.
3. Import a CA-issued 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 instance, you can delete the source Oracle SOA Cloud Service instance and supporting cloud resources in Oracle Cloud Infrastructure Classic.

To delete Oracle Cloud Infrastructure Classic resources to avoid costs for services that you no longer use:

1. Access the Oracle SOA Cloud Service console.

2. Delete the source Oracle SOA 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 SOA Cloud Service instances.
 - a. Click **Delete**  for the IP reservation.
 - b. When prompted for confirmation, click **OK**.
5. Access the Oracle Database Classic Cloud Service console (Database Classic).
6. Delete the Oracle Database Classic Cloud Service instances that you created in Oracle Cloud Infrastructure Classic to support your source Oracle SOA Cloud Service 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 Classic 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 Oracle SOA Cloud Service 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**.