Contents

Preface

Audience v
Documentation Accessibility v
Related Resources v
Conventions v

1 Learn About Migrating to Oracle Cloud Infrastructure

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

2 Prepare to Migrate Oracle SOA Cloud Service to Oracle Cloud Infrastructure

About Downtime Requirements 2-1
Select Oracle Cloud Infrastructure Shapes 2-1
Design the Oracle Cloud Infrastructure Network 2-2

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

Create Infrastructure Resources 3-1
Provision Oracle SOA Cloud Service 3-2
Prepare Clients for Migration 3-2
Prepare Your Source for Migration 3-3
Prepare Your Target Environment 3-4
Transition from Old Deployment to New Deployment 3-5
Re-configure Configuration Parameters and Tune in Oracle SOA Cloud Service 3-6
Migrate Data Components 3-7
  Move LDAP Data 3-7
4 Complete the Post-Migration Tasks

Test Your Target Environment 4-1
Migrate FastConnect and VPN Connections to Oracle Cloud Infrastructure 4-1
Configure Load Balancer 4-2
Clean Up Resources in Oracle Cloud Infrastructure Classic 4-2

A Migrate Oracle SOA Cloud Service with the Oracle SOA Cloud Service Migration Plug-in

Oracle SOA Cloud Service Migration Plug-in Overview A-1
Restrictions and Prerequisites A-2
Set Up Your Source Profile A-3
Set Up Your Target Configuration File A-5
Migrate Oracle SOA Cloud Service A-6
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 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.

**Conventions**

The following text conventions are used in this document:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Learn About Migrating to Oracle Cloud Infrastructure

Learn about the benefits to migrating your existing Oracle SOA Cloud Service instances to 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

Why Migrate to Oracle Cloud Infrastructure

Oracle encourages you to migrate your existing cloud resources from Oracle Cloud Infrastructure Classic 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.

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 of SOA 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 SOA Cloud Service

For the migration of Oracle SOA Cloud Service to Oracle Cloud Infrastructure, you’ll provision a new cloud instance of Oracle SOA 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 SOA instance that you want to migrate can be 12.1.3 or later.

• SOA Cloud Service uses internal LDAP.

• SOA Cloud Service uses Oracle Traffic Director (OTD).


• You can directly copy and import security information between the source and the target SOA Cloud Service instances.

• The target version of the cloud SOA instance that you’ll migrate to is 12.2.1.3.

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 the Migration Task Flow

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

Note:

As an alternative to performing the procedures described in this guide, you can use Rubicon Red’s MyST platform to migrate Oracle SOA Cloud Service instances on Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. Contact Rubicon Red for information about their free trial promotion. Use of MyST after the trial period completes would require payment directly to Rubicon Red.

https://myst.cloud/oracle

The following diagram shows the migration topology for a typical Oracle SOA Cloud Service instance.

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 SOA 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 SOA Cloud Service instance.

5. Use the Oracle WebLogic Server Deploy Tooling to update the domain configuration on your target Oracle SOA Cloud Service instance and to deploy your applications.

6. Test your applications on the target instance, and perform any other post-migration tasks.
Prepare to Migrate Oracle SOA 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
• Select Oracle Cloud Infrastructure Shapes
• Design the Oracle Cloud Infrastructure Network

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.
Migrate an Oracle SOA Cloud Service Instance to Oracle Cloud Infrastructure

Create a new Oracle SOA 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
- Provision Oracle SOA Cloud Service
- Prepare Clients for Migration
- Prepare Your Source for Migration
- Prepare Your Target Environment
- Transition from Old Deployment to New Deployment
- Re-configure Configuration Parameters and Tune in Oracle SOA Cloud Service
- Migrate Data Components
- Transition Inbound Adapters/Transports

Note:
You can also use the opc migrate tool to migrate Oracle SOA Cloud Service instances to Oracle Cloud Infrastructure. See Migrate Oracle SOA Cloud Service with the Oracle SOA Cloud Service Migration Plug-in.

Create Infrastructure Resources

Before you create an Oracle SOA 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:
   - 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
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 SOA Cloud Service will provision the required infrastructure schema to this database. See Create an Oracle Cloud Infrastructure Native Database for Use with Oracle SOA Cloud Service in Administering Oracle SOA Cloud Service in a Customer-Managed Environment.

Provision Oracle SOA Cloud Service

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

See Provision Oracle SOA Cloud Service Instances in Oracle Cloud Infrastructure of Administering Oracle SOA Cloud Service in a Customer-Managed Environment.

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

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 Oracle SOA Cloud Service port number. Add routing rule to this new port to route to the original load balancer port in the source environment.

   Note that on-premises SOA applications can use a different port number than the target Oracle SOA 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.

   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.

**Prepare Your Source for Migration**

You have to migrate the Integrated Development Environment (IDE) projects and export or capture needed artifacts from the source environment to prepare your source for migration.

To prepare your source:

1. Migrate IDE projects to the 12c IDE that matches the Oracle SOA Cloud Service version for SOA/Oracle Service Bus (OSB).

2. Export metadata from the source environment for B2B/OSB, where the IDE is not used.

3. Grab the domain file system artifacts such as custom XPath functions, B2B java callouts, SOA token mapping file and any script scheduled with Oracle Enterprise Scheduler (ESS) for OSB/SOA.

4. Ensure that there are no hard-coded URLs in the job definitions for Oracle Enterprise Scheduler. Use tokens instead.
   - See Using Token Substitution in *Developing Applications for Oracle Enterprise Scheduler*.

5. Export the shared artifacts which are stored in MetaData Services (MDS) schemas in the source environment by using the offline WLST command:
   
   ```
   sca_exportSharedData(serverURL, JARfile, pattern, [user], [password]).
   ```

6. Export `/oracle/apps/ess/custom namespace in the ESS partition:`
   essUserMetadata for Oracle Enterprise Scheduler. Do this export using MDS export in the application essnativehostingapp in MDS.

7. Export `/oracle/as/ess/essapp/custom namespace in the ESS partition: essapp-internal-partition for Oracle Enterprise Scheduler. Do this export using MDS export in the application ESSAPP in MDS.

8. Note the token values in URLs for Oracle Enterprise Scheduler. You will need this later.
   - Note the token values to be used for cloud, if different.

9. For SOA, if there are references to Schemas and abstract WSDLs that are different in the cloud, change the source environment for composites or capture it in the configuration plan.
10. For OSB/SOA, adjust the customization files/configuration plans for deployment to the target SOA Cloud Service. Change URLs to values appropriate for SOA Cloud Service.

11. Use the t3 syntax cluster:t3://<clusternam e> for local loopback t3 references in configurations.

Some products like Oracle Service Bus do not support this syntax. For loopback WebLogic JMS URL, use jms://connection_factory/.....

Prepare Your Target Environment

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

To prepare your target environment:

1. Create the required WLS artifacts.

WLS artefacts 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 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.

3. Test that your security configurations work.

   • Create a simple application comprising of SOA composite, OSB proxy service, B2B agreement, ESS job.
   
   • Ensure that the application uses at least one of the keys/certificates/credentials.
   
   • Test to check if the application works.
• 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/cust
   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. Redo all the SOA Composer customizations manually.

15. Redo any Enterprise Manager configuration steps manually.
    For details, see Re-configure Configuration Parameters and Tune in Oracle SOA
    Cloud Service.

16. If Oracle SOA Cloud Service is going to access endpoints on-premises then you
    may need VPN.
    You can setup VPN through VPNaaS.

17. Apply UMS configuration manually to the target environment.

Transition from Old Deployment to New Deployment

After you have prepared your source and target environments for the migration, you
can transition your production system from old deployment to new deployment. You
can do this by transitioning: HTTP Clients, inbound adapters where address is the
same for old and new, clients of inbound adapters where 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. De-activate the inbound composite/adapter/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/adapter/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.

Re-configure Configuration Parameters and Tune in Oracle SOA Cloud Service

Re-configure 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.

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

**OSB**
• Results cache
• Work managers

**B2B**

## Migrate Data Components

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

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

Migrate your data components in the following order:

1. Migrate LDAP Data
2. Migrate OPSS Data
3. Migrate OWSM Data
4. Migrate the remaining data (ESS, B2B, OSB and SOA) in any order.

## 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:


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 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 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 *User’s Guide for Oracle B2B*.

**Move OSB Projects**

The easiest way to export and import 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 12.2.1.3 by generating a SAR archive (instead of deploying to the server). This can be deployed to the target SOA Cloud Service 12.2.1.3 server from the console, ant script or WLST script.

See Deploying SOA Composite Application in Oracle JDeveloper in *Developing SOA Applications with Oracle SOA Suite*.

**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.

  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.
Complete the Post-Migration Tasks

After successfully migrating your Oracle SOA 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
• Migrate FastConnect and VPN Connections to Oracle Cloud Infrastructure
• Configure Load Balancer
• Clean Up Resources in Oracle Cloud Infrastructure Classic

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 SOA 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 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 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 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 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.
Migrate Oracle SOA Cloud Service with the Oracle SOA Cloud Service Migration Plug-in

As an alternative to the migration steps discussed in the previous sections of this guide, you can use the Oracle SOA Cloud Service Migration Plug-in (opcmigrate) to migrate Oracle SOA Cloud Service instances to Oracle Cloud Infrastructure.

Topics:

• Oracle SOA Cloud Service Migration Plug-in Overview
• Restrictions and Prerequisites
• Set Up Your Source Profile
• Set Up Your Target Configuration File
• Migrate Oracle SOA Cloud Service

Oracle SOA Cloud Service Migration Plug-in Overview

Migrating an Oracle SOA Cloud Service instance from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure is a multistep process. You must complete several prerequisites prior to starting Oracle SOA Cloud Service migration. The Oracle SOA Cloud Service Migration Plug-in (opcmigrate) does the following:

1. Uses the existing Oracle Cloud Infrastructure Classic discovery mechanism to identify the Oracle SOA Cloud Service instances to migrate.
2. Automates the creation of the target Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure.
3. Automates the creation of the migration archive from the source Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure Classic for the following components:
   a. Oracle BPEL Process Manager
   b. Oracle B2B
   c. Oracle Service Bus
   d. Oracle Enterprise Scheduler
   e. LDAP
   f. Oracle WebLogic Server data source, JNDI, and JMS configurations
4. Automates the process to transfer the artifacts archive to the target Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure and automates the required modifications to the domain metadata used.
Migration is performed as a plug-in to the Oracle Cloud Infrastructure Classic migration tooling command line interface (CLI), and included in the product available to you.

**Oracle SOA Cloud Service Migration Commands**

The Oracle SOA Cloud Service Migration Plug-in is implemented as part of the existing `opcmigrate` CLI tool that you already use to perform network, storage, virtual machine (VM), and database migrations from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. Using the existing discovery functionality of `opcmigrate`, the plug-in facilitates migration of discovered Oracle SOA Cloud Service instances in Oracle Cloud Infrastructure Classic using a set of subcommands within the existing `opcmigrate migrate` command of the migration CLI. Following a defined order, you run each subcommand to move the Oracle SOA Cloud Service instance from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure. The following subcommands are implemented:

- `opcmigrate migrate soacs list`: Lists the Oracle SOA Cloud Service instances discovered in Oracle Cloud Infrastructure Classic that can be migrated.
- `opcmigrate migrate soacs export`: Takes additional command line arguments from you to specify the Oracle Cloud Infrastructure Classic-based Oracle SOA Cloud Service instance to export, create an archive from the source Oracle SOA Cloud Service, and persist it in a storage container in your Oracle Cloud Infrastructure tenancy.
- `opcmigrate migrate soacs create`: Takes additional command line arguments from you to generate the Terraform required to create the target Oracle SOA Cloud Service instance in your Oracle Cloud Infrastructure tenancy.
- `opcmigrate migrate soacs import`: Takes additional command line arguments from you to hydrate the target Oracle SOA Cloud Service instance with the exported resources from the specific source Oracle SOA Cloud Service service and modify the target configuration based on the customer-created configuration.

In addition to the migration commands above, a further command group is provided to manage the archives within the migration storage container. This enables you to list, download, and delete previously-created archives using the same interface as the migration uses.

- `opcmigrate migrate soacs archive list`: Lists the available exported archives that are found in the storage container.
- `opcmigrate migrate soacs archive get`: Takes additional command line arguments to fetch the requested archive from the storage container and save it locally.
- `opcmigrate migrate soacs archive delete`: Takes additional command line arguments from you to delete the requested archive from the storage container.

**Restrictions and Prerequisites**

Note the following restrictions and prerequisites for the Oracle SOA Cloud Service migration plug-in.

- Oracle SOA Cloud Service database migrations are not performed. You must migrate your Oracle Cloud Infrastructure Classic-based application databases prior to migrating Oracle SOA Cloud Service and must also ensure that an Oracle Cloud Infrastructure-based database is available for the target Oracle
SOA Cloud Service to use for the specific schema created by the Repository Creation Utility (RCU).

- Custom load balancer configurations or custom Oracle Identity Cloud Service applications, roles, and role membership are not migrated. If you have custom load balancer configurations and/or Oracle Identity Cloud Service entities that must be migrated, perform these steps using the existing documentation either pre- or post-migration.

**Note:**

For additional information about preparing for migration, see Prepare to Migrate Oracle SOA Cloud Service to Oracle Cloud Infrastructure.

## Set Up Your Source Profile

The opc migrate tool connects to your Oracle Integration source environment using connection information that you provide in a profile file.

The information you provide in the profile file includes the user name or identity for each service in the source environment and the service endpoint and region. If you want to run the tool in multiple regions or tenancies, you can create separate profile files for each region and tenancy.

1. You need the user name and API end point for each service. Look up service-specific details in your Oracle Cloud Dashboard.

2. Create the directory for the profile file, if the directory does not already exist. By default, profile files are created in the directory ~/.opc/profiles. If you create profiles in a location other than ~/.opc/profiles, provide the full path to the profile location by using the --profile-directory option when you run the tool.

3. Use the following template to create your profile file.

4. Save this profile with the file name default in the path ~/.opc/profiles.

5. Replace the sample values with values specific to each service.
Note:

If you use the opc migrate tool on an instance:

- The profiles directory and a default profile may already exist. However, the default profile may contain only the "compute" section.

Modify the profile or create a new profile, as required.

- paas: Specify the PaaS user name and identity domain, endpoint, and region.
- compute: Provide the endpoint of the compute resources to discover the password file and user name.
- soa: Specify the source instances to migrate, the SSH private and public keys, the admin user name and password, and SOA profile. For this example, two instances (MigTest1 and soa2instance) are specified.

```
{
    "global": {
        "format": "text",
        "debug-request": true
    },
    "compute": {
        "user": "/Compute-example/firstname.lastname@example.com",
        "endpoint": "compute.uscom-central-1.oraclecloud.com"
    },
    "paas": {
        "user": "firstname.lastname@example.com",
        "identity_id": "orcdev0000",
        "endpoint": "psm.us.oraclecloud.com",
        "region": "uscom-central-1"
    },
    "soacs": {
        "MigTest1": {
            "ssh_private_key": "path_to_SSH_privateKey",
            "admin_username": "weblogic",
            "admin_password": "password"
        },
        "soa2instance": {
            "ssh_private_key": "path_to_SSH_privateKey",
            "admin_username": "weblogic",
            "admin_password": "password",
            "soa_profile": "/Users/mynasname/.opc/profiles/soa.profile"
        }
    }
}
```
The content for the soa.profile referenced above is as follows:

```json
{
    "identityDomain": "idcs-00000000000000000000000000000000",
    "ociUsername": "firstname.lastname@example.com",
    "subnet": "ocid1.subnet.oc1.iad.0000000000000000000000000000000000000000000000000000000",
    "cloudStorageUser": "oracleidentitycloudservice/firstname.lastname@example.com",
    "subscriptionId": "71877111",
    "cloudStorageContainer": "ocicmigration/soatestbucket",
    "region": "us-ashburn-1",
    "connectString": "//host_name:port/PDB1....",
    "meteringFrequency": "HOURLY",
    "serviceName": "createtest11",
    "pdbServiceName": "PDB1",
    "adminPassword": "password",
    "dbaPassword": "password",
    "dbaUsername": "SYS",
    "isRacDb": "false",
    "enableNotification": "true",
    "notificationEmail": "firstname.lastname@example.com",
    "availabilityDomain": "HeYD:US-ASHBURN-AD-1"
}
```

Passwords are not specified in the profile file for security reasons. You are prompted to provide the password for each service when you run the tool.

6. If you create multiple profiles in the ~/.opc/profiles directory, use the --profile option to specify the profile you want to use when you run the tool. If no profile is specified, the default profile is used.

**Set Up Your Target Configuration File**

You must create an Oracle Integration target configuration file. The file can be any name and go in the same ~/.opc/profiles directory as the profile file or a different directory. This file defines the details to create a new Oracle Integration instance with the opcmigrate tool.

The target configuration file (import_config.json) contains the source instance name and the custom resources.

```json
SourceSOACSServiceName       "MigTest1"
TargetSOACSSAdminIPAddress    "IP_Address"
TargetSOACSSSSHPrivateKey     "path_to_SSH_privateKey"
WeblogicAdminUser            "weblogic"
WeblogicAdminPassword        "password"
resources
   JDBCSystemResources
      CustomDataSource
         password      "password"
         name         "CustomDataSource"
         url          "jdbc:oracle:thin:@//IP_Address/PDB1....."
```
Migrate Oracle SOA Cloud Service

You can migrate Oracle SOA Cloud Service instances to Oracle Cloud Infrastructure.

Note:
Oracle Managed File Transfer Cloud Service cannot currently be migrated.

- Learn About Available Commands
- Discover and List Instances
- Export the Instance
- Provision an Oracle SOA Cloud Service Instance
- Import the Instance

Learn About Available Commands

In addition to the `opcmigrate` commands described in Oracle SOA Cloud Service Migration Plug-in Overview, other commands are available for obtaining help.

1. Enter the following command to return a list of all available commands and general options.

   opcmigrate --help

2. Enter the following command to return a list of cloud services that can be migrated with this tool (including Oracle SOA Cloud Service).

   opcmigrate migrate --help

The following output is returned.

   {rsm, oic, soacs, jcs, instance, database}
3. Enter the following command to return a list of options specific to migrating Oracle SOA Cloud Service.

```bash
opcmigrate migrate soacs --help
```

The following output is returned.

```
Oracle SOA Classic (SOACS) Migration Commands:
{list,create,archive,export,import}
```

- `list`: List Oracle SOA Cloud Service Classic resources available for export.
- `create`: Provision Oracle SOA Service Instance in OCI.
- `archive`: Manage SOA Cloud Service resource archives in OCI Object Storage.
- `export`: Export a SOACS archive.
- `import`: Import SOACS resources from an archive in OCI Object Storage to an OCI target environment.

4. Enter the following commands to return a list of options specific to each command you specify during the migration process. For example:

```bash
opcmigrate migrate soacs create -h
```

```bash
opcmigrate migrate soacs import -h
```

5. Enter the following command to identify the version of the tool.

```bash
opcmigrate --version
```

**Discover and List Instances**

---

**Note:**

Ensure that you complete configuration of the source profile and target configuration file before beginning the migration process. See Set Up Your Source Profile and Set Up Your Target Configuration File.

---

The first step is to discover the Oracle SOA Cloud Service instances available for migration.

1. Discover the Oracle SOA Cloud Service instance resources.

```bash
opcmigrate discover
```

The following output is returned.

```
2019-07-15T15:25:30 INFO Authenticating with OCI
```
2019-07-15T15:25:30 INFO Discovering resources for "620659788".

2019-07-15T15:25:51 INFO Storing discovered resources to 'resource-default.json'

2. List the Oracle SOA Cloud Service Classic discovered instances and their states when the instances were discovered (this may differ from their current states).

opcmigrate migrate soacs list

The following Oracle SOA Cloud Service instances available in Oracle Cloud Infrastructure Classic are returned.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MigTest1</td>
<td>12cRelease213</td>
<td>READY</td>
<td></td>
</tr>
<tr>
<td>SOAMigrationTest</td>
<td>12cRelease213</td>
<td>READY</td>
<td></td>
</tr>
<tr>
<td>soa2instance</td>
<td>12cRelease213</td>
<td>READY</td>
<td></td>
</tr>
</tbody>
</table>

This matches with the instances shown in the My Services Console.

Export the Instance

The export command takes the source Oracle Cloud Infrastructure Classic Oracle SOA Cloud Service instance to export as an argument. This is the only command needed to generate the required Oracle SOA Cloud Service-specific artifacts used in migration to Oracle Cloud Infrastructure. The result of this command is a gzipped-TAR file archive that is persisted in the storage container and a JSON configuration template file. You must edit the template file to add the secrets used when rehydrating the target Oracle SOA Cloud Service in Oracle Cloud Infrastructure and optionally to redefine JDBC data source connection strings, external JMS provider endpoints, and any other configuration that is also migrating to the Oracle Cloud Infrastructure environment.
The `export` command internally does the following:

1. Uses the service name argument to find the source Oracle Cloud Infrastructure Classic Oracle SOA Cloud Service instance details.
2. Connects to the source Oracle Cloud Infrastructure Classic Oracle SOA Cloud Service admin server.
3. Retrieves the Oracle Service Bus, Oracle Enterprise Scheduler, LDAP data, and artifacts.
6. Packages the artifacts into an archive.
7. Generates a configuration template with placeholders for values that may have to change in the target environment, such as database TNS strings.
8. Uploads the archive and configuration template to the storage container.

You are required to allow the migration VM to access the source Oracle SOA Cloud Service through SSH. However, no other network connectivity is required.

1. Export the instance. You can only specify a single instance at as time as the value for `source_instance`. This action exports that instance to an archive file.

   ```
   opc migrate soacs export -s source_instance
   ```

The following output is returned.

```
2019-07-22T15:26:44 INFO Loaded resources from 'resources-default.json' with modification time 2019-07-15T00:34:58
2019-07-22T15:26:46 INFO Extracting composites from ManagedServer 'IP_Address' and port '9073'
2019-07-22T15:26:46 INFO Extract Composites from SOA Cloud Service node IP_Address
2019-07-22T15:26:58 INFO Create temporary directory on target Node
2019-07-22T15:26:58 INFO Copy scripts folder to target Node
2019-07-22T15:27:34 INFO Creating sub directories
2019-07-22T15:27:34 INFO Extract the Composites to Jar files
2019-07-22T15:28:26 INFO debug
2019-07-22T15:28:33 INFO debug
2019-07-22T15:28:33 INFO find
2019-07-22T15:28:34 INFO fetch
2019-07-22T15:28:41 INFO Delete temp folder
2019-07-22T15:28:41 INFO SOA Managed Server Resources archived created
2019-07-22T15:28:43 INFO Extracting OSB Resources from AdminServer 'IP_Address' and port '9073'
2019-07-22T15:28:43 INFO Extract Composites from SOA Cloud Service node IP_Address
2019-07-22T15:28:50 INFO Create temporary directory on target Node
2019-07-22T15:28:52 INFO Copy scripts folder to target Node
2019-07-22T15:29:28 INFO Creating sub directories
2019-07-22T15:29:36 INFO Export OSB Configs and Resources to Jar file
2019-07-22T15:30:13 INFO debug
```
Provision an Oracle SOA Cloud Service Instance

The `soacs create` command is optionally used to create the target instance on Oracle Cloud Infrastructure. If you have not already created your target instance using the existing My Services Console, use the `soacs create` command. This initial release supports creation of the target through the Oracle PaaS API. The `create` command accepts an argument indicating the source Oracle Cloud Infrastructure Classic Oracle SOA Cloud Service instance being migrated and a configuration file with TNS strings and admin passwords, and triggers the creation of instances in Oracle Cloud Infrastructure. The result is an Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure matching with the source Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic, with the exception of the customer artifacts that are imported into the target instance with the `import` command.

