

# Oracle® Cloud

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



F25561-89  
May 2024



Oracle Cloud Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure,

F25561-89

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

Primary Author: Oracle Corporation

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

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

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

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

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

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

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

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

# Contents

## 1 What's New in Oracle SOA Suite on Marketplace

---

## 2 Get Started with Oracle SOA Suite on Marketplace

---

About Oracle SOA Suite on Marketplace	2-1
Differences Between Oracle SOA Cloud Service and Oracle SOA Suite on Marketplace	2-2
Differences Between Oracle SOA Suite On-Premises and Oracle SOA Suite on Marketplace	2-3
About the Oracle SOA Suite on Marketplace License	2-4
About the Components of Oracle SOA Suite on Marketplace	2-5
About the Components of Oracle Cloud Infrastructure Used By Oracle SOA Suite on Marketplace	2-8
About Life Cycle Management of Oracle SOA Suite on Marketplace Instances	2-9
Typical Workflow for Managing the Life Cycle of Oracle SOA Suite on Marketplace Instances	2-10
About Oracle SOA Suite on Marketplace Roles and User Accounts	2-11
About Adapters for Oracle SOA Suite on Marketplace	2-11
About Managing Oracle SOA Suite on Marketplace Instances	2-13
About Security for Oracle SOA Suite on Marketplace Instances	2-14
About Managing Patches for Instances Provisioned With Earlier Releases	2-15
About Oracle SOA Suite on Marketplace Roles and Responsibilities between Oracle and Customer	2-17

## 3 Before You Begin

---

Understand Oracle SOA Suite on Marketplace Topologies	3-1
Sign in to the Oracle Cloud Infrastructure Console	3-3
Prerequisites	3-4
Create a Compartment	3-6
Set Up a Virtual Cloud Network	3-7
Configure Security Lists	3-8
Generate a Secure Shell (SSH) Public/Private Key Pair	3-10
About SSH Keys	3-11
Generate an SSH Key Pair on UNIX and UNIX-Like Platforms Using the ssh-keygen Utility	3-11

Generate an SSH Key Pair on Windows Using the PuTTYