Oracle® Cloud

Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure
## Contents

### 1  Getting Started with Oracle SOA Suite on Marketplace

- About Oracle SOA Suite on Marketplace .............................................. 1-1
- About the Oracle SOA Suite on Marketplace License ......................... 1-2
- About the Components of Oracle SOA Suite on Marketplace .............. 1-2
- About the Components of Oracle Cloud Infrastructure for Oracle SOA Suite 1-5
- About Life Cycle Management of Oracle SOA Suite on Marketplace Instances 1-5
- About Oracle SOA Suite on Marketplace Roles and User Accounts ........ 1-7
- About Adapters for Oracle SOA Suite on Marketplace ....................... 1-7
- Adding a Managed Server IP in a Non Proxy Host to Enable Deployment from Fusion Middleware Control 1-8
- About Keeping Oracle SOA Suite on Marketplace Instances Manageable 1-11

### 2  Before You Begin

- Signing in to the Oracle Cloud Infrastructure Console ....................... 2-1
- Restrictions ....................................................................................... 2-2
- Prerequisites ..................................................................................... 2-2
  - Creating a Compartment .................................................................. 2-3
  - Setting Up a Virtual Cloud Network ............................................... 2-4
  - Creating an Oracle Cloud Infrastructure Database for Oracle SOA Suite 2-5
  - Accessing a VM Through a Secure Shell (SSH) .............................. 2-5
    - Understanding SSH Keys ................................................................. 2-6
    - Generating a Secure Shell (SSH) Public/Private Key Pair .............. 2-7
    - Connecting to an Administration Server VM .................................. 2-9
    - Connecting to a Managed Server VM ............................................. 2-11
    - Creating an SSH Tunnel ................................................................. 2-14
    - Switching VM Users ...................................................................... 2-16

### 3  Creating and Managing Oracle SOA Suite Instances

- Creating an Oracle SOA Suite Instance .............................................. 3-2
- Completing Post-Provisioning Tasks .................................................... 3-6
  - Completing Post-Provisioning Tasks for an MFT Cluster Service Type 3-6
Configuring Mail Settings

Configuring User Messaging Service on a Cluster 4-1
   Creating the User Messaging Service JMS Server 4-2
   Creating a Persistent Store 4-3
   Creating a Subdeployment 4-4
   Deploying a User Messaging Service Adapter 4-4
Configuring Mail Sessions 4-5
   Importing a CA-Issued SSL Certificate into the Oracle SOA Suite Instance 4-5
   Configuring the Mail Driver for Outgoing Mails 4-7
   Updating the Workflow Notification Properties 4-8
Troubleshooting Oracle SOA Suite on Marketplace

Finding Diagnostic Information to Help with Troubleshooting
- Using the WebLogic Server Administration Console to Find Diagnostic Information
- Using the WebLogic Server Administration Console to Find Log Files
Problems Accessing the Worklist Application from Enterprise Manager
Problems with Failure of a Running Service When the Schema User Password Expires
Problems with Connectivity
Problems with the Node Manager
Problems with Database File System Mounting on Second Managed Server Node
Problems with a Database Deployment
Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control
Preface

Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure describes how to provision and administer Oracle SOA Suite 12.2.1.4 on Marketplace in Oracle Cloud Infrastructure Console.

Note:

In this guide, Oracle SOA Suite refers to any of the three service types that you can provision with Oracle SOA Suite on Marketplace:

- SOA with SB & B2B Cluster
- MFT Cluster
- BAM Cluster (single node recommended)

Topics:

- Audience
- Documentation Accessibility
- Related Resources
- Conventions

Audience

This guide is intended for users who want to create and manage Oracle SOA Suite instances provisioned from Marketplace in Oracle Cloud Infrastructure Console.

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:

- Oracle SOA Suite documentation for 12.2.1.4 in the Oracle Fusion Middleware 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><code>monospace</code></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>
Getting Started with Oracle SOA Suite on Marketplace

Review the following topics for an introduction to Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure.

Topics:

• About Oracle SOA Suite on Marketplace
• About the Oracle SOA Suite on Marketplace License
• About the Components of Oracle SOA Suite on Marketplace
• About Life Cycle Management of Oracle SOA Suite on Marketplace Instances
• About Oracle SOA Suite on Marketplace Roles and User Accounts
• About Adapters for Oracle SOA Suite on Marketplace
• About Keeping Oracle SOA Suite on Marketplace Instances Manageable

About Oracle SOA Suite on Marketplace

Oracle SOA Suite on Marketplace is based on Oracle SOA Suite 12c (12.2.1.4.0). It is provided as a VM-based solution on Oracle Cloud Infrastructure, using your existing Oracle SOA Suite 12c (12.2.1.4.0) on-premises license or a new license.

Oracle SOA Suite on Marketplace provides a PaaS (Platform as a Service) computing platform solution for running the following applications in the cloud:

• Oracle SOA Suite
• Oracle Service Bus
• Oracle B2B
• Oracle Managed File Transfer (MFT)
• Oracle Business Activity Monitoring (BAM)

Oracle SOA Suite on Marketplace provides a complete set of service infrastructure components for designing, deploying, and managing composite applications.

The components of the suite are described in About the Components of Oracle SOA Suite on Marketplace.

Oracle SOA Suite on Marketplace provides a rich variety of features that enable you to save time and money in the following ways:

• Reduce costs. You can reduce IT maintenance and administrative costs. Oracle handles all platform provisioning, installation, and domain configuration. Oracle SOA Suite on Marketplace is subscription-based, meaning you only pay when using the service. No large investment in hardware and IT expertise is required.
This lets you fully concentrate on design, test, and deployment of integration solutions.

- **Create test environments in the cloud.** You can quickly subscribe to Oracle SOA Suite on Marketplace to create application test environments in the cloud. There is no need to provision and configure your own servers. Move workloads to the cloud, from cloud to cloud, and from cloud to on-premises environments. When testing is done, you can release your subscription.

- **Monitor and manage your environment.** You can initiate VM backups and restore with minimal configuration from the cloud.

In addition, you can extend your enterprise to the cloud and deploy Oracle SOA Suite projects where you need them. For example, you can integrate an Oracle Sales Cloud new customer account with a Siebel application. This enables a customer that purchases a product through Oracle Sales Cloud to receive support for that product through the Siebel system. For this same Oracle Sales Cloud event, you can also synchronize the customer account information to an on-premises finance application to ensure that the billing and accounts receivable modules receive payment from the customer.

**More Information**

For documentation about Oracle SOA Suite 12c (12.2.1.4), see the Oracle Help Center.

---

**About the Oracle SOA Suite on Marketplace License**

Oracle SOA Suite on Marketplace supports Bring Your Own License (BYOL), or you can purchase a new license for Oracle SOA Suite 12c (12.2.1.4.0).

When you activate Oracle SOA Suite on Marketplace, you are charged the BYOL rate provided that you have sufficient supported on-premises licenses as required and specified in the Service Description for Oracle PaaS.

For the processor conversion ratios and license requirements, go to the Cloud Services Service Descriptions page and click the link to the Oracle PaaS and IaaS Universal Credits Service Descriptions PDF.

---

**About the Components of Oracle SOA Suite on Marketplace**

Oracle SOA Suite on Marketplace includes the following components:

- **Oracle SOA Suite.** Oracle SOA Suite is a comprehensive, hot-pluggable software suite that enables you to build, deploy, and manage integrations using service-oriented architecture (SOA). Oracle SOA Suite provides the following capabilities:
  - Consistent tooling
  - A single deployment and management model
  - End-to-end security
  - Unified metadata management

Oracle SOA Suite enables you to transform complex application integrations into agile and reusable service-based applications to shorten the time to market, respond faster to business requirements, and lower costs. Critical business services, such as customer, financial, ordering information, and others that were
previously accessible only in packaged application user interfaces can now be rapidly modeled for mobile devices such as smart phones and tablets.

Oracle SOA Suite includes the following core components:

- **BPEL** — (Business Process Execution Language) Orchestrates integration processes.
- **Human Workflow** — Creates interactions that require human input, like approvals or manual routing decisions.
- **Business Rules** — Defines flexible business rules to direct actions in an integration process, such as approval routing decisions.
- **Mediator** — Mediates messages and provides routing and the capability to transform simple message flows.

See:

- *Understanding Oracle SOA Suite*
- *Developing SOA Applications with Oracle SOA Suite*

**Oracle Service Bus.** Oracle Service Bus provides standards-based integration for high-volume SOA environments. Oracle Service Bus is a core component in Oracle SOA Suite on Marketplace, acting as a back-bone for SOA messaging. Oracle Service Bus connects, mediates, and manages interactions between heterogeneous services, legacy applications, packaged applications, and multiple enterprise service bus (ESB) instances across an enterprise-wide service network. Oracle Service Bus adheres to the SOA principles of building coarse-grained, loosely coupled, and standards-based services, creating a neutral container in which business functions can connect service consumers and back-end business services, regardless of underlying infrastructure.

Oracle Service Bus is deployed on the Admin Server and one non-clustered (stand-alone) Managed Server. Management features are deployed on the Admin Server, and runtime features are deployed on the Managed Server.

You can provision Oracle Service Bus with the **SOA with SB & B2B Cluster** service type.

See:

- *Administering Oracle Service Bus*
- *Developing Services with Oracle Service Bus*

**Oracle B2B.** Oracle B2B is an e-commerce gateway that enables the secure and reliable exchange of business documents between an enterprise and its trading partners. Oracle B2B supports business-to-business document standards, security, transports, messaging services, and trading partner management. With Oracle B2B used as a binding component within an Oracle SOA Suite composite application, end-to-end business processes can be implemented. Oracle B2B also supports Health Level 7, which enables health care systems to communicate with each other.

You can provision Oracle B2B with the **SOA with SB & B2B Cluster** service type.

See *Using Oracle B2B*.

**Oracle Managed File Transfer (MFT).** Oracle MFT is a high performance, standards-based, end-to-end managed file gateway. It features design, deployment, and monitoring of file transfers using a lightweight web-based design-
time console that includes transfer prioritization, file encryption, scheduling, and embedded FTP and sFTP servers.

You can provision Oracle MFT with the **MFT Cluster** service type.

See [*Using Oracle Managed File Transfer*](#).

**Oracle Business Activity Monitoring (BAM).** Oracle BAM is used to monitor business processes for making tactical and strategic decisions. You can create dashboards that contain graphical views of data updated either in real time as streams or on a scheduled basis. Oracle BAM also supports alerting capabilities for business users to monitor business events, manage business exceptions, and continuously optimize their processes.

You can provision Oracle BAM with the **BAM Cluster** service type.

See [*Monitoring Business Activity with Oracle BAM*](#).

**Oracle Technology Adapters.** Oracle JCA-compliant adapters enable you to integrate your business applications, and provide a robust, lightweight, highly-scalable and standards-based integration framework for disparate applications to communicate with each other.

With the growing need for business process optimization, efficient integration with existing back-end applications has become the key to success. To optimize business processes, you can integrate applications by using JCA 1.5 compliant resource adapters. Adapters support a robust, light weight, highly scalable, and standards-based integration framework, which enables disparate applications to communicate with each other. For example, adapters enable you to integrate packaged applications, legacy applications, databases, and Web services. Using Oracle JCA adapters, you can ensure interoperability by integrating applications that are heterogeneous, provided by different vendors, based on different technologies, and run on different platforms.

See: *

– [*About Adapters for Oracle SOA Suite on Marketplace*](#)
– [*Understanding Technology Adapters*](#)

**Oracle Cloud Adapters.** Cloud adapters simplify and accelerate integration with your SaaS applications. These adapters provide value to your SaaS integrations. Specifically, they provide lower costs of implementation and maintenance, ease of use, improved developer productivity and faster time-to-market for SaaS application integrations.

See [*About Adapters for Oracle SOA Suite on Marketplace*](#).

**Oracle Enterprise Scheduler.** Oracle Enterprise Scheduler is installed with Oracle SOA Suite on Marketplace. Oracle Enterprise Scheduler enables you to define, schedule, and run jobs. A job is a unit of work done on an application’s behalf. For example, you might define a job that runs a particular PL/SQL function or command-line process.

See:

– [*Administering Oracle Enterprise Scheduler*](#)
– [*Developing Applications for Oracle Enterprise Scheduler*](#)
About the Components of Oracle Cloud Infrastructure for Oracle SOA Suite

The components of Oracle Cloud Infrastructure that are used by Oracle SOA Suite on Marketplace are:

- **Marketplace.** An online store that's available in the Oracle Cloud Infrastructure console. When you launch an Oracle SOA Suite application from Marketplace, it prompts you for some basic information, and then directs you to Resource Manager to complete the configuration of your Oracle SOA Suite instance.
  
  See Overview of Marketplace in the Oracle Cloud Infrastructure documentation.

- **Resource Manager.** An Oracle Cloud Infrastructure service that uses Terraform to provision, update, and destroy a collection of related cloud resources as a single unit called a stack.
  
  See Overview of Resource Manager in the Oracle Cloud Infrastructure documentation.

- **Compute.** An Oracle Cloud Infrastructure service that lets you provision and manage compute hosts, known as instances
  
  See Overview of the Compute Service in the Oracle Cloud Infrastructure documentation.

- **Virtual Cloud Network.** A virtual, private network set up in Oracle data centers.
  
  See:
  - Setting Up a Virtual Cloud Network
  - Overview of Networking in the Oracle Cloud Infrastructure documentation

- **Load Balancer.** Provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN)
  
  See Overview of Load Balancing in the Oracle Cloud Infrastructure documentation.

- **Database.** Must be preprovisioned and provided as an input when configuring the Oracle SOA Suite on Marketplace instance in Oracle Cloud Infrastructure.
  
  See:
  - Creating an Oracle Cloud Infrastructure Database for Oracle SOA Suite
  - Overview of the Database Service in the Oracle Cloud Infrastructure documentation

About Life Cycle Management of Oracle SOA Suite on Marketplace Instances

With a few clicks of the mouse, you can create an Oracle WebLogic Server production environment in the cloud that is based on best practices, optimized for high performance and reliability, and is integrated with your Oracle SOA Suite on Marketplace instances.
When you create an Oracle SOA Suite on Marketplace instance, you create and configure an Oracle Fusion Middleware Infrastructure domain with the resources defined in the following table.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server</td>
<td>Operates as the central control entity for the configuration of the entire domain. It maintains the domain's configuration documents and distributes changes in the configuration documents to Managed Servers. Each Oracle SOA Suite Managed Server instance has one server instance that hosts the administration server.</td>
</tr>
<tr>
<td>Managed Servers</td>
<td>Host business applications, application components, Web services, and their associated resources. When creating a service instance, you can configure up to four Managed Servers, then scale out, as needed. Each Oracle SOA Suite Managed Server instance has one or more Managed Servers, each hosted by its own administration server. By default, the Managed Servers are named as follows: <code>first8charsOfDomainName_server_n</code> (where <code>n</code> starts with 1 and is incremented by 1 for each additional Managed Server to guarantee unique names).</td>
</tr>
<tr>
<td>Cluster</td>
<td>Consists of multiple Oracle WebLogic Server instances running simultaneously and working together to provide increased scalability and reliability. In a cluster, most resources and services are deployed identically to each Managed Server (as opposed to a single Managed Server), enabling failover and load balancing. A cluster is configured automatically for a production-level service instance. By default, the cluster name is generated from the first eight characters of the Oracle SOA Suite Managed Server instance name using the following format: <code>first8charsOfServiceInstanceName_cluster</code>.</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>Employs the Oracle Cloud Infrastructure load balancer to manage routing requests across all Managed Servers and provide failover and replication. It is recommended that you enable the load balancer (during provisioning) when you configure more than one Managed Server in your environment. Enabling the load balancer is optional.</td>
</tr>
</tbody>
</table>

If you want more information about Oracle WebLogic Server domains, see WebLogic Server Domains in Understanding Oracle WebLogic Server.

After the Oracle SOA Suite instance is created, the administration server in the domain is started automatically. You can deploy applications and manage the domain resources using the standard administration tools, including Enterprise Manager Fusion Middleware Control, Oracle WebLogic Server Administration Console, Oracle WebLogic Scripting Tool (WLST), Node Manager, and Oracle Cloud Infrastructure load balancer.

**Note:**

If you extend your domain using the administration tools, for example, to add an additional cluster, you are responsible for maintaining those additional resources.
About Oracle SOA Suite on Marketplace Roles and User Accounts

Oracle SOA Suite on Marketplace uses roles to control access to tasks and resources. A role assigned to a user gives certain privileges to the user.

Access to Oracle SOA Suite on Marketplace is based on the roles and users set up for the Oracle Cloud Infrastructure Console. To administer Oracle SOA Suite on Marketplace, you must have access to the network, permissions to manage compute instances, and Oracle Cloud Infrastructure database privileges.

For information about how to add user accounts in Oracle Cloud, see Managing User Accounts in Getting Started with Oracle Cloud.

About Adapters for Oracle SOA Suite on Marketplace

Oracle SOA Suite on Marketplace includes a number of adapters.

See the Oracle Integration Adapters Certification Matrix for certification information about the various integration adapters.

**Oracle Technology Adapters**

All of the technology adapters delivered with Oracle SOA Suite 12c (12.2.1.4) are available for Oracle SOA Suite on Marketplace for the SOA with SB & B2B Cluster service type. Connectivity to on-premises applications should be verified, and either SSH tunnels or VPN service should be used for connectivity to on-premises applications.

See Understanding Technology Adapters.

**Oracle Cloud Adapters**

Oracle Cloud Adapters are automatically installed and available as part of the Oracle SOA Suite on Marketplace provisioned environment.

Oracle SOA Suite on Marketplace supports the following cloud adapters for the SOA with SB & B2B Cluster service type:

- Ariba Adapter
- Oracle Eloqua Cloud Adapter (outbound from Oracle SOA Suite on Marketplace to Eloqua only)
- Oracle ERP Cloud Adapter
- Oracle NetSuite Adapter (outbound from Oracle SOA Suite on Marketplace to NetSuite only)
- Oracle RightNow Cloud Adapter
- Oracle Sales Cloud Adapter
- Salesforce Adapter
- ServiceNow Adapter
- SuccessFactors Adapter
Certified Application Adapters

The following enterprise application adapters are available:

- Oracle E-Business Suite Adapter
- Integration Adapter for SAP R/3
- Integration Adapter for JD Edwards World
- Integration Adapter for Siebel

B2B Adapter for EDI

The B2B Adapter for EDI Adapter provides a comprehensive platform for the implementation and management of business processes utilizing EDI and its related standards.

The B2B adapter for EDI is only available for use with the Universal Credits billing model and is billed as an additionally metered amount on the Oracle SOA Suite on Marketplace OCPUs at the instance level during provisioning or scaling. You cannot add the B2B Adapter for EDI to existing instances, nor can you remove it from an instance that it is assigned to. The adapter can only be set during the initial provisioning process and can only be removed by deleting the instance. Billing can be paused by stopping the instance, since the Universal Credits model is billed by the hour. See About the Oracle SOA Suite on Marketplace License.

It is recommended that B2B processing be done in an instance separate from your SOA processing so that you can dedicate resources to CPU intensive tasks like the batch processing of EDI transactions and not impact your real-time SOA transaction processing. For existing Oracle SOA Suite on Marketplace customers that have metered or non-metered Oracle SOA Cloud Service instances, the recommended path forward for using the B2B Adapter for EDI, is to provision a new Oracle SOA Suite on Marketplace instance in the Universal Credits account, and then use that instance exclusively for B2B processing. This allows you to run an existing SOA instance in parallel with your B2B instance.

You can download the B2B Document Editor to use with Oracle B2B from the Oracle SOA Suite Download page.

To download the B2B Document Editor:

1. Accept the license agreements.
2. Expand Free Oracle SOA Suite 12c Installations and then expand Recommended Install Process.

Adding a Managed Server IP in a Non Proxy Host to Enable Deployment from Fusion Middleware Control

If you use a cloud adapter, before you can use Fusion Middleware Control to deploy applications, you must add a Managed Server IP in to a non-proxy host.

To add a Managed Server IP to a non-proxy host:

1. Log in to Fusion Middleware Control.
2. Find the server in the **Target Navigation** pane.

3. Right-click the server and select **Administration > System MBean Browser**.

4. Search for the getURL operation.
   a. Click the binocular icon.
   b. Select **Operations**.
   c. Enter **getURL**
   d. Click the arrow button to start the search.
5. Click getURL.

6. Type **http** in the **Value** field and then click **Invoke**.
7. Follow the instructions in Configuring the Proxy Server for Runtime in the Oracle Cloud Adapters Postinstallation Configuration Guide to update the setDomainEnv.sh file.

You must invoke the getURL operation for all the MBeans found (each MBean maps to a Managed Server in the cluster). Note all the IPs and update the non-proxy hosts in setDomainEnv.sh and you can include the host IP address explicitly as shown in the following:

```
```

You must restart the servers (both administration and managed) for this settings to take effect.

## About Keeping Oracle SOA Suite on Marketplace Instances Manageable

Following best practices ensures that your Oracle SOA Suite on Marketplace instances stay manageable.

Reliable management of Oracle SOA Suite instances requires a specific software environment that includes service instances of an Oracle Cloud Infrastructure database and a secure shell (SSH) public key. For details on these features, see Before You Begin.

To keep your service instances manageable by Oracle SOA Suite on Marketplace, follow these guidelines:

- To ensure that you can restore the database for an Oracle SOA Suite instance without risking data loss for other service instances, do not use the same Oracle Cloud Infrastructure database as a Service instance with multiple Oracle SOA Suite instances. Backups of an Oracle Cloud Infrastructure database instance that are used with multiple Oracle SOA Suite instances contain data for all the Oracle SOA Suite instances. If you restore the database while restoring an Oracle SOA Suite instance, data for all the Oracle SOA Suite instances is restored.
• **Apply only** patches that are available through Oracle SOA Suite on Marketplace. Do **not** apply patches from any other source.

• Use only the default domain that was provisioned when a service instance was created. Do not add any Oracle WebLogic Server domains to the service instance.

• If you plan to integrate multi-domain environments, ensure that the first eight characters of your Oracle SOA Suite instance name are unique so that all domains and associated resources have unique names.

By default, the names of the domain and cluster in the Oracle SOA Suite instance are generated from the first eight characters of the Oracle SOA Suite instance name, and will use the following formats, respectively:

– `first8charsOfServiceInstanceName_domain`
– `first8charsOfServiceInstanceName_cluster`

See *Administering JMS Resources for Oracle WebLogic Server*.

• Do not detach, change file access permissions for, or change the mount point of any disk volume that Oracle SOA Suite Managed Server attaches to a service instance's VMs during creation of the service instance.

For details about these volumes, see About the Disk Volumes.

• Except for the `DOMAIN_HOME` volume, do not change the content of any disk volume that Oracle SOA Suite Managed Server attaches to a service instance’s VMs during creation of the service instance.

For details about these volumes, see About the Disk Volumes.

• Do not change the egress and ingress network and security settings of any infrastructure resources that the service instance uses.

• Do not close any ports or protocols that Oracle SOA Suite Managed Server opened during creation of a service instance.

You can open new ports and protocols, but closing existing ports and protocols may impair the functioning of a service instance.

• Do not detach NAT IP addresses from any of a service instance’s VMs.

• Do not change the Oracle Fusion Middleware component schemas with which a service instance was provisioned.

• Do not change the ports for the Oracle WebLogic Server administration server and the Oracle Cloud Infrastructure load balancer administration server.

• Do not change OS users and SSH key settings that Oracle SOA Suite Managed Server configured during creation of a service instance.
Before You Begin

Before provisioning Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure, make sure you are able to sign in to the Oracle Cloud Infrastructure Console and review the restrictions and prerequisites.

Topics:

• Signing in to the Oracle Cloud Infrastructure Console
• Restrictions
• Prerequisites

Signing in to the Oracle Cloud Infrastructure Console

Sign in to the Oracle Cloud Infrastructure Console as a user federated through Oracle Identity Cloud Service. A federated environment enables business partners to integrate in the identity management realm by providing a mechanism for users to share identity information across respective security domains.

1. Use the link provided to you to sign in to your cloud account.
   The Sign In screen is displayed, where you enter your cloud account name, which is your tenant name.
2. If needed, enter your cloud tenant, and click Continue.
   Identity options are displayed.
3. Under Single Sign-On (SSO) options, note the identity provider selected in the Identity Provider field and click Continue.
   The Oracle Identity Cloud Service sign in screen is shown.

4. Enter the user name and password provided in the welcome email, and click Sign In.
   One Console is shown. Want to learn more about One Console? See Oracle Cloud Infrastructure Blog.

Restrictions

Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure currently has the following restrictions:

- Does not support adding a load balancer post-provisioning using the current Terraform plan/stack.
- Does not support stopping and starting an instance from the Marketplace interface. See Stopping and Starting an Oracle SOA Suite Instance.
- If JET-based business views are used in a BAM dashboard, then enabling active data will not reflect any changes done to data objects in the BAM dashboard.
- Does not support BAM time-based alerts associated with business queries. To fix this issue, apply patch http://aru.us.oracle.com:8080/ARU/ViewPatchRequest/process_form?aru=23436184

Prerequisites

Before you can create an Oracle SOA Suite on Marketplace instance in Oracle Cloud Infrastructure, you must meet or complete several prerequisites.

Note:

Oracle SOA Suite on Marketplace instances created in Oracle Cloud Infrastructure require certain networking and storage resources that you must create in Oracle Cloud Infrastructure.

To use Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure, you need:

- A license for Oracle SOA Suite 12c (12.2.1.4.0), either Bring Your Own License (BYOL) or purchase a new license. See About the Oracle SOA Suite on Marketplace License.
- A compartment for your Oracle SOA Suite instances. See Creating a Compartment.
- A virtual cloud network (VCN) with at least one public subnet. See Setting Up a Virtual Cloud Network.
- An Oracle Cloud Infrastructure database that is preprovisioned and provided as an input when configuring the Oracle SOA Suite on Marketplace instance in Oracle Cloud Infrastructure. If you have not already created a database, you will need to
do so. See Creating an Oracle Cloud Infrastructure Database for Oracle SOA Suite.

**Note:**

The VCN in which the database is launched must be the same VCN used by your Oracle SOA Suite instance.

- A secure shell (SSH) public/private key pair for authenticating access to a VM through an SSH client. See Accessing a VM Through a Secure Shell (SSH).
- Oracle JDeveloper 12.2.1.4.0, available from the Oracle JDeveloper Software page.

Prior to using Oracle SOA Suite on Marketplace, you should be familiar with:

- Oracle Cloud
  
  Create and configure your account on Oracle Cloud. See Purchasing a Subscription to Oracle Public Cloud Services in Getting Started with Oracle Cloud.

- Oracle Compute VMs
  
  Oracle SOA Suite on Marketplace runs on Oracle Compute VMs. See Using Oracle Compute Cloud Service for information about disk images, compute shapes, storage volumes, public IP addresses, network groups, access rules, and SSH public/private key pairs.

- Oracle WebLogic Server
  
  Applications are deployed to Oracle WebLogic Server. Oracle SOA Suite on Marketplace supports Oracle WebLogic Server 12.2.1.4.0.

- Oracle Cloud Infrastructure Load Balancing service
  
  To provide load balancing for applications, Oracle SOA Suite on Marketplace uses the Oracle Cloud Infrastructure load balancer. See Overview of Load Balancing in the Oracle Cloud Infrastructure documentation

Creating a Compartment

If your tenancy does not already include the compartment for your Oracle SOA Suite instances, you can create a new one.

To create a compartment in Oracle Cloud Infrastructure:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Governance and Administration, go to Identity and click Compartments.

   A list of the existing compartments in your tenancy is displayed.

2. Click Create Compartment.

3. Enter the following:
   - **Name**: Restrictions for compartment names are: Maximum 100 characters, including letters, numbers, periods, hyphens, and underscores. The name must be unique across all the compartments in your tenancy.
Setting Up a Virtual Cloud Network

Set up a Virtual Cloud Network (VCN) for your Oracle SOA Suite instance to use.

This VCN quickstart procedure is useful for getting started and trying out Oracle Platform Services on Oracle Cloud Infrastructure. For production, use the procedure in VCNs and Subnets in the Oracle Cloud Infrastructure documentation. That topic explains features such as how to specify the CIDR ranges for your VCN and subnets, and how to secure your network. When you use the advanced procedure in that topic, remember that the VCN that you create must have a public subnet for Oracle Platform Services to use.

To set up a VCN:

1. In the Oracle Cloud Infrastructure Console, from the Regions menu, select the region in which you want to create your Oracle SOA Suite instance.
   
   Select a region that's within the default data region of your account. For example, if your default data region is EMEA, then select Germany Central (Frankfurt) or UK South (London).

2. From the Compartment list, select the compartment you created.

3. Click in the top left corner. In the navigation menu, under Core Infrastructure, select Networking, then Virtual Cloud Networks.

4. Click Networking Quickstart.

5. Select VCN with Internet Connectivity, and then click Start Workflow.

6. Enter the following:
   
   - **VCN Name**: Enter a name for your cloud network, for example, `your_initials_Network` (for example, `LB_Network`). The name is incorporated into the names of all the related resources that are automatically created. Avoid entering confidential information.
   
   - **Compartment**: Leave the default value (the compartment you're currently working in). All the resources will be created in this compartment.
   
   - **VCN CIDR Block**: Enter a valid CIDR block for the VCN. For example: `10.0.0.0/16`.
   
   - **Public Subnet CIDR Block**: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block. For example: `10.0.0.0/24`.
   
   - **Private Subnet CIDR Block**: Enter a valid CIDR block for the subnet. The value must be within the VCN's CIDR block and not overlap with the public subnet's CIDR block. For example: `10.0.1.0/24`.
   
   - Accept the defaults for any other fields.

7. Click Next.

8. Review the list of resources that the workflow will create for you. Notice that the workflow will set up security list rules and route table rules to enable basic access for the VCN.

9. Click Create to start the short workflow.
Creating an Oracle Cloud Infrastructure Database for Oracle SOA Suite

If it does not exist, create an Oracle Cloud Infrastructure database for use with Oracle SOA Suite.

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartement, and then click Create DB System.
3. In the Create DB System wizard, provide the information for the database. See the Oracle Cloud Infrastructure documentation for field descriptions.

-notes:
- The virtual cloud network (VCN) in which the DB system is launched must be the same VCN used by your Oracle SOA Suite instance.
- For Choose Storage Management Software, select Oracle Grid Infrastructure to use Oracle Automatic Storage Management. Oracle SOA Suite on Marketplace provisioned with the Oracle Cloud Infrastructure database supports only Oracle Grid Infrastructure storage management software. Oracle SOA is not supported with an Oracle Cloud Infrastructure database using Logical Volume Manager (LVM) storage management software.

4. Click Create DB System. The DB system appears in the list with a status of Provisioning. The DB system's icon changes from yellow to green (or red to indicate errors).
5. Wait for the DB system's icon to turn green, with a status of Available, and then click the highlighted DB system name.
   Details about the DB system are displayed.
6. Note the IP addresses; you'll need the private or public IP address, depending on network configuration, to connect to the DB system.

Accessing a VM Through a Secure Shell (SSH)

You can access the services and resources that an Oracle SOA Suite on Marketplace instance's VM provides by logging into the VM as the opc user through SSH. You can use any SSH utility (such as PuTTY or OpenSSH).
Notes:

- Only the opc user can remotely connect to your VMs. You cannot use SSH to connect to a VM as the oracle user. After successfully connecting to a VM, tasks such as starting and stopping the server and accessing the administrative logs should only be performed by the oracle user.

- Oracle pushes regular OPC/PSM related updates to the VMs to support interaction between the Oracle Cloud Portal and the VMs silently. Oracle does not send notifications of these updates as they only affect Oracle owned files and scripts that should not be modified, and the updates do not require any down-time either.

- VM start and stop is controlled by SSH access. SSH access is not allowed when Oracle SOA Suite on Marketplace quota reaches the limit. When you try to access SSH a quota limit message is displayed.

Topics:

- Understanding SSH Keys
- Generating a Secure Shell (SSH) Public/Private Key Pair
- Connecting to an Administration Server VM
- Connecting to a Managed Server VM
- Creating an SSH Tunnel
- Switching VM Users

Understanding SSH Keys

In order to access an Oracle SOA Suite on Marketplace virtual machine (VM) with a secure shell (SSH) client, you must create a public/private key pair and configure the service instance with the public key.

When you create an Oracle SOA Suite on Marketplace instance, you are prompted to supply the public key. To connect to a VM in an Oracle SOA Suite on Marketplace instance, you supply the paired private key when logging in to the machine using an SSH client.

You can provide an existing public key that you previously created with an external tool, or Oracle SOA Suite on Marketplace can create a new key pair for you.

You may also use the same SSH public/private key pair that you used for creating an Oracle Cloud Infrastructure database deployment.
Generating a Secure Shell (SSH) Public/Private Key Pair

Several tools exist to generate SSH public/private key pairs. The topics in this section show how to generate an SSH key pair on UNIX, UNIX-like, and Windows platforms.

Topics:

- Generating an SSH Key Pair on UNIX and UNIX-Like Platforms Using the ssh-keygen Utility
- Generating an SSH Key Pair on Windows Using the PuTTYgen Program

Generating an SSH Key Pair on UNIX and UNIX-Like Platforms Using the ssh-keygen Utility

UNIX and UNIX-like platforms (including Solaris and Linux) include the ssh-keygen utility to generate SSH key pairs.

To generate an SSH key pair on UNIX and UNIX-like platforms using the ssh-keygen utility:

1. Navigate to your home directory:

   ```
   $ cd $HOME
   ```

2. Run the ssh-keygen utility, providing as `filename` your choice of file name for the private key:

   ```
   $ ssh-keygen -b 2048 -t rsa -f filename
   ```

   The ssh-keygen utility prompts you for a passphrase for the private key.

3. Enter a passphrase for the private key, or press Enter to create a private key without a passphrase:

   ```
   Enter passphrase (empty for no passphrase): passphrase
   ```

   While a passphrase is not required, you should specify one as a security measure to protect the private key from unauthorized use. When you specify a passphrase, a user must enter the passphrase every time the private key is used.
The ssh-keygen utility prompts you to enter the passphrase again.

4. Enter the passphrase again, or press Enter again to continue creating a private key without a passphrase:
   Enter the same passphrase again: passphrase

5. The ssh-keygen utility displays a message indicating that the private key has been saved as `filename` and the public key has been saved as `filename.pub`. It also displays information about the key fingerprint and randomart image.

Generating an SSH Key Pair on Windows Using the PuTTYgen Program

The PuTTYgen program is part of PuTTY, an open source networking client for the Windows platform.

To generate an SSH key pair on Windows using the PuTTYgen program:

1. Download and install PuTTY or PuTTYgen.
   To download PuTTY or PuTTYgen, go to http://www.putty.org/ and click the You can download PuTTY here link.

2. Run the PuTTYgen program.
   The PuTTY Key Generator window is displayed.

3. Set the Type of key to generate option to SSH-2 RSA.

4. In the Number of bits in a generated key box, enter 2048.

5. Click Generate to generate a public/private key pair.
   As the key is being generated, move the mouse around the blank area as directed.

6. (Optional) Enter a passphrase for the private key in the Key passphrase box and reenter it in the Confirm passphrase box.

   Note:
   While a passphrase is not required, you should specify one as a security measure to protect the private key from unauthorized use. When you specify a passphrase, a user must enter the passphrase every time the private key is used.

7. Click Save private key to save the private key to a file. To adhere to file-naming conventions, you should give the private key file an extension of .ppk (PuTTY private key).

   Note:
   The .ppk file extension indicates that the private key is in PuTTY’s proprietary format. You must use a key of this format when using PuTTY as your SSH client. It cannot be used with other SSH client tools. Refer to the PuTTY documentation to convert a private key in this format to a different format.
8. Select all of the characters in the **Public key for pasting into OpenSSH authorized_keys file** box.

   Make sure you select all the characters, not just the ones you can see in the narrow window. If a scroll bar is next to the characters, you aren’t seeing all the characters.

9. Right-click somewhere in the selected text and select **Copy** from the menu.

10. Open a text editor and paste the characters, just as you copied them. Start at the first character in the text editor, and do not insert any line breaks.

11. Save the text file in the same folder where you saved the private key, using the `.pub` extension to indicate that the file contains a public key.

12. If you or others are going to use an SSH client that requires the OpenSSH format for private keys (such as the `ssh` utility on Linux), export the private key:
   a. On the **Conversions** menu, choose **Export OpenSSH key**.
   b. Save the private key in OpenSSH format in the same folder where you saved the private key in `.ppk` format, using an extension such as `.openssh` to indicate the file’s content.

**Connecting to an Administration Server VM**

You can access an Administration Server VM through a secure shell (SSH) utility.

To access an Administration Server VM through SSH:

1. In the Oracle Cloud Infrastructure Console, click ☐ in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.

2. Click the instance associated with the VM you want to access.

3. Note the **Public IP Address** of the Administration Server VM.
4. On UNIX and UNIX-like platforms, use the standard OpenSSH command (`ssh`) to connect to the VM as the `opc` user.

Provide the following:

- The path to the private key corresponding to the public key used at the time of provisioning.
- The VM's public IP address.

in this format:

```
ssh -i path_to_private_key opc@VM_IP_address
```

For example:

```
ssh -i /home/myuser/id_rsa opc@111.111.111.111
```

5. On Windows, you can use PuTTY, an open source networking client for the Windows platform, to connect to the VM as the `opc` user.

a. Launch PuTTY.

   The PuTTY Configuration window is displayed, showing the Session panel.

b. In the **Host Name (or IP address)** field, enter the public IP address of the VM.
c. In the Category tree, expand **Connection** if necessary and then click **Data**.

d. In the **Auto-login username** field, enter opc.

e. Confirm that the **When username is not specified** option is set to **Prompt**.

f. In the Category tree, expand **Connection > SSH**, and then click **Auth**.

g. Under **Private key file for authentication**, click **Browse**.

h. Navigate to and select your private key file. Then click **Open**.

![Note:

The .ppk file extension indicates that the private key is in PuTTY’s proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.]

i. Click **Open** to open the connection to the VM.

6. If the private key was defined with a passphrase, enter this value when prompted.

When the VM command line appears, you can use any resource accessible from the VM. For example, you can run the WebLogic Scripting Tool on the Administration Server VM.

Connecting to a Managed Server VM

You can access a Managed Server VM through a secure shell (SSH) utility by using the Administration Server VM as a proxy.

Alternatively, you can connect to the Administration Server VM with SSH, and from within this SSH session start another SSH connection to the Managed Server VM.

To connect to a Managed Server VM by using the proxy method:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.

2. Click the instance associated with the VM you want to access.

3. Note the **Public IP Address** of the Administration Server VM (used as the proxy).
4. On UNIX and UNIX-like platforms, use the standard OpenSSH command (`ssh`) to connect to the VM as the `opc` user.

Provide the following:

- The path to the private key corresponding to the public key used at the time of provisioning.
- The Administration Server VM’s public IP address.

in this format:

```bash
ssh -i path_to_private_key -o ProxyCommand="ssh -W %h:%p -i path_to_private_key opc@admin_server_VM_IP_address" admin_server_VM_IP_address
```

For example:

```bash
ssh -i /home/myuser/id_rsa -o ProxyCommand="ssh -W %h:%p -i /home/myuser/id_rsa opc@111.111.111.111" 111.111.111.111
```

5. On Windows, you can use PuTTY, an open source networking client for the Windows platform, to connect to the VM as the `opc` user.
a. Launch PuTTY. If your private key was defined with a passphrase, then you
must use the pageant utility to launch PuTTY:

```
pageant "path to private key" -c "path to putty"
```

For example:

```
c:\PuTTY\pageant "c:\oracle\rsa.ppk" -c "c:\PuTTY\putty"
```

b. If you used pageant to start PuTTY, enter the passphrase for the private key.
The PuTTY Configuration window is displayed, showing the Session panel.

c. In the Host Name (or IP address) field, enter the host name of the Managed
Server VM.

d. In the Category tree, expand Connection if necessary and then click Data.

e. In the Auto-login username field, enter opc.

f. Confirm that the When username is not specified option is set to Prompt.

g. In the Category tree, click Connection > Proxy.

h. Set Proxy type to Local.

i. In the Proxy hostname field, enter the IP address of the Administration
Server VM.

j. Set the Port to 22.

k. In the Telnet command or local proxy command field, enter the following
value:

```
plink -i "path to private key" opc@%proxyhost -nc %host:%port
```

For example:

```
plink -i "c:\oracle\rsa.ppk" opc@%proxyhost -nc %host:%port
```

l. In the Category tree, expand Connection > SSH, and then click Auth.

m. Under Private key file for authentication, click Browse.

n. Navigate to and select your private key file. Then click Open.

---

### Note:

The .ppk file extension indicates that the private key is in PuTTY's proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.

o. Click Open to open the connection to the VM.
Creating an SSH Tunnel

An SSH tunnel to an Oracle SOA Suite on Marketplace VM enables you to connect to other non-public ports on the VM through a port on your local machine.

You can create access rules to an Oracle SOA Suite on Marketplace instance as an alternative to creating an SSH tunnel. However, use caution and consider possible security implications before opening up ports to external access.

If a resource provided by a VM uses a port that is not directly accessible through the Internet, you can access that resource by creating an SSH tunnel to the port. For example, you can use an SSH tunnel to connect a local Integrated Development Environment (IDE) such as Eclipse to the dedicated deployment port (9001) of the Administration Server.

In general an SSH tunnel may map a remote port to any available port number on your local machine. However, port 9001 on the Administration Server uses JMX/RMI for communication, which requires that the remote and local port numbers be the same value. Therefore, the following instructions configure the tunnel’s local port number to the same value as the VM’s port number.

**Tutorial**

To set up an SSH tunnel to an Administration Server VM:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.
2. Click the instance associated with the VM you want to access.
3. Note the **Public IP Address** of the Administration Server VM.
4. On UNIX and UNIX-like platforms, use the standard OpenSSH command (ssh) to create an SSH tunnel to the VM.

   Provide the following:
   - The path to the private key corresponding to the public key used at the time of provisioning.
   - The VM’s public IP address.
   - The port number on the VM to which you want to connect. The SSH tunnel will enable connectivity to this remote port though the same port number on your local machine.
in this format:

```bash
ssh -i path_to_private_key -L port:VM_IP_address:port opc@VM_IP_address
-N
```

For example, to create an SSH tunnel to port 9001 on the Administration Server VM:

```bash
ssh -i /home/myuser/id_rsa -L 9001:111.111.111.111:9001 opc@111.111.111.111 -N
```

5. On Windows, you can use PuTTY, an open source networking client for the Windows platform, to create an SSH tunnel to the VM.
   a. Launch PuTTY.
      The PuTTY Configuration window is displayed, showing the Session panel.
   b. In the Host Name (or IP address) field, enter the public IP address of the VM.
   c. In the Category tree, expand Connection if necessary and then click Data.
   d. In the Auto-login username field, enter opc.
   e. Confirm that the When username is not specified option is set to Prompt.
   f. In the Category tree, click Connection > SSH.
   g. Under Protocol options, select the checkbox Don't start a shell command at all.
   h. In the Category tree, expand Connection > SSH, and then click Auth.
   i. Under Private key file for authentication, click Browse.
   j. Navigate to and select your private key file. Then click Open.

   ![Note:](image)
   The .ppk file extension indicates that the private key is in PuTTY’s proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.

   k. In the Category tree, click Connection > SSH > Tunnels.
   l. In the Destination field, enter IP:port,
      where IP is the IP address of the VM and port is the port number on the VM to which you want to connect.
   m. In the Source Port field, enter the same port number.
   n. Click the Add button.
   o. Click Open to create the SSH tunnel to the VM.
6. If the private key was defined with a passphrase, enter this value when prompted. Applications running on your local machine can now communicate with the VM by using localhost:port, where port is the local port number.

For example, after creating an SSH tunnel to port 9001 on the Administration Server VM, launch a web browser and connect to http://localhost:9001/console.

Note: After your work with the SSH tunnel is complete, perform a <ctrl> C to shut down the SSH tunnel.

Switching VM Users

You can change users on a VM in order to perform specific administration tasks.

You must SSH to a VM only as the opc user. This user has root privileges on the OS running in the VM. For example, opc can be used to create other OS users on a VM. Simply prefix root operations with the sudo command. For example:

```bash
sudo useradd myuser
```

Note: There is no default password for the opc user.

Switching to Oracle

The oracle VM user has regular OS user permissions. It is intended to be used to start and stop Oracle products that have been installed on the VM, or to run other Oracle applications and utilities on the VM.

Type the following to become the oracle user:

```bash
sudo su - oracle
```

Note: There is no default password for the oracle user.
Switching to Root

An alternative to using the `sudo` command to perform root OS operations with the opc user is to switch to the root user.

Type the following to become the root user:

```
sudo -s
```

**Note:**

Avoid using the root user except to perform privileged OS administration tasks.
Creating and Managing Oracle SOA Suite Instances

Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure is customer-managed, not Oracle-managed. This means that you are responsible for managing instances, including performing database management, completing backups, and installing patches.

You can perform several management tasks from the Oracle Cloud Infrastructure Console. Some tasks are performed outside the Console.

>Note:
In this guide, Oracle SOA Suite refers to either service type that you can provision with Oracle SOA Suite on Marketplace:
- SOA with SB & B2B Cluster
- MFT Cluster

Topics:
- Creating an Oracle SOA Suite Instance
- Completing Post-Provisioning Tasks
- Viewing Oracle SOA Suite Instance Details
- Accessing an Oracle SOA Suite Instance
- Accessing the WSDL of a Composite Deployed to a SOA Server
- Editing an Oracle SOA Suite Instance
- Stopping and Starting an Oracle SOA Suite Instance
- Scaling an Oracle SOA Suite Instance Out or In
- Scaling an Oracle SOA Suite Instance Up or Down
- Patching Oracle SOA Suite Instances
- Backing Up a Block Volume
- Restoring a Block Volume
- Deprovisioning an Oracle SOA Suite Instance
Creating an Oracle SOA Suite Instance

Create an Oracle SOA Suite instance in a selected compartment in Oracle Cloud Infrastructure.

Notes:

- Before you begin these steps, make sure that you have met the necessary Prerequisites.
- With administration privileges in Oracle Cloud Infrastructure, you can delete compute instances from an Oracle SOA Suite cluster. To delete nodes from a cluster when you no longer need the cluster, it is recommended that you use Terraform Actions > Destroy (see Deprovisioning an Oracle SOA Suite Instance). As a best practice, use a dedicated compartment for provisioning Oracle SOA Suite compute instances, and restrict administrator access to this compartment. This will ensure that Oracle Cloud Infrastructure Console users cannot delete the instances and administrators will use Terraform Actions > Destroy to terminate instances.

To create an Oracle SOA Suite instance:

1. In Marketplace, launch by direct URL or by browsing:
   - Browsing: In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Solutions and Platform, click Marketplace, and search for Oracle SOA Suite 12.2.1.4.

The Marketplace listing for SOA Suite 12.2.1.4 is displayed.
2. Click **Oracle SOA Suite** to open the landing page, and review the information on the **Overview** page.

3. Click **Get App**.

4. Select your region, and click **Sign In**.

5. **Sign in to the Oracle Cloud Infrastructure Console**.

6. Select the **Compartment** in which you want to create the new instance.

7. Accept the terms and restrictions, then click **Launch Stack**.

   The Create Stack wizard is displayed.

8. Provide information about the stack for the instance as described in the following table.

<table>
<thead>
<tr>
<th>Field Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Optionally, modify the default name for the stack after it’s deployed. The name must be unique within the identity domain and must meet the following conditions: start with a letter, not longer than 30 characters, not contain non-alphanumeric character (including spaces).</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Optionally, enter a description of the stack. For example, you can specify the name of the application that will run on the stack after it is deployed.</td>
</tr>
<tr>
<td>CREATE IN COMPARTMENT</td>
<td>Automatically populated with the compartment you selected on the landing page. This is the compartment where the stack will be created in the tenancy. (Stacks are attached to a specific region. However, where necessary, the resources on a given stack can be deployed across multiple regions.)</td>
</tr>
<tr>
<td>TERRAFORM VERSION</td>
<td>Prefilled with the Terraform version used for the Marketplace offering.</td>
</tr>
<tr>
<td>TAGS</td>
<td>Optionally, select existing tags or add tags to associate with the stack. For more information about tagging, see Resource Tags. If you do not assign tags during provisioning, you can create and manage tags after the stack is created.</td>
</tr>
</tbody>
</table>

9. Configure variables for the instance as described in the following table.

<table>
<thead>
<tr>
<th>Field Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Instance</td>
<td></td>
</tr>
<tr>
<td>INSTANCE NAME PREFIX</td>
<td>Enter the prefix you wish to use for the instance name.</td>
</tr>
<tr>
<td>Field Label</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SERVICE TYPE                    | Select the service type you are provisioning:  
  - SOA with SB & B2B Cluster  
  - MFT Cluster  
  - BAM Cluster (single node recommended)  
  **Note:** In this guide, *Oracle SOA Suite* refers to any of the three service types.                                                                 |
<p>| COMPUTE SHAPE                   | Select a compute shape with at least 15GB of memory. See Compute - Virtual Machine Instances. You cannot change the compute shape after you have created the Oracle SOA Suite instance.                                        |
| SSH PUBLIC KEY                  | Enter the public key for the secure shell (SSH). This key is used for authentication when connecting to the Oracle SOA Suite instance using an SSH client. See Generating a Secure Shell (SSH) Public/Private Key Pair |
| AVAILABILITY DOMAIN             | Select the name of the availability domain in which to create the instances.                                                                                                                                |
| CLUSTER NODE COUNT              | Enter the initial number of SOA Server compute instances. This is also the number of Managed Servers in the cluster.                                                                                           |
| ADMINISTRATION USERNAME         | Enter the name of the SOA Server domain administrator.                                                                                                                                                      |
| ADMINISTRATION PASSWORD         | Enter a password that meets the specifications shown below the field. If you select the USE KMS DECRYPTION option, enter the encrypted password.                                                           |
| Key Management Service Configuration |                                                                                                                                                          |
| USE KMS DECRYPTION             | Select to enable Key Management Service (KMS) password encryption. For more information, see Overview of Key Management.                                                                                     |
| KEY MANAGEMENT SERVICE KEY ID   | If you selected USE KMS DECRYPTION, enter the OCID for your encryption key.                                                                                                                                  |
| KEY MANAGEMENT SERVICE CRYPTOGRAPHIC ENDPOINT | If you selected USE KMS DECRYPTION, enter the KMS endpoint for decryption.                                                                                                                                   |
| Instance Network                |                                                                                                                                                          |
| NETWORK COMPARTMENT             | Automatically populated with the compartment you selected on the landing page. This is the compartment where the instance will be created in the tenancy.                                                     |
| VIRTUAL CLOUD NETWORK STRATEGY  | Select to create or use an existing VCN in which to create the instances, network resources, and load balancers.                                                                                              |
| EXISTING NETWORK                | If you select to use an existing VCN, select the name of the VCN.                                                                                                                                              |
| SUBNET STRATEGY                 | Select to create or use an existing subnet.                                                                                                                                                                   |
| SUBNET TYPE                     | Select either a public or private subnet.                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>Field Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBNET SPAN</td>
<td>Select either a region or a subnet specific to the availability domain.</td>
</tr>
<tr>
<td>EXISTING SUBNET</td>
<td>Select an existing subnet to use for service instances. This subnet must already be present in the chosen VCN.</td>
</tr>
<tr>
<td>PROVISION LOAD BALANCER</td>
<td>Select to provision a load balancer to distribute traffic. For more information, see Overview of Load Balancing in the Oracle Cloud Infrastructure documentation.</td>
</tr>
<tr>
<td>EXISTING SUBNET FOR LOAD BALANCER</td>
<td>If you selected PROVISION LOAD BALANCER, select an existing subnet to use for the load balancer. This subnet must already be present in the chosen VCN.</td>
</tr>
<tr>
<td>LOAD BALANCER SHAPE</td>
<td>If you selected PROVISION LOAD BALANCER, select the load balancer shape.</td>
</tr>
</tbody>
</table>

**Database**

<table>
<thead>
<tr>
<th>DATABASE STRATEGY</th>
<th>Select the database strategy for WebLogic Server:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* Database System (the Oracle Cloud Infrastructure database), supported for any service type.</td>
</tr>
<tr>
<td></td>
<td>* Autonomous Transaction Processing Database, supported only for the SOA with SB &amp; B2B Cluster service type. If you select the ATP database for the MFT Cluster service type, provisioning will fail.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DB SYSTEM</th>
<th>Select the DB system to use for this WebLogic Server domain. This should be in the same VCN as WebLogic instances.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATABASE HOME IN THE DB SYSTEM</td>
<td>Select the database home within the DB system.</td>
</tr>
<tr>
<td>DATABASE IN THE DB SYSTEM</td>
<td>Select the database in which to provision the schemas for a JRF-enabled WebLogic Server domain.</td>
</tr>
<tr>
<td>PDB</td>
<td>Enter the name of the pluggable database (PDB) in which to provision the schemas for a JRF-enabled WebLogic Server domain.</td>
</tr>
<tr>
<td>DATABASE ADMINISTRATOR</td>
<td>Enter the name of a database user with DBA privileges.</td>
</tr>
<tr>
<td>DATABASE ADMINISTRATOR PASSWORD</td>
<td>Enter a password for the database administrator. If you selected USE KMS DECRYPTION above, enter the encrypted password.</td>
</tr>
</tbody>
</table>

**Service Instance Advanced**

| SERVICE INSTANCE ADVANCED CONFIGURATION | Select to specify port configuration properties. Refer to the descriptions below each field. |

**Tags** For more information, see Resource Tags.

<table>
<thead>
<tr>
<th>DEFINED TAG KEY</th>
<th>Optionally, enter a defined tag key for the instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFINED TAG VALUE</td>
<td>Enter the value for the specified defined key.</td>
</tr>
</tbody>
</table>
Completing Post-Provisioning Tasks

Review the following topics to learn about additional tasks to perform after provisioning.

Topics:
- *(Required for MFT)* Completing Post-Provisioning Tasks for an MFT Cluster Service Type
- *(Optional)* Extending Your On-Premises Network with a VCN on Oracle Cloud Infrastructure
- *(Optional)* Registering a Custom Domain Name with a Third-Party Registration Vendor

Completing Post-Provisioning Tasks for an MFT Cluster Service Type

After provisioning an Oracle Managed File Transfer (MFT) Cluster, you need to perform several post-provisioning tasks for the service to work correctly.

MFT includes an embedded sFTP server. However by default, the sFTP server is disabled after MFT provisioning. You need to enable the sFTP server so that it can receive encrypted messages from partners using public/private key encryption. In this encryption and connection process, the private key decrypts messages that were encrypted using the associated public key. As illustrated in the diagram below, the private key is placed in the embedded sFTP server, and the partners/sFTP clients get a copy of the public key.
Configuring the SSH Keystore for the MFT sFTP Server

In Oracle MFT Cloud Service, you need to configure the SSH keystore to enable an embedded sFTP server secured connection. The configuration includes importing the private key of the SSH key pair and entering the password in the SSH keystore if the private key has a passphrase.

Importing the Private Key

The private key of the SSH key pair from the provisioning process is used by the MFT server to start the sFTP server so clients can connect to it using the SSH protocol. Note that the key must have an RSA style and be in OpenSSH format, otherwise the embedded sFTP server won’t accept it.

1. In the MFT Console, on the Administration page, select Keystore Management.
2. Select the Keys tab. You can list, create, update, export, import or delete a key.
3. Click the Import icon on the right side of the page.
   - The Import key dialog opens.
4. Enter the following details:
   - **Alias**: alias name
   - **Format**: select PGP or SSH type of key
• **Browse**: enter the path of the key file
• **Type**: specify private or public key

5. Click **Import** to import the key.

**Entering the Private Key Password in the SSH Keystore**

If your private key was created with a password/passphrase, which is intended to provide a secondary security in case the private key file is lost, then you will provide the password in MFT SSH Keystore.

1. Go to the Details page of the MFT instance you want to access, as described in Viewing Oracle SOA Suite Instance Details.
2. In the **Jobs** section, click the job name to display the log file.
3. Scroll to the bottom of the log file, and copy the URL of the MFT Console.
4. Enter the URL in your browser to display the MFT Console for working with the Oracle SOA Suite instance.
5. Sign in to MFT Console with the user name and password you defined when provisioning the service.
6. Click the **Administration** tab on the top of the Console page.
7. To set the SSH Keystore password, select the **Keystores** node in the left navigator tree and enter the WebLogic admin password from the provisioning process in the **SSH Keystore** section.

8. Click **Save**.

**Enabling and Starting the MFT sFTP Server**

After configuring the SSH Keystore, you must enable the embedded sFTP server, configure its security settings, and then restart the sFTP Server.

To enable and start the MFT sFTP Server:

1. Enable the sFTP server and configure it with the private key alias:
a. In the MFT Console, select the **Embedded Servers** node in the left navigation tree.
b. Click the **sFTP** tab.
c. Select the **Enabled** checkbox to enable sFTP.
d. For **Authentication Type**, choose **Password**.
e. Set **Host Key Alias** to the private key alias you just imported.

2. Click **Save**.

3. Use the **WebLogic Server Console** to restart the MFT managed servers.

4. To verify the embedded sFTP server is started properly, select the **Embedded Servers > Ports** node in the left navigation tree. You should see the sFTP server is running on port 7522.

5. To test the sFTP connection, use an sFTP client or a command line tool on your local machine. For example:

   `$sftp -oPort=7522 mftadmin@192.1.1.1`  

6. Enter the password when prompted.

7. At the sFTP prompt, enter the following:

   `sftp> ls  
   payloads`
Extending Your On-Premises Network with a VCN on Oracle Cloud Infrastructure

A Virtual Cloud Network (VCN) is a customizable private network in Oracle Cloud Infrastructure.

Just like a traditional data center network, a VCN provides you with control over your network environment. This includes assigning your own private IP address space, creating subnets, creating route tables and configuring stateful firewalls. A single tenant can have multiple VCNs, thereby providing grouping and isolation of related resources.

One way to connect your on-premises network and your VCN is to use an Internet Protocol Security (IPSec) VPN. IPSec is a protocol suite that encrypts the entire IP traffic before the packets are transferred from the source to the destination.

The overall process for creating an IPSec VPN comprises the following steps:

1. Create your VCN.
2. Create a subnet in the VCN.
3. Create a Dynamic Routing Gateway (DRG).
4. Attach the DRG to your VCN.
5. Create a Customer Premises Equipment (CPE) object and provide your router's public IP address.
6. From your DRG, create an IPSec connection to the CPE object and provide your static routes.
7. Get the IPSec tunnel information
8. Configure the IPSec connection on the remote end.
9. Create a route table and route rule for the DRG.
10. Create a security list and required rules.
To set up and manage an IPSec VPN for your VCN:

1. Create a VCN.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click Create Virtual Cloud Network.
   c. In the Create Virtual Cloud Network dialog, select a compartment, enter a name for your VCN, and select Create Virtual Cloud Network Only to explicitly create the subnetworks and their configuration.
   d. Click Create Virtual Cloud Network.

Your VCN is created with some default components (default route table, default security list, default set of DHCP options).

2. Next, you'll create subnets in separate Availability Domains. This allows distributing your instances across the subnets for high availability.
   a. In the Virtual Cloud Network details page, in the left pane, under Resources, select Subnets.
   b. Click Create Subnet.

Enter the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the subnet</td>
</tr>
<tr>
<td>Availability Domain</td>
<td>Select an availability domain for your subnet.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CIDR Block</td>
<td>Specify a CIDR block to indicate the network address that can be allocated to the resources.</td>
</tr>
<tr>
<td>Route Table</td>
<td>Select a route table to provide mapping for the traffic from the subnet to destinations outside the VCN.</td>
</tr>
<tr>
<td>SUBNET ACCESS</td>
<td><strong>PRIVATE SUBNET:</strong> Select this option to prohibit public IP addresses for instances in the subnet.</td>
</tr>
<tr>
<td></td>
<td><strong>PUBLIC SUBNET:</strong> Select this option to allow public IP addresses for instances in the subnet.</td>
</tr>
<tr>
<td>DNS HOSTNAMES IN THIS SUBNET</td>
<td>Select this option to allow assignment of DNS hostname when launching an instance.</td>
</tr>
<tr>
<td>DNS LABEL</td>
<td>Auto-generated if no name is specified.</td>
</tr>
<tr>
<td>DNS DOMAIN NAME</td>
<td>Read-only field</td>
</tr>
<tr>
<td>DHCP OPTIONS</td>
<td>Select the DHCP option for the VCN.</td>
</tr>
<tr>
<td>Security Lists</td>
<td>Specify security list/s for the VCN.</td>
</tr>
</tbody>
</table>

c. Click Create.

3. Create a Dynamic Routing Gateway (DRG) to provide a path for private network traffic between your VCN and on-premises network.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Dynamic Routing Gateway.
   b. Click Create Dynamic Routing Gateway.
   c. Specify a compartment, enter a name for the DRG and click Create.

4. Once the Dynamic Routing Gateway is created, you can attach it to your VCN.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Virtual Cloud Networks.
   b. Click your VCN to open its details.
   c. In the Virtual Cloud Network Details page, in the left navigation pane, under resources, select Dynamic Routing Gateways.
   d. Click Attach Dynamic Routing Gateway.
   e. Select the dynamic routing gateway that you created and click Create.

5. After attaching the Dynamic Routing Gateway to your VCN, create a Customer Premises Equipment (CPE) to logically represent the on-premises VPN device within Oracle Cloud Infrastructure networking configuration.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Customer-Premises Equipment.
   b. Click Create Customer-Premises Equipment.
   c. Select the compartment, enter a name and IP address for the customer-premises equipment, and click Create.
6. Next, create an IPSec connection to the customer-premises equipment.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Dynamic Routing Gateways.
   b. Click the dynamic routing gateway that you created in step 3.
   c. In the Dynamic Routing Gateway details page, in the left navigation pane, under resources, click IPSec Connections.
   d. Enter a name and public (external) IP address of the VPN device to be used to establish IPSec VPN and click Create.

   Once the IPSec connection is created, Oracle Cloud Infrastructure creates IPSec tunnel endpoints in each availability domain. You can use the tunnel information to configure the on-premises VPN device.

7. Get the IPSec tunnel information. Select the IPSec Connection and click Tunnel Information. The tunnel information contains the IP addresses of the tunnel endpoints and the shared secret to be used to initiate the IPSec connection. It also shows the status of the IPSec connection.

8. Configure the IPSec connection on the remote end. Your network administrator can configure your on-premises VPN device(s) to initiate an IPSec connection to the tunnels created on Oracle Cloud Infrastructure.

   Note:
   It is recommended to establish at least two IPSec tunnels, from the on-premises VPN device.

9. Configure routing for subnets to go through Dynamic Routing Gateway for on-premises traffic. The default routing table created for a VCN has no rules by default. All instances in VCN have a route to other instances in the VCN only.
   a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Virtual Cloud Network.
   b. Click the VCN to open its details.
   c. In the Virtual Cloud Network details page, in the left pane, under Resources, select Route Tables and then click Edit Route Rules.
   d. Modify the default route table to add a default route and set the Dynamic Routing Gateway as the route target. This routes any non-VCN traffic through the Dynamic Routing Gateway into the on-premises network.

10. Configure security rules to allow valid traffic in/out of your subnets.
    a. Click in the top left corner. In the navigation menu, under Core Infrastructure, go to Networking and click Virtual Cloud Network.
    b. In the Virtual Cloud Network details page, in the left pane, under Resources, select Security Lists.
    c. Select the security list for your VCN and click Security List Details.
    d. The default security list has only three ingress rules and one egress rule to allow all outgoing traffic. Click Edit All Rules to modify the rules to allow SSH.
as required and to open up specific ports for the application running on your compute instances within the subnets.

Registering a Custom Domain Name with a Third-Party Registration Vendor

Third-party vendors enable you to register custom domain names.

To register your custom domain and resolve it to the Oracle Cloud Infrastructure load balancer:

1. Register your domain name through a third-party domain registration vendor, such as verisign.com, register.com and namecheap.com.

2. Resolve your domain name to the IP address of the Oracle Cloud Infrastructure load balancer, using the third-party domain registration vendor console.

Note:
- For more information, refer to the third-party domain registration documentation.
- Configure all clients that invoke Oracle SOA Suite with the DNS name, and not the IP address of the load balancer.
- Don't get a self-signed certificate. Get a CA (certificate authority)-issued certificate.

Viewing Oracle SOA Suite Instance Details

You can view the details about an Oracle SOA Suite instance in Oracle Cloud Infrastructure and perform actions on the instance.

To view stack details for the instance and perform stack actions:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Solutions and Platform, go to Resource Manager and click Stacks.

2. If needed, select a compartment in the Compartment field. The page is refreshed to show stacks in the selected compartment.

3. Click a stack name to open the Stack Details page. The word Active is displayed in the left pane to indicate that this stack is running.

The following table describes the key information shown on the Details page:
### Field Description

**Stack Information**
- **Usage instructions.**
- **Description of the stack.**
- **Compartment to which the stack is assigned.**
- **OCID value that uniquely identifies the stack.**
- **Created date and time.**
- **Terraform version.**

**Edit Stack**
Click to edit the provisioning settings for the stack.

**Move Stack**
Click to move the stack to a different compartment. This action can take some time to complete.

**Terraform Actions**
Click to select the following actions to perform on the selected stack and instance:
- **Plan**: Creates the build plan for the environment required to create an instance.
- **Apply**: Executes the Plan operation to create the instance.
- **Import State**
- **Destroy**: Deletes the compute instances, VCNs, subnets, load balancer, and backend servers created during provisioning. If you select this action, then want to re-create an instance using the same stack, select the **Plan** and **Apply** operations.

See [Deprovisioning an Oracle SOA Suite Instance](#).

**Delete Stack**
Click to delete the selected stack after selecting Terraform Actions > Destroy. See [Deprovisioning an Oracle SOA Suite Instance](#).

**Add Tags**
Click to add tags to the selected stack. You can use tags to search for and categorize your instances in your tenancy. See [Resource Tags](#).

**Tags tab**
Displays any tags associated with the stack. Click **Add Tags** to add a tag.

**Jobs section**
Click a job to display its details, including logs, variables, associated resources, outputs and state. The logs and outputs include URLs for working with the Oracle SOA Suite instance. See [Accessing an Oracle SOA Suite Instance](#).

On the Job Details page, you can download:
- **Logs** `.log` file
- **Terraform configuration** `.zip` file
- **Terraform state** `.json` file

To view the compute instance details:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Compute and click Instances.
2. Click the instance name to display its details on the Instance Information and Tags tabs.
Accessing an Oracle SOA Suite Instance

You can access an Oracle SOA Suite instance through the URLs in the log file.

**Notes:**

- The steps described in this section assume that you have view permission to the compartment containing one or more Oracle SOA Suite instances. For users without view (or greater) permission to the console, a URL to the Oracle SOA Suite instance should be provided by the administrator.

- A user who creates an instance automatically has the ServiceAdministrator role assigned. All other users must have the appropriate role assigned for access.

To access a deployed Oracle SOA Suite instance:

1. Go to the Stack Details page of the instance you have provisioned, as described in Viewing Oracle SOA Suite Instance Details.

2. In the Jobs section, click the job name to display the Job Details page.

3. Under Resources in the left pane, click Outputs to view the IP addresses and URLs that you can use to access the instance.

4. Alternatively, click Logs and scroll through the log file to identify IP addresses and URLs that you can use to access the instance. For example:

```
PM Console = https://150.126.163.170:7002/en
Instance Subnet ID = ocid1.subnet.oc1.iad.aaaaaaaaabcdefg
Public Ip = [150.213.69.48]

Service Console =
SOA Composer = https://129.213.69.88/soa/composer
B2B Console = https://129.213.69.88/b2bconsole
Service Bus Console = https://158.136.163.170:7002/servicebus
Workflow Application = https://129.213.69.88/integration/workflowapp

Service Instances =

Version = 12.2.1.4 (JRF with OCI DB)
Virtual Cloud Network Id = ocid1.vcn.oc1.iad.aaaaaaaaabcdefg
WebLogic administration Console = https://150.136.163.170:7002/console
for MFT we will display mft URL in service Console URLs, remaining is same
MFT Console = https://150.136.199.148/mftconsole
```
Refer to the following table for example IP addresses and URLs. Note that the URLs to some components differ depending on whether or not you configured a load balancer during provisioning.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Provisioned with Load Balancer</th>
<th>Provisioned without Load Balancer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Public (Admin) IP 150.136.163.170</td>
<td>150.136.163.170</td>
</tr>
<tr>
<td></td>
<td>Load Balancer IP 129.213.69.88</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>B2B Console <a href="https://129.213.69.88/b2bconsole">https://129.213.69.88/b2bconsole</a></td>
<td><a href="https://150.136.163.170/b2bconsole">https://150.136.163.170/b2bconsole</a></td>
</tr>
<tr>
<td>MFT Cluster</td>
<td>MFT Console <a href="https://129.213.69.88/mftconsole">https://129.213.69.88/mftconsole</a></td>
<td><a href="https://150.136.163.170/mftconsole">https://150.136.163.170/mftconsole</a></td>
</tr>
</tbody>
</table>

5. Enter a URL in your browser to display the associated Console for working with the Oracle SOA Suite instance.

### Accessing the WSDL of a Composite Deployed to a SOA Server

You can use a browser or SOAP client to access the WSDL of a composite that is deployed to a SOA Server.

To access the WSDL:

1. For the instance in which the composite is running, get the IP address of the WebLogic Server console as described in Accessing an Oracle SOA Suite Instance.
   
   For example: 12.251.267.111

2. Copy the WSDL URL from the Test Web Service page WSDL field to your browser or SOAP client's URL field.

   For more information about the Test Web Service page, see Administering Web Services.
3. Replace the host name portion of the WSDL URL with the IP address from the Oracle WebLogic Server console.

   http://ws_console_IP_address/services/default/HelloWorld/helloworlddprocess_client_ep?WSDL

   For example:


**Editing an Oracle SOA Suite Instance**

You can edit an Oracle SOA Suite instance from Resource Manager or the Details page.

1. To view the SOA Suite instance you want to edit, see Viewing Oracle SOA Suite Instance Details.

2. Edit the instance in either of two ways:
   - In Resource Manager, at the far right of the row for the instance, click and select Edit.
   - On the Details page, click Edit Stack.

3. In the Edit Stack wizard, edit fields as required. See Creating an Oracle SOA Suite Instance for field descriptions.

**Stopping and Starting an Oracle SOA Suite Instance**

You can stop or start all nodes in an Oracle SOA Suite instance cluster.

**Topics:**

- About Stopping and Starting an Oracle SOA Suite Instance and Individual VMs
- Stopping an Oracle SOA Suite Instance
- Starting an Oracle SOA Suite Instance

**About Stopping and Starting an Oracle SOA Suite Instance and Individual VMs**

You can stop and start an Oracle SOA Suite instance and, when the service instance is running, stop, start, and restart individual server VMs.

**Note:**

The stop and restart procedures stop VMs. If you want to shut down the WebLogic Administration Server or Managed Server processes running on the VMs, without stopping the VMs, see Stopping an Oracle SOA Suite Instance. You might want to do this if you have other processes besides the servers running on the VMs and you do not want to shut down these other processes.
Why Stop an Oracle SOA Suite Instance?

Stopping an Oracle SOA Suite instance frees up compute resources used by the service instance’s VMs.

What Happens When an Oracle SOA Suite Instance is Stopped or Started?

Stopping and starting an Oracle SOA Suite instance has the following results:

- **Stopping the service instance**: The VMs on which the administration server, Managed Servers, and load balancer are running are stopped. You cannot start, stop, or restart the administration server, Managed Server, or load balancer VMs individually while the service instance is stopped.

- **Starting the service instance**: All VMs on which the administration server, Managed Server, and load balancer are running are started. You can restart the administration server, and stop, start, or restart the Managed Servers and load balancer VMs individually.

Why Stop, Start, or Restart an Administration Server, Managed Server, or Load Balancer VM?

If an Oracle SOA Suite instance is running:

- You can restart the VMs on which the Administration Server, Managed Server, or load balancer are running if you are experiencing problems with the server that would warrant a reboot. The restart operation is the same as stopping the server or load balancer VM, then starting it immediately.

- You can stop the VMs on which the Managed Server or the load balancer are running to free up resources. You might also want to stop the service instance instead of scaling, keeping the server or load balancer ready for a later time. If you stop all but one Managed Server VM, you might want to stop the load balancer VM because it is not needed.

- You can start a Managed Server or load balancer VM if it is stopped and you want to use it again.

Stopping an Oracle SOA Suite Instance

Use the WebLogic Server Administration Console to shut down the server processes for your Oracle SOA Suite instance, then use the Oracle Cloud Infrastructure Console to stop the Oracle SOA Suite instance.

To shut down the Managed Servers and Administration Server:

1. Navigate to the WebLogic Server Console, as described in Accessing an Oracle SOA Suite Instance.

2. When the console login page appears, enter the WebLogic username and password you provided when you created the Oracle SOA Suite instance.

3. Under **Domain Structure**, expand **Environment**.

4. Select **Servers**.

5. On the **Configuration** tab of the Summary of Servers page, notice that the state of the Administration Server and Managed Servers is RUNNING.

6. Select the **Control** tab.
7. Click the check box to the left of each Managed Server name.

8. Click **Shutdown**, and then select **Force Shutdown Now** or **When Work Completes**.

9. Repeat steps 7 and 8 for the Administration Server.

When you shut down the Administration Server, a message warns you that the browser session will end. Confirm the prompt to end the session.

To stop the Oracle SOA Suite instance:

1. In the Oracle Cloud Infrastructure Console, click ![icon] in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.

2. On the Compute page, at the far right of the row for the instance, click ![icon] and select **Stop**.

---

Starting an Oracle SOA Suite Instance

Use the Oracle Cloud Infrastructure Console to start the Oracle SOA Suite instance, then start the Managed Servers through the WebLogic Server Administration Console.

To start an Oracle SOA Suite instance:

1. In the Oracle Cloud Infrastructure Console, click ![icon] in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.

2. On the Compute page, at the far right of the row for the instance, click ![icon] and select **Start**.

To start the Managed Servers:

1. Navigate to the WebLogic Server Console, as described in *Accessing an Oracle SOA Suite Instance*.

2. When the console login page appears, enter the WebLogic username and password you provided when you created the Oracle SOA Suite instance.

3. Under **Domain Structure**, expand **Environment**.

4. Select **Servers**.

5. On the **Configuration** tab of the Summary of Servers page, notice that the Administration Server state is **RUNNING**, and the Managed Servers state is **SHUTDOWN**.

6. Select the **Control** tab.

7. Click the check box to the left of each Managed Server name.

8. Click **Start**.

9. On the Server Life Cycle Assistant, click **Yes**.

   The server state changes to **STARTING**.

10. Click the **Refresh** icon.

   The server state changes to **RUNNING**.
Changing the Database Schema and Wallet Passwords

Update the password used by an Oracle SOA Suite instance to access the Oracle schemas in the Oracle Cloud Infrastructure database.

Password expiration leads to the following scenarios:

- The following Oracle SOA Suite instance-specific datasources fail:
  - EDNDataSource
  - mds-owsm
  - EDNLocalTxDataSource
  - mds-soa
  - OraSDPMDDataSource
  - SOADatasource
  - SOALocalTxDataSource

- The following non-Oracle SOA Suite instance-specific datasources fail and the failure to connect to schemas may lead to production environment shutting down:
  - opss-data-source
  - opss-audit-viewDS
  - opss-audit-DBDS

- The database user account can get locked because data sources still use the old password and the administrator enters a different password.

When you change the password, the passwords for the Oracle SOA Suite and non-Oracle SOA Suite schemas are reset.

You can only use Oracle SOA Suite to change the password for the Oracle Required Schemas found in the Infrastructure database for a service instance. To change the password for schemas hosted in an Application database in your service instance, you must directly modify the configuration of both the database and your WebLogic Server domain.

After you update the database schema password, the Oracle Database File System (DBFS) mount point does not work because its wallet is not synchronized with the credentials and fails to mount. To avoid this problem, you must manually update the wallet password.

Topics:

- Changing the Database Schema Password Manually
- Changing the Wallet Password

Changing the Database Schema Password Manually

The following summary shows the high-level tasks to change the database schema password. Detailed steps are below.

1. Update each infrastructure repository schema's password on the database deployment.
2. If the WebLogic Servers are running and the WebLogic Server Administration Console is accessible, change the password for all the corresponding data sources from the Weblogic Administration Console.

3. If the WebLogic Servers are not running and the WebLogic Server console is inaccessible, manually change the passwords in the WebLogic Server configuration.

4. Update the bootstrap credentials using the WebLogic Scripting Tool (WLST).

5. Start the Administration Server with the Node Manager, and then start the Managed Servers.

Detailed steps to change the database schema password:

1. Update each infrastructure repository schema's password on the database deployment.

   If the schema prefix is already known, go to Step b.

   a. Connect to the Oracle SOA Suite instance node that hosts the Administration Server, and get the value of the schema prefix.

      ```
      ssh -i private_key opc@IP_address_of_admin_server_VM
      sudo su oracle
      curl http://192.1.1.192/latest/user-data/chef/initial_attributes/wlss/schema_prefix
      ```

      The Schema Prefix value returned is similar to the following:

      ```
      SP255951777
      ```

   b. Log in to the Oracle Cloud Infrastructure database deployment node.

      ```
      ssh -i ssh_key opc@DB_vm_ip_address
      sudo su oracle
      ```

   c. Connect to the Oracle Cloud Infrastructure database deployment.

      ```
      sqlplus / as sysdba
      ```

      Use the username provided when provisioning the database deployment.

      If your database deployment version is 12c, the following step is also required:

      ```
      alter session set container=PDB1
      ```

      Use the PDB name provided during Oracle SOA Suite provisioning.

   d. Change the password for the infrastructure repository schema users:

      ```
      schema_prefix_IAU
      schema_prefix_IAU_APPEND
      schema_prefix_IAU_VIEWER
      schema_prefix_MDS
      ```
schema_prefix_OPSS
schema_prefix_STB
schema_prefix_UMS

Change the password for each of the schema users pertaining to the WebLogic Server version on the database deployment. For example:

```sql
ALTER USER schema_prefix_IUA identified by new_password;
```

The password must start with a letter, be between 8 and 30 characters long, and contain at least one number. The password can optionally include the special characters: $, #, _.

e. Unlock all the user accounts on the database to cover for the case that they are locked due to repeated login failures after password expiry.

```sql
ALTER USER schema_prefix_IAU ACCOUNT UNLOCK;
```

### Note:

If the WebLogic Administration Server is running and the WebLogic Administration Console is accessible, follow Step 2, else go to Step 3.

2. Update all the datasources from the WebLogic Administration Console to reflect the new password.

a. Log in to the WebLogic Administration Console and navigate to the **Services — Datasources** menu on the Domain Structure box.

b. Click **Lock & Edit**.

c. For each datasource, navigate to the **Datasource Name — Configuration — Connection Pool** tab and update the **Password** and **Confirm Password** field with the new password.

d. Click **Save** on this page, and then **Activate**.

e. Stop all the WebLogic Servers.

   From the WebLogic Administration Console, click on **Servers** under Environments in the Domain Structure section.

   Under the **Control** tab, select all of the servers and click **Shutdown — Force Shutdown Now**.

   Proceed to Step 4.

3. If the WebLogic Server is not running or the Administration Console is not accessible:

   a. Encrypt the new schema password and Update Data Source Configuration files:

```
ssh -i private_key opc@ipaddress_of_Admin_VM
sudo su oracle; cd /u01/data/domain/domain_name
```
Ensure WebLogic Servers are not running. If running, stop the processes:
Find the process IDs:

```
ps -ef | grep java
```

Kill processes:

```
kil -9 pid
```

Run:

```
domain_home/bin/setDomainEnv.sh
```

b. Run the WebLogic Encryption Utility and enter the password you set for the database schemas.

```
/u01/jdk/bin/java weblogic.security.Encrypt
password: <Enter the new password for the schema user>
```

c. Note the encrypted password output for future reference.
The following example shows an encrypted password:

```
AES]JHyrhOMB5hVRuDU/pV0qX86qz98ZV0xWXBSEANA4Gs=
```

d. Update the new password in the datasource xml files.

```
cd domain_home/domain_name/config/jdbc
```

Open the datasource xml files found in the domain_home/domain_name/config/jdbc directory that need to be updated with the new encrypted password:

- LocalSvcTblDataSource-jdbc.xml
- opss-auditview-jdbc.xml
- mds-owsm-jdbc.xml
- opss-datasource-jdbc.xml
- opss-audit-jdbc.xml

4. Run the modifyBootStrapCredential WLST command to update jps-config.xml with the new password for the SCHEMA_PREFIX_OPSS user.

a. Connect to the Oracle SOA Suite node hosting the Administration Server.

```
ssh -i private_key opc@IP_of_admin_server
sudo su oracle
```

b. Invoke WLST.

```
/u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh
```
c. Run the `modifyBootStrapCredential` command. Specify the full path to the `jps-config.xml` file.

Use the following syntax:

```
wls:offline>modifyBootStrapCredential(jpsConfig_File='domain_home/directory_name/config/fmwconfig/jps-config.xml',username='schema_prefix_OPSS',password='new_password_set_for_this_schema_user')
```

5. Start the Administration Server through the Node Manager and then the Managed Server(s).
   a. Log in to the Oracle SOA Suite node hosting the WebLogic Administration Server.
   
   b. Start WLST.

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

   c. Connect to the Node Manager.

Before running the command, get the required values of some of the variables involved.

- **Host name** — At the command prompt, type `hostname`.
- **Node Manager port number, domain name, domain home** — Open the `nodemanager.properties` files to determine the respective values.

```
/u01/data/domains/domain_name/nodemanager/nodemanager.properties
```

- **Administration Server name** —

```
  cd /u01/data/domains/domain_name/servers.
  Look for the server name ending in `adminserver`.
```

Run the `nmConnect` command.

```
nmConnect('weblogic_username','weblogic_password','hostname','domain_name','domain_home/directory_name','ssl')
```

d. Start the Administration Server.

```
nmStart("admin_server_name")
```

e. After the Administration Server has status RUNNING, access the WebLogic Administration Console and start the Managed Servers.

- Click **Servers** under Environments in the Domain Structure section.
- Under the **Control** tab, select the Managed Servers and click **Start**.

### Changing the Wallet Password

After you update the schema password, the Oracle Database File System (DBFS) mount point does not work because its wallet is not synchronized with the credentials...
and fails to mount. To avoid this problem, you must manually update the wallet password.

To update the wallet password:

1. Regenerate the DBFS wallet with a new password:
   a. `ssh` to the Administration Server and `sudo` to the `oracle` user.
   b. Go to the DBFS directory:
      
      ```bash
      /u01/data/domains/domain_name/dbfs
      ```
   c. Back up the old wallet:
      
      ```bash
      mv wallet wallet_bckup
      ```
   d. Create a new wallet directory:
      
      ```bash
      mkdir wallet
      ```
   e. Create a temp file to store the database credentials:
      
      ```bash
      vi /var/tmp/dbfsp
      ```
   f. Enter the new credentials three times in the `dbfsp` file on three different lines.
   g. Save the file.
   h. Generate the Oracle Wallet at `/u01/data/domains/domain_name/dbfs` by executing the following command:
      
      ```bash
      $middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/
      domain_name
      /dbfs/wallet -create < /var/tmp/dbfsp
      ```
   i. Add the new credentials in the wallet by executing the following command. For this example, `SchemaPrefix_DBFS` is the DBFS user name specified:
      
      ```bash
      $middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/
      domain_name/dbfs/wallet
      -createCredential ORCL SchemaPrefix_DBFS < /var/tmp/dbfsp
      ```
   j. Repeat Step 1 on all nodes of the managed server.

2. Verify the status of the mount:

   ```bash
   ls -ltr /u01/soacs
   ```
If the permissions on mount directories `/u01/soacs/dbfs` and `/u01/soacs/dbfs_directio` are corrupted (shows `????` in place of permissions), execute the following commands:

```bash
fusermount -u /u01/soacs/dbfs

fusermount -u /u01/soacs/dbfs_directio
```

b. Verify the status of the mount directory again:

```bash
ls -ltr /u01/soacs
```

c. Once the directory permissions are restored, go to step 3.

3. Stop and then restart the Managed Servers. It is not necessary to stop and start the Oracle SOA Suite instance. See Stopping and Starting an Oracle SOA Suite Instance

### Scaling an Oracle SOA Suite Instance Out or In

You can scale an Oracle SOA Suite on Marketplace instance out or in by scaling a cluster or a node.

Determine what you need to scale from metrics associated with the instance. For example, if response times are long, consider scaling out the cluster. If heap usage is high, consider scaling up the nodes in the cluster.

Scale an Oracle SOA Suite on Marketplace instance cluster to add nodes to or remove nodes from the cluster in response to changes in the load on the cluster. A node is a virtual machine (VM) running a Managed Server instance that is a member of a cluster.

### Notes:

- When you scale out, Oracle SOA Suite on Marketplace creates a new VM running an Oracle WebLogic Server Managed Server instance. When you scale in, Oracle SOA Suite on Marketplace removes an Oracle WebLogic Server Managed Server instance and the VM that it is running on.

- Scale out and in operations support the addition and deletion of Managed Servers one node at a time.

- On Oracle Weblogic Server, every node of the cluster will be associated with an index starting from 1.
  - During scale out, this index is incremented and a new node or Managed Server will be added with new index.
  - During scale in, the Managed Server with the highest index in the cluster will be deleted.
Topics:
- About Scaling Out an Oracle SOA Suite Instance Cluster
- About Scaling In an Oracle SOA Suite Instance Cluster
- Scaling Out an Oracle SOA Suite Instance Cluster
- Scaling In an Oracle SOA Suite Instance Cluster

About Scaling Out an Oracle SOA Suite Instance Cluster

Scaling out an Oracle SOA Suite on Marketplace instance cluster adds one node to the cluster.

If an attempt to scale out a cluster fails, you will need to complete a scale in operation to revert the Oracle SOA Suite instance to its original state.

For steps to scale out an Oracle SOA Suite on Marketplace instance cluster, see Scaling Out an Oracle SOA Suite Instance Cluster.

About Scaling In an Oracle SOA Suite Instance Cluster

Scaling in an Oracle SOA Suite on Marketplace instance cluster removes the selected node from the cluster.

Before scaling in an Oracle SOA Suite instance cluster, ensure that the cluster contains at least one node for the administration server and first Managed Server. You cannot scale in a cluster that contains only the node for the administration server and first Managed Server. If you no longer require that node, you must delete the entire instance. See Deprovisioning an Oracle SOA Suite Instance.

If an attempt to scale in a cluster fails, you can try rerunning the Terraform apply operation.

For steps to scale in an Oracle SOA Suite on Marketplace instance cluster, see Scaling In an Oracle SOA Suite Instance Cluster.

Scaling Out an Oracle SOA Suite Instance Cluster

Scaling out an Oracle SOA Suite on Marketplace instance cluster will add one node to the cluster.

For more information about scaling out an Oracle SOA Suite on Marketplace instance cluster, see About Scaling Out an Oracle SOA Suite Instance Cluster.

To scale out an Oracle SOA Suite on Marketplace instance cluster:

1. In the Oracle Cloud Infrastructure Console, click ☐ in the top left corner. In the navigation menu, under Solutions and Platform, go to Resource Manager and click Stacks.
2. If needed, select a compartment in the Compartment field.
   The page is refreshed to show stacks in the selected compartment.
3. Click a stack name to open the Stack Details page. The word Active is displayed in the left pane to indicate that this stack is running.
4. Click **Edit Stack**.

5. On the Edit Stack page, click **Configure Variables**.

6. Increment the **CLUSTER NODE COUNT** value by 1.

**Note:**

Add only one node at a time.
7. Click **Next** to navigate to the Review page showing the new cluster node count value.

8. Click **Save Changes**.

9. On the Stack Details page, click **Terraform Actions** and select **Plan**.

10. In the Plan dialog, click **Plan**.

11. When the Terraform plan job completes successfully, click **Terraform Actions** and select **Apply**.

12. In the Apply dialog, click **Apply**.
13. At the end Terraform apply log, review the updated instance summary with the new node details. For example:

If the scale out operation fails, you will need to complete a scale in operation to revert the Oracle SOA Suite instance to its original state.
Scaling In an Oracle SOA Suite Instance Cluster

Scaling in an Oracle SOA Suite on Marketplace instance cluster will delete one node from the cluster.

For more information about scaling in an Oracle SOA Suite on Marketplace instance cluster, see About Scaling In an Oracle SOA Suite Instance Cluster.

To scale in an Oracle SOA Suite instance cluster, first complete prerequisite steps:

1. Use ssh to access the Admin VM (as the opc user):
   
   ```
   ssh -i private_key opc@Admin_VM_Public_IP
   ```

2. Change to the oracle user:
   
   ```
   sudo su oracle
   ```

3. Change the current working directory to `/opt/scripts` and execute a shell script that prompts for the Managed Server name and the Oracle WebLogic Server Admin password:
   
   ```
   /opt/scripts
   ./delete_server.sh
   ```

4. At the prompt, enter the name of the Managed Server that you want to remove as part of the scale in. This name can be obtained from the Oracle WebLogic Server Console **Servers** section.

---

**Note:**

The shell script performs the following operations on your Oracle WebLogic Server:

- Deletes the managed server.
- Deletes the Unix machine.
- Deletes JMS servers and other resources associated to this node.

It does not delete the VM and block volumes associated with the instance.

Example script output:
After completing the prerequisite steps, perform the following steps to scale in an Oracle SOA Suite instance cluster:

1. Follow steps 1-5 in Scaling Out an Oracle SOA Suite Instance Cluster.

2. Decrement the CLUSTER NODE COUNT value by 1.

   **Note:**
   
   Remove only one node at a time.

3. Follow steps 7-13 in Scaling Out an Oracle SOA Suite Instance Cluster.

   If the scale in operation fails, you can try rerunning the Terraform apply operation.

### Scaling an Oracle SOA Suite Instance Up or Down

After provisioning, you can scale an Oracle SOA Suite on Marketplace instance up or down.

**Note:**

A scale up or down operation causes a server restart. Before scaling, make sure that there are no active running processes on the servers.

To scale an Oracle SOA Suite on Marketplace instance up or down:

1. In the Oracle Cloud Infrastructure Console, click ![icon] in the top left corner. In the navigation menu, under **Solutions and Platform**, go to **Resource Manager** and click **Stacks**.

2. If needed, select a compartment in the **Compartment** field.

   The page is refreshed to show stacks in the selected compartment.

3. Click a stack name to open the Stack Details page. The word **Active** is displayed in the left pane to indicate that this stack is running.
4. Click **Edit Stack**.

5. On the Edit Stack page, click **Configure Variables**.

6. In the **COMPUTE SHAPE** drop-down list, select the shape you want your instance to be scaled to. You can choose either a higher compute shape or lower compute shape.

7. Click **Next** to navigate to the Review page showing the new compute shape value.

8. Click **Save Changes**.

9. On the Stack Details page, click **Terraform Actions** and select **Plan**.
10. In the Plan dialog, click **Plan**.

11. When the Terraform plan job completes successfully, click **Terraform Actions** and select **Apply**.

12. In the Apply dialog, click **Apply**.

After the Terraform apply job completes, the servers are automatically started. This may take some time.
Backing Up a Block Volume

You can back up a block volume manually, or configure automatic backups.

Topics:
• Backing Up a Block Volume Manually
• Configuring Automatic Block Volume Backups

Backing Up a Block Volume Manually

To back up a block volume manually:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Block Storage and click Block Volumes.
2. At the far right of the row for the block volume for which you want to create a backup, click and select Create Manual Backup.
3. In the Create Block Volume Backup dialog, enter a name for the backup and select the backup type, either Full or Incremental.
4. Click Create Block Volume Backup.

The backup is completed once its icon no longer lists it as CREATING in the volume list.

Configuring Automatic Block Volume Backups

To configure automatic block volume backups:

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Block Storage and click Block Volumes.
2. At the far right of the row for the block volume for which you want to create a backup, click and select Assign Backup Policy.
3. In the Assign Backup Policy dialog, select a policy from the BACKUP POLICY list.
4. Click Assign.

Patching Oracle SOA Suite Instances

It is your responsibility to keep instances up-to-date with the latest software bundle patches.

When you create an instance, it contains all of the latest patches associated with the product. However, instances are not automatically updated with the latest bundle patches from subsequent releases. You are responsible for keeping the instances patch levels current.
Applying bundle patches to existing instances can be complicated. You might have multiple Oracle SOA Suite on Marketplace instances that were provisioned at different times that might include different bundle patches.

Contact Oracle Support for information about the latest Oracle SOA Suite certified patches and instructions on how to apply the patches.

Restoring a Block Volume

You can restore a block volume that has been previously backed up.

To restore a block volume, perform the following steps:

Unmount the Oracle Database File System (DBFS)

> **Note:**

These steps apply only if your DBFS is not mounted on `/u01/soacs`.

1. Use `ssh` to access the Admin VM (as the `opc` user):
   ```
   ssh -i private_key opc@Admin_VM_Public_IP
   ```
2. Enter the following commands:
   ```
   sudo fusermount -u /u01/data/dbfs
   sudo fusermount -u /u01/data/dbfs_directio
   ```

Unmount the old volume

1. Use `ssh` to access the Admin VM (as the `opc` user).
   ```
   ssh -i private_key opc@Admin_VM_Public_IP
   ```
2. Enter the following commands:
   ```
   sudo fdisk -l (Make a note of the `/dev/sdc device)
   df -h (Check that `/u01/data` is mounted)
   sudo umount /u01/data
   df -h (Check that `/u01/data` is not mounted)
   ```

Disable the old volume

For volumes attached with iSCSI as the volume attachment type, you need to disconnect the volume from an instance before you detach the volume.

1. Log on to your instance’s guest OS and unmount the volume.
2. In the Oracle Cloud Infrastructure Console, click `Create` in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Compute** and click **Instances**.
3. Click the name of the instance to display the Instance Details page.
4. In the **Resources** section, click **Attached Block Volumes**.
5. At the far right of the row for the block volume that you want to disconnect, click "..." and select iSCSI Commands & Information.

6. In the iSCSI Commands & Information dialog, copy the DETACH COMMANDS and execute the commands on your Admin VM. These commands will unmount the volume and disconnect the instance from the volume.

Note:

If you see the following error, the unmount was not successful. You need to unmount DBFS mounts from /u01/soacs.

.sudo iscsiadm -m node -T ign.
2015-12.com.oracleiaas:d7ebe8-4ef7-430d-87cd-8127332bb0fd -p 169.254.2.2:3260 -u
Logging out of session [sid: 2, target: ign.
2015-12.com.oracleiaas:d7ebe8-4ef7-430d-87cd-8127332bb0fd,
portal: 169.254.2.2,3260]
iscsiadm: Could not logout of [sid: 2, target: ign.
2015-12.com.oracleiaas:d7ebe8-4ef7-430d-87cd-8127332bb0fd,
portal: 169.254.2.2,3260].
iscsiadm: initiator reported error (28 - device or resource in use)
iscsiadm: Could not logout of all requested sessions

A successful logout response resembles the following:

Logging out of session [sid: 2, target: ign.
2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418,
portal: 169.254.0.2,3260]
Logout of [sid: 2, target: ign.
2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418,
Detach the old volume from Compute

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Compute and click Instances.
2. Click the name of the instance to display the Instance Details page.
3. In the Resources section, click Attached Block Volumes.
4. At the far right of the row for the block volume that you want to disconnect, click and select Detach.
5. In the Detach Block Volume dialog, click Continue Detachment.

Create new volume from backup volume

1. Select the compartment in which the block volume backup you are restoring is saved.
2. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Block Storage and click Block Volume Backups.
3. At the far right of the row for the block volume backup you want to restore, click and select Create Block Volume.
4. In the Create Block Volume dialog, enter a name for the block volume and choose the availability domain in which you want to restore it.
5. Click Create Block Volume.

The volume is ready to attach once its icon no longer lists it as PROVISIONING in the volume list.

Attach the new volume to the SOA instance

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Compute and click Instances.
2. Click the name of the instance to which you want to attach the new volume.

3. In the Resources section, click Attached Block Volumes.

4. Click Attach Block Volume.

5. In the Attach Block Volume dialog, select iSCSI the volume attachment type.

6. For ACCESS, select Read/Write or Read Only - SHAREABLE.

7. In the BLOCK VOLUME COMPARTMENT list, select the compartment.

8. To select the volume you want to attach to by name, select SELECT VOLUME and then select the volume from the BLOCK VOLUME list.

9. Click Attach.

Connect to the new volume

Use the Oracle Cloud Infrastructure Console to obtain the iSCSI data you need to connect the volume.

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Compute and click Instances.

2. Click the name of the instance to display the instance details.

3. In the Resources section, click Attached Block Volumes.
4. At the far right of the row for the block volume that you want to attach, click **iSCSI Commands and Information**.

   ![iSCSI Commands and Information dialog](image)

   The iSCSI Commands and Information dialog displays specific identifying information about your volume and the iSCSI commands you'll need. The commands are ready to use with the appropriate information included.

5. Use `ssh` to access the Admin VM on your SOA instance's OS.

6. Copy and paste the **ATTACH COMMANDS** into your instance session window to connect the volume and configure iSCI to automatically connect to the authenticated block storage volumes after a reboot.

**Mount the new volume**

1. Use `ssh` to access the Admin VM (as the `opc` user).

2. Enter the following commands:
   
   ```bash
   sudo fdisk -l  # Note that the device is on /dev/sdb
   df -h  # Check that /u01/data is not available, then continue.
   sudo mount /dev/sdb /u01/data
   df -h  # Check that /u01/data is mounted
   ```

3. Restart the VM from the Oracle Cloud Infrastructure console to ensure that /u01/data is mounted after restart.

**Mount the Oracle Database File System (DBFS)**

> **Note:**
> These steps apply only if your DBFS is *not* mounted on /u01/soacs

1. Use `ssh` to access the Admin VM (as the `opc` user).
2. Enter the following commands:

```
sudo su - oracle
cd /u01/data/domains/DomainName/dbfs
./dbfsMount.sh -o wallet /@ORCL -o direct_io /u01/data/dbfs_directio
./dbfsMount.sh -o wallet /@ORCL -o direct_io /u01/data/dbfs
df -h Check that /u01/data/dbfs* are mounted
```

3. Restart the VM from the Oracle Cloud Infrastructure console to ensure that /u01/data is mounted after restart. If you see that DBFS is not mounted, then mount DBFS for every restart.

(Optional) Delete the old volume

1. In the Oracle Cloud Infrastructure Console, click in the top left corner. In the navigation menu, under Core Infrastructure, go to Block Storage and click Block Volumes.

2. At the far right of the row for the block volume backup you want to delete, click and select Terminate and confirm when prompted.

Deprovisioning an Oracle SOA Suite Instance

You can deprovision an Oracle SOA Suite instance using the Terraform Destroy action. Optionally, you can also delete the stack.

To deprovision an Oracle SOA Suite instance:

1. To view the Oracle SOA Suite instance you want to deprovision, see Viewing Oracle SOA Suite Instance Details.

2. On the Stack Details page, click Terraform Actions and select Destroy.

3. In the Destroy dialog, click Destroy.
This action deletes the RCU schemas, compute instances, VCNs, subnets, load balancer, and backend servers created during provisioning.

**Note:**

If you subsequently want to re-create the instance using the same stack, select the **Plan** and **Apply** operations from the **Terraform Actions** menu.

4. Optionally, click **Delete Stack**, and click **Yes** when prompted to confirm your selection.

This action deletes the stack entry on the Stacks page in Resource Manager.

**Notes:**

- Deleting the stack cannot be undone.
- Never delete a stack directly from Resource Manager without running the Terraform Destroy action. That is, do not select the **Delete** option from the menu at the far right of the row for the stack. If you accidentally delete a stack using Resource Manager before running the Terraform Destroy action, make sure you delete all the compute instances (in the case of a multinode cluster) and delete the corresponding load balancer instance, if it exists.
Configuring Mail Settings

To configure email settings using User Messaging Service (UMS), UMS must be set up on your SOA servers and the UMS adapter configured for your Oracle SOA Suite instance. You can then configure the User Messaging Service to send emails to SSL-configured external mail servers using Oracle SOA Suite with Oracle Service Bus and Oracle B2B.

Topics:
- Configuring User Messaging Service on a Cluster
- Configuring Mail Sessions

Configuring User Messaging Service on a Cluster

To configure email settings using User Messaging Service (UMS), UMS must be set up on your SOA servers and the UMS adapter configured for your Oracle SOA Suite instance.

If not already done, configure User Messaging Service (UMS) on a cluster:

1. Log in to the Oracle WebLogic Server Administration console.
2. Navigate to Home, then Summary of Deployments.
3. If the UMS adapter is not created, follow the steps in Creating the User Messaging Service JMS Server to create a UMS JMS server.
4. Navigate to Home, then Summary of Deployments, and click UMSJMSSystemResource.
5. Click Lock and Edit if not already in edit mode and then click New.
6. Select Distributed Queue and click Next.
7. Provide the distributed queue name and the JNDI name.

<table>
<thead>
<tr>
<th>Queue Name</th>
<th>JNDI Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMAppDefRcvErrorQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMAppDefRcvErrorQ1</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMAppDefRcvQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMAppDefRcvQ1</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMDriverDefSndQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMDriverDefSndQ1</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMEngineCmdQ_auto</td>
<td>OraSDPM/Queues/OraSDPMEngineCmdQ</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMEnginePendingRcvQ_auto</td>
<td>OraSDPM/Queues/OraSDPMEnginePendingRcvQ</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMEngineRcvQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMEngineRcvQ1</td>
</tr>
<tr>
<td>Queue Name</td>
<td>JNDI Name</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMEngineSndQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMEngineSndQ1</td>
</tr>
<tr>
<td>dist_OraSDPM/Queues/OraSDPMWSRcvQ1_auto</td>
<td>OraSDPM/Queues/OraSDPMWSRcvQ1</td>
</tr>
</tbody>
</table>

8. Select the UMSJMSSubdeployment from the dropdown list. If the subdeployment is not created, follow the steps in Creating a Subdeployment to create the subdeployment.

9. Select the UMSJMSServer and click Finish.

10. Create all the queues given in the table and click Apply.

11. Navigate to Home, then Summary of Deployments and verify if the UMSAdapter deployment is displayed. If the UMSAdapter is not in active state, follow the steps in Deploying a User Messaging Service Adapter to deploy the UMS adapter.

For more information on how to monitor User Messaging Service from Oracle Fusion Middleware Control Console, see Monitoring Oracle User Messaging Service in Administering Oracle User Messaging Service.

Creating the User Messaging Service JMS Server

On a cluster, you need to create two or more UMS JMS servers, one for each of the servers in the cluster.

1. Log in to the Oracle Weblogics Server console.

2. Go to the Summary of JMS servers section and click New.

3. Enter the name of the User Messaging Service JMS server and its scope, and click Next.

4. Select a persistent store from the drop down list and click Next. If the persistent store is not available, follow the steps in Creating a Persistent Store to create a persistent store.
5. Select a target for the UMS JMS server and save the changes.

![Screenshot of UMS JMS server targets]

Repeat the steps for the other UMS servers in the cluster.

Creating a Persistent Store

Create two or more User Messaging Service persistent stores, one for each of the nodes in the cluster.

1. Log in to Oracle Weblogic Server Administration console.
2. In the left pane of the console, expand Services and select Persistent Stores.
3. On the Summary of Persistent Stores page, click New and then Create JDBC Store.
4. On the Create a new JDBC Store page, update the following:
   - **Name** -- Enter a name for the JDBC Store.
   - **Scope** -- Specify the scope of the JDBC Store.
   - **Prefix Name** -- Specify a prefix name to prepend to the table name in this JDBC store for use with multiple instances.
5. Click Finish.

![Screenshot of creating a JDBC store]
Repeat the steps for other persistent stores based on the servers available in the cluster.

Creating a Subdeployment

Configure the mail driver for outgoing mails using the Universal Messaging Server.

1. Log in to Oracle Weblogic Server Administration console.
2. In the left pane of the console, expand Services then Messaging, and select JMS Modules.
3. Expand JMS modules and select UMSJMSSystemResource.
4. Click Test to test the driver configuration.
5. Click the Subdeployments tab and click the New button in the Subdeployments table.
6. On the Subdeployment Properties page, enter a name for the subdeployment and click Next.
7. On the Targets page, select both the UMS JMS servers and click Save.

Deploying a User Messaging Service Adapter

If the User Messaging Service adapter is not in active state, delete and redeploy the adapter.

1. Log in to the Oracle Weblogic Server Administration console.
2. Navigate to Home, then Summary of Deployments.
3. If the User Messaging Service adapter is not in active state, select the check box against the UMSAdapter and click Delete.
4. Click Install, select the UMS Adapter RAR file in the following location: $DOMAIN_HOME/soa/soa/connectors/UMSAdapter.rar.
5. Select the cluster from the available targets, click Next and Finish.
6. Activate all changes.
7. Restart the administration and managed servers. See Starting an Oracle SOA Suite Instance.
Configuring Mail Sessions

You can configure the User Messaging Service to send mails to SSL configured external mail servers using Oracle SOA Suite with Oracle Service Bus and Oracle B2B.

In this example, we'll configure to send mails using the yahoo mail server. Before you configure your Oracle SOA Suite instance and User Messaging Service to send mails, make a note of the yahoo mail server SSL settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>smtp.mail.yahoo.com</td>
</tr>
<tr>
<td>Port</td>
<td>465 or 587</td>
</tr>
<tr>
<td>Requires SSL</td>
<td>Yes</td>
</tr>
<tr>
<td>Requires TLS</td>
<td>Yes (if available)</td>
</tr>
<tr>
<td>Requires authentication</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:**

For Oracle SOA Suite instances using IP networks, verify if a ping to the smtp mail server is working. For example, ping smtp.office365.com. If the ping does not work, manually add the smtp mail server host name in your DNS entry.

**Topics:**

- Importing a CA-Issued SSL Certificate into the Oracle SOA Suite Instance
- Configuring the Mail Driver for Outgoing Mails
- Updating the Workflow Notification Properties
- Verifying Mail Configuration Settings

**Importing a CA-Issued SSL Certificate into the Oracle SOA Suite Instance**

The first step is to import the CA-issued SSL certificate into the trust store being used in your server.

1. Log in to the Admin server node as an Oracle user.
2. Execute the following openssl command:
### Email Server and Command Used

<table>
<thead>
<tr>
<th>Email Server</th>
<th>Command Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>openssl s_client -connect smtp.mail.yahoo.com:465 &gt; yahoocert.pem</td>
</tr>
<tr>
<td>Office 365</td>
<td>openssl s_client -showcerts -starttls smtp -crlf -connect smtp.office365.com:587</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>openssl s_client -showcerts -starttls smtp -connect smtp-mail.outlook.com:587</td>
</tr>
<tr>
<td>Gmail</td>
<td>openssl s_client -connect smtp.gmail.com:465 &gt; gmail-smtp-cert.pem</td>
</tr>
</tbody>
</table>

3. Make a copy of yahoocert.pem file. For example, `cp yahoocert.pem yahoo.cer`.

   a. Run the following command:

      ```
      Vi yahoo.cer
      ```

      The certificate is displayed.

   b. Keep only the certificate from **BEGIN CERTIFICATE** entry till **END CERTIFICATE** entry and remove all the unwanted lines to create the yahoo certificate.

   ![Note:](img)

   **Note:**

   In the case of **Office 365**, two certificates are presented. Run the following command to display the certificates:

   ```
   openssl s_client -showcerts -connect smtp.office365.com:587 -starttls smtp  </dev/null
   ```

   Save both the certificates as individual .cer files and import them to the keystore.

4. Add the certificate to the trust store being used in your admin server. By default the trust store used is **Demotrust.jks**. Use the following command to add the certificate created in the previous step to **Demotrust.jks**:

   ```
   keytool -import -alias smtp.yahoo.com -keystore /u01/app/oracle/middleware/wlserver/server/lib/DemoTrust.jks -file yahoo.cer -storepass DemoTrustKeyStorePassPhrase
   ```
5. Stop and then restart the admin and managed servers.

Configuring the Mail Driver for Outgoing Mails

Configure the mail driver for outgoing mails using the User Messaging Service.

1. In Oracle Enterprise Manager Fusion Middleware Control, navigate to User Messaging Server.
2. Expand the User Messaging Service node and select usermessagingdriver-email.

3. Enter the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Email driver name. For example, yahooss1</td>
</tr>
<tr>
<td>Sender address</td>
<td>EMAIL:<a href="mailto:YourMail@yahoo.com">YourMail@yahoo.com</a></td>
</tr>
<tr>
<td>Capability</td>
<td>Send</td>
</tr>
<tr>
<td>EMAIL Receiving protocol</td>
<td>IMAP</td>
</tr>
<tr>
<td>Message Retrieval Frequency</td>
<td>30</td>
</tr>
<tr>
<td>Message Folder</td>
<td>INBOX</td>
</tr>
<tr>
<td>Outgoing mail Server port</td>
<td>smtp.mail.yahoo.com</td>
</tr>
</tbody>
</table>
### Configuring Mail Sessions

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing Mail Server port</td>
<td>465</td>
</tr>
<tr>
<td>Outgoing Mail Server Security</td>
<td>SSL</td>
</tr>
<tr>
<td>Outgoing Username</td>
<td>Your email user name which you give for authentication. For Office 365, test the driver settings to verify that your email user name is a fully qualified name as Office 365 requires the user name in your SMTP configuration to be your full email address including the domain. For example, <a href="mailto:myuser@mydomain.com">myuser@mydomain.com</a>.</td>
</tr>
<tr>
<td>Outgoing Password</td>
<td>Your email password in cleartext password type. Note that Office 365 requires users to change their passwords regularly. The SMTP service may not notify you about expired passwords. Double-check the password provided in the driver configuration.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Select this option</td>
</tr>
</tbody>
</table>

4. Click **Test** to test the driver configuration.

**Note:**

If test fails with authentication failure, log into your mail ID and check for a mail from Yahoo or your mail server with a subject similar to “Sign in attempt prevented”. Perform the steps mentioned in the email to enable less secure sign in.

### Updating the Workflow Notification Properties

Update the workflow notification properties with details of the external mail server.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.
2. Expand the **SOA** node and select **soa-infra**.
3. Right-click **soa-infra**, select **SOA Administration** and then **Workflow Properties**.
4. In the Mailer tab, under Notification Service, enter **From Address**, **Actionable Address**, and **Reply To Address** for your outgoing mail address. For example, YourMail@yahoo.com.

5. Click **Apply**.

**Verifying Mail Configuration Settings**

You can test your mail server configuration by sending a test mail.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.
2. Expand the SOA node and select soa-infra.
3. Right-click soa-infra, select SOA Administration and then Workflow Properties.
4. Click the arrow next to SOA Infrastructure, select Service Engine and then Human Workflow.

5. Click the Notification Management tab and click Send Test Notification.
6. Enter the details of the mail ID to which you want to send the test mail and click Send.

A successful mail delivery is sent to the intended recipient.
Troubleshooting Oracle SOA Suite on Marketplace

These topics describe how to troubleshoot problems you might encounter while using Oracle SOA Suite on Marketplace.

Topics:
- Finding Diagnostic Information to Help with Troubleshooting
- Problems Accessing the Worklist Application from Enterprise Manager
- Problems with Failure of a Running Service When the Schema User Password Expires
- Problems with Connectivity
- Problems with the Node Manager
- Problems with Database File System Mounting on Second Managed Server Node
- Problems with a Database Deployment
- Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control

Finding Diagnostic Information to Help with Troubleshooting

You can use the WebLogic Administration Console and other tools to find more information about problems with Oracle SOA Suite on Marketplace and help you troubleshoot them.

Topics:
- Using the WebLogic Server Administration Console to Find Diagnostic Information
- Using the WebLogic Server Administration Console to Find Log Files

Using the WebLogic Server Administration Console to Find Diagnostic Information

You can find diagnostic information easily by using the WebLogic Server Administration Console.

To find diagnostic information:
1. Open the WebLogic Administration Console. To find the URL, see Accessing an Oracle SOA Suite Instance.
2. Click the menu icon and select WebLogic Server Console.
   A new browser opens and you are redirected to the WebLogic Server Administration Console’s login page.
If the console is protected by a self-signed certificate, you will be warned that this certificate is not trusted.

3. Accept the certificate.

4. When the console log-in page appears, enter the log-in credentials you entered for the WebLogic Administrator when you created the service instance.
   The WebLogic Administration Console is displayed.

5. In the Domains area, expand **Diagnostics**.

6. Click on the diagnostics that interests you.
   For information on the diagnostic choices, click on **Diagnostics**.

**Using the WebLogic Server Administration Console to Find Log Files**

You can find log files easily by using the WebLogic Server Administration Console.

To find the log files:

1. Open the WebLogic Administration Console. To find the URL, see Accessing an Oracle SOA Suite Instance.

2. In the Domains area, expand **Diagnostics**.

3. Click **Log Files**.

4. The Log Files table is displayed.

5. Click the option to the left of the log file you want to view.

6. Click **View**.

7. The log file you selected is displayed in the table.

8. (Optional) If you do not find the information you are looking for, customize the table to select the time interval you want to view.
   a. View the log file.
   b. Click the **Customize this table** link above the log file.
   c. From the Time Interval drop-down menu, select the time interval for filtering the information in the table.

     You can choose an interval ranging from the last five minutes to the last one week. You can also view all log entries or customize the time interval.

**Problems Accessing the Worklist Application from Enterprise Manager**

When deploying an Oracle SOA Suite on Marketplace application from Oracle Enterprise Manager Fusion Middleware Control, clicking the **Go To Worklist Application** button does not open the Worklist Application as expected.

To work around this issue


2. Select the task and approve it.
Problems with Failure of a Running Service When the Schema User Password Expires

An Oracle SOA Suite on Marketplace instance can fail suddenly and issue password expiry error messages.

This failure occurs because the user password for the infrastructure repository schemas is set to expire in 180 days after an Oracle SOA Suite on Marketplace instance is created. You see the following error messages:

Received exception while creating connection for pool X: ORA-28001: the password has expired

java.sql.SQLException: ORA-01017: invalid username/password; logon denied

Note:

By default the schema password is set to Weblogic Administrator password during the provisioning of the JCS instance.

You must be able to log onto the VM that hosts the WebLogic Server Administration Server as opc. Doing so allows you to sudo as oracle. All actions on files on the VM that hosts the Administration Server or VMs that host Managed Servers should be executed as oracle.

The following summary shows the high-level steps to perform. Detailed steps are below.

1. Update each infrastructure repository schema's password on the database deployment.

2. If WebLogic Servers are running and the WebLogic Server Console is accessible, change the password for all the corresponding datasources from the Weblogic Administration Console.

3. If WebLogic Servers are not running and WebLogic Server Console is inaccessible, manually change the passwords in WebLogic Server configuration.

4. Run offline WLST command modifyBootStrapCredential.

5. Start the Administration Server through Node Manager, and then start the Managed Servers.

Detailed steps:

1. Update each infrastructure repository schema's password on the database deployment.

   If the schema prefix is already known, go to Step b.

   a. Connect to the Oracle SOA Suite on Marketplace Instance VM that hosts the Administration Server, and get the value of the schema prefix.

      ```
      ssh -i private_key opc@IP_address_of_admin_server_VM
      sudo su oracle curl http://192.1.1.192/latest/user-data/chef/initial_attributes/wlss/schema_prefix
      ```
The Schema Prefix value returned would be similar to the following:
SP255951777

b. Log in to the Oracle Cloud Infrastructure database deployment VM.

```
ssh -i ssh_key opc@DB_vm_ip_address
sudo su oracle
```

c. Connect to the Oracle Cloud Infrastructure database deployment.

```
sqlplus / as sysdba
```

Use the username provided when provisioning the database deployment.

If your database deployment version is 12c, the following step is also required:
```
alter session set container=PDB1
```

Use the PDB name provided during Oracle SOA Suite provisioning.

d. Change the password for the infrastructure repository schema users.

```
ALTER USER schema_prefix_IAU identified by new_password;
```

e. Unlock all the user accounts on the database to cover for the case that they are locked due to repeated login failures after password expiry.

```
ALTER USER schema_prefix_IAU ACCOUNT UNLOCK;
```

---

**For Fusion Middleware 12.2.1.x**

```
schema_prefix_IAU
schema_prefix_IAU_APPEND
schema_prefix_IAU_VIEWER
schema_prefix_MDS
schema_prefix_OPSS
schema_prefix_STB
schema_prefix_UMS
```

Change the password for each of the schema users pertaining to the WebLogic Server version on the database deployment. For example:
```
ALTER USER schema_prefix_IAU identified by new_password;
```

---

**Note:**

If the WebLogic Administration Server is running and the WebLogic Administration Console is accessible, follow Step 2, else go to Step 3.

2. Update all the datasources from the WebLogic Administration Console to reflect the new password.

   a. Log in to the WebLogic Administration Console and navigate to the Services — Datasources menu on the Domain Structure box.

   b. Click **Lock & Edit**.

   c. For each datasource, navigate to the **Datasource Name — Configuration — Connection Pool** tab and update the **Password** and **Confirm Password** fields with the new password.

   d. Click on **Save** button on this page, and then **Activate**.
e. Stop all the WebLogic Servers.
   From the WebLogic Administration Console, navigate to the **Environment > Servers > Control** tab.
   Select all the servers and click **Shutdown —Force Shutdown Now**.
   Proceed to Step 4.

3. If the WebLogic Server is not running or the Administration Console is not accessible:
   a. Encrypt the new schema password and update datasource configuration files.
      ```bash
      scp -i private_key opc@ipaddress_of_Admin_VM
      sudo su oracle
      cd /u01/data/domain/domain_name
      Ensure WebLogic Servers are not running. If running, stop the processes.
      Find the process IDs:
      ps -ef | grep java
      Kill processes:
      kill -9 pid
      then run:
      . domain_home/bin/setDomainEnv.sh
      ```

   b. Run the WebLogic Encryption Utility and enter the password you set for the database schemas.
      ```bash
      /u01/jdk/bin/java weblogic.security.Encrypt password: new_password
      ```

   c. Note the encrypted password output for future reference.
      The following example shows an encrypted password:
      ```text
      AES}JHyrhOMB5hVRuDU/pV0qX86qz98ZV0xWXBSEAAAN4Gs=
      ```

   d. Update the new password in the datasource XML files.
      ```bash
      cd domain_home/domain_name/config/jdbc
      Open the datasource XML files found in the domain_home/domain_name/config/jdbc directory that need to be updated with the new encrypted password:
      ```

**For Fusion Middleware 12.2.1.x**

- LocalSvcTblDataSource-jdbc.xml
- opss-auditview-jdbc.xml
- mds-owsm-jdbc.xml
- opss-datasource-jdbc.xml
- opss-audit-jdbc.xml

4. Run the **Modify BootStrapCredential WLST command** to update `jps-config.xml` with the new password for **SCHEMA_PREFIX_OPS** user.
   a. Connect to the Oracle SOA Suite VM hosting the Administration Server.
      ```bash
      ssh -i private_key opc@IP_of_admin_server
      ```
sudo su oracle

b. Invoke WLST.
   `/u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh`

c. Run the modifyBootStrapCredential command to update the jps-config file with the new password for the schema user.

   **Note:**
   The full path to the JPS configuration file must be specified.

   Use the following syntax:
   `wls:offline>modifyBootStrapCredential(jpsConfig_File=domain_home/domain_name/config/fmwconfig/jps-config.xml,username=prefix_OPSS,password=new_password_set_for_this_schema_user)`

5. Start the Administration Server through the Node Manager and then the Managed Server(s).

   a. Log in to the Oracle SOA Suite VM hosting the WebLogic Administration Server.

   b. Start WLST.
      `/u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh`

   c. Connect to the Node Manager.
      Before running the command, get the required values of some of the variables involved.
      - Host name — At the command prompt, type `hostname`.
      - Node Manager port number, domain name, domain home — Open the nodemanager.properties files to determine the respective values:
        `/u01/data/domains/domain_name/nodemanager/nodemanager.properties`
      - Administration Server name — Enter the following command:
        `cd /u01/data/domains/domain_name/servers`
        Look for the server name ending in adminserver.
      Run the `nmConnect` command.
      `nmConnect('weblogic_username','weblogic_password','hostname','domain_name','domain_home/domain_name','ssl')`

   d. Start the Administration Server.
      `nmStart("admin_server_name")`

   e. If the Administration Server has status RUNNING, access the WebLogic Administration Console and start the Managed Servers.
      - Click on `Servers` under `Environments` in the `Domain Structure` section.
      - Under the `Control` tab, select the Managed Servers and click `Start`. 
The password expiry problem has been fixed.

## Problems with Connectivity

Problems might occur when you attempt to connect to an Oracle SOA Suite on Marketplace instance.

The following solutions apply to problems with connectivity to an Oracle SOA Suite on Marketplace instance.

### My private key is lost or corrupted

When you create an Oracle SOA Suite on Marketplace instance you must provide an SSH public key. You will be unable to establish an SSH connection to the VMs that comprise the service instance unless you provide the matching SSH private key, as described in Accessing a VM Through a Secure Shell (SSH).

Perform the following steps:

1. Create a new pair of SSH keys.
2. Add the new SSH public key to your existing Oracle SOA Suite on Marketplace instance.
3. SSH to the VMs in your service instance by using the new SSH private key.

### My connection to a VM is refused

Be sure you are connecting to the VM as the opc user. Other OS users such as oracle and root cannot be used to establish a remote connection to a VM. After successfully connecting to a VM as opc, you can switch to a different user. See Accessing a VM Through a Secure Shell (SSH).

### I received a hostname verification error when attempting to connect to Node Manager

When attempting to connect to the Node Manager using WLST, a hostname verification error is returned, similar to the following:

```
WLSTException: Error occurred while performing nmConnect : Cannot connect to Node Manager. : Hostname verification failed:
@HostnameVerifier=weblogic.security.utils.SSLWSHostnameVerifier, hostname=myjcs1-wls-1.
```

To disable hostname verification, use the following -D flag when invoking WLST:

```
java -Dweblogic.SSL.ignoreHostnameVerification=true weblogic.wlst
```

## Problems with the Node Manager

Problems may occur if you are trying to restart the Administration Server through the Node Manager.

When you check to see whether the Node Manager is running, you could find that it is not running.
When I try to restart the Administration Server, I discover that the Node Manager is not running

To restart the Node Manager:

1. Use an SSH client of your choice to access the VM of the Administration Server. If you do not have an SSH client on Windows, you can use PuTTY to access the VM by establishing an SSH tunnel.
   If you are not automatically logged in as user opc, log in accordingly.
2. In the command window, change to user oracle.
   sudo su - oracle
3. Change directories to where startNodeManager.sh exists.
   /u01/data/domains/domain_name/bin
   For example:
   cd /u01/data/domains/OurService_domain/bin
4. Start the Node Manager:
   nohup startNodeManager.sh
5. Check to see that the Node Manager is running:
   ps -ef | grep NodeManager
   You should receive messages showing that the Node Manager is running.
6. (Optional) If you have more than one host in your Oracle SOA Suite on Marketplace instance, you must restart the Node Manager on each host.
   a. SSH to the second host:
      ssh hostname
      For example:
      ssh ourserviceinstance-wls-2
   b. Change directories to where startNodeManager.sh exists.
      /u01/data/domains/domain_name/bin
      For example:
      cd /u01/data/domains/OurService_domain/bin
   c. Start Node Manager:
      nohup startNodeManager.sh
   d. Check to see whether the Node Manager is running:
      ps -ef | grep NodeManager
      You should receive messages showing that the Node Manager is running.
   e. Exit the second host:
      exit
7. Exit the oracle session:
   exit
8. Exit out of the command window:

   exit

Problems with Database File System Mounting on Second Managed Server Node

When you mount Oracle Database File System on non-Administration pods, Oracle Database File System mounts on the first managed server node but not on the second managed server node.

To mount Oracle Database File System on the second managed server node:

1. Log in to the scaled out Virtual Machine or the Virtual Machine where you have created two or more node clusters. For example:

   `ssh -i opc_rsa opc@123.123.12.34`

2. In the command window, change to user `oracle`.

   `sudo su - oracle`

3. Copy the existing workaround script to the `/tmp` directory.

   `cp /u01/data/domains/<domain>/dbfs/dbfswa.sh /tmp`


   `chmod 777 /tmp/dbfswa.sh`

5. Change from `oracle` to `opc` user.

   `sudo su - opc`

6. Run the workaround script from tmp directory

   `cd /tmp/
    ./dbfswa.sh`

Verify Oracle Database File System on Second Managed Server Node

1. In the command window, change to user `oracle`.

   `sudo su - oracle`

2. Run the following commands:

   • `df -h`
   • `touch /u01/soacs/dbfs/share/test`

3. `ssh` to AdminServer Virtual Machine.

   `ssh -i opc_rsa opc@AdminServer_IP`

4. List the file that was touched on Virtual Machine 2. `ls -ltr /u01/soacs/dbfs/share/`

   If you see the test file on Virtual Machine 1, then mount on second managed server node and file sharing is successful on Oracle Database File System.
Problems with a Database Deployment

Problems related to the database deployment used by Oracle SOA Suite on Marketplace can occur.

Creating an opss datasource fails
An attempt to create an opss datasource can fail because the database deployment's opss user account is locked.

To unlock the opss user account:

1. Log in to the database deployment's VM by using the private key.
   
   ```
   ssh -i private-key opc@ip-address-of-db-vm
   ```

2. Change to user oracle.
   
   ```
   cd $ORACLE_HOME/bin
   ```

3. Start sqlplus.
   
   ```
   ./sqlplus
   ```

4. Log in using the system user, and enter the password.
   
   ```
   Enter user-name: system
   Enter password: system_user_password
   ```

5. Unlock the account.
   
   ```
   ALTER USER schema_prefix_opss ACCOUNT UNLOCK;
   ```

6. Change the password.
   
   ```
   ALTER USER schema_prefix_opss IDENTIFIED BY new_password;
   ```

7. Exit sqlplus.
   
   ```
   exit
   ```

Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control

You can experience problems opening the WebLogic Server Administration Console from Fusion Middleware Control.

You can use the WebLogic Server Administration Console and Fusion Middleware Control to administer Oracle SOA Suite on Marketplace instances. If you attempt to
open the WebLogic Server Administration Console from the Fusion Middleware Control Console, the console will not open and you will receive an error message:

The Host is not resolvable. Most commonly this is due to mistyping the URL in the browser bar. Please verify the spelling and that the site exists and hit refresh.

The problem occurs three ways.

From the Deployments tile:
1. Click on the Deployments tile.
2. Click the name of your deployed application.
3. From the Domain Application Deployment drop-down menu, select Administration — General Settings.
4. Select the Instrumentation tab.
5. In “To configure Instrumentation, use the WebLogic Server Administration Console,” click Weblogic Server Administration Console.

The error message appears in a new browser tab.

From the WebLogic Domain drop-down menu:

• From the WebLogic Domain drop-down menu, select WebLogic Server Administration Console.

The error message does not appear, but neither does the WebLogic Service Administration Console.

When administering a security realm from the WebLogic Domain drop-down menu:
2. Select myrealm.
4. Click WebLogic Server Administration Console.

The error message appears in a new browser tab.

By design, Fusion Middleware Control has a URL composed of the hostname and HTTP port 7001 for the console. In the Oracle Java Cloud Service environment, only HTTPS port 7002 is enabled and accessible because it is a secure port. Additionally, the Administration Server VM host is not DNS resolvable to its IP address because the IP address is a public NAT IP address.

Use the HTTPS protocol, NAT IP address instead of host name, and port 7002 to access the console, for example:

https://198.51.100.1:7002/console