1. Create a new Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure.

   opc migrate migrate soacs create -s source_instance

2. Enter the Oracle Cloud Infrastructure Platform Services Manager (PSM) password when prompted.

3. Enter the Oracle Cloud Infrastructure cloud storage password when prompted.

Once instance creation completes, you can import your Oracle Cloud Infrastructure Classic instance into the new Oracle Cloud Infrastructure instance.

Import the Instance

The `soacs import` command is the last command to run in a migration. It completes the migration of customer deployments from Oracle Cloud Infrastructure Classic to Oracle Cloud Infrastructure-based Oracle SOA Cloud Service instances. This results in an Oracle SOA Cloud Service instance on Oracle Cloud Infrastructure that has the application deployments, data sources, and other migrated artifacts to allow for your workload to move to Oracle Cloud Infrastructure. The `soacs import` command requires that you first update the configuration template JSON document locally on the migration VM to add in all secrets (WLS admin passwords, JDBC data source passwords, and so on).

1. Import the archive file into the new instance. You specify the source instance so that the profile file can be accessed for storage container information. You are
prompted to enter the configuration file name (for this example, named import_config.json) if the file is not found by opcmigrate.

```bash
opcmigrate migrate soacs import -a MigTest1-20190728-22:54:30.tgz -c import_config.json
```

The following output is returned.

```
2019-07-29T07:27:59 INFO Using local archive file
MigTest1-20190728-22:54:30.tgz
2019-07-29T07:27:59 INFO Exploding instance archive
"MigTest1-20190728-22:54:30.tgz"
2019-07-29T07:27:59 INFO Creating Common Resource Configurations on admin node IP_Address
2019-07-29T07:28:07 INFO Create temporary directory on target Node
2019-07-29T07:28:09 INFO Copy scripts folder to target Node
2019-07-29T07:28:42 INFO Verify Weblogic Credentials
2019-07-29T07:29:13 INFO command
2019-07-29T07:29:13 INFO debug
2019-07-29T07:29:13 INFO debug
2019-07-29T07:29:13 INFO command
2019-07-29T07:29:14 INFO Creating Directories
2019-07-29T07:29:16 INFO Copy archive to target Node
2019-07-29T07:30:25 INFO Import Common Configurations (JDBC, JMS, JNDI Configs)
2019-07-29T07:31:16 INFO Log stdout
2019-07-29T07:31:17 INFO Log stderr
2019-07-29T07:31:17 INFO command
2019-07-29T07:31:17 INFO Delete temp folder
2019-07-29T07:31:19 INFO SOA Admin Resources common configs created.
2019-07-29T09:11:32 INFO Import Composites to SOA Cloud Service node IP_Address
2019-07-29T09:11:40 INFO Create temporary directory on target Node
2019-07-29T09:11:43 INFO Copy scripts folder to target Node
2019-07-29T09:12:20 INFO Creating Directories
2019-07-29T09:12:22 INFO Copy archive to target Node
2019-07-29T09:13:29 INFO Import BPEL Processes
2019-07-29T09:14:01 INFO B2B Metadata
2019-07-29T09:14:08 INFO Delete temp folder
2019-07-29T11:39:15 INFO Import OSB, OWSM, ESS artifacts to SOA Cloud Service node IP_Address
2019-07-29T11:39:23 INFO Create temporary directory on target Node
2019-07-29T11:39:25 INFO Copy scripts folder to target Node
2019-07-29T11:40:12 INFO Creating Directories
2019-07-29T11:40:14 INFO Copy archive to target Node
2019-07-29T11:41:22 INFO Import OSB Configs and Resources to Jar file
2019-07-29T11:42:59 INFO Delete temp folder
```

2. Once the import process completes, log in to your new Oracle SOA Cloud Service instance.

3. Browse the pages and note that the instance you exported from Oracle SOA Cloud Service Classic is now visible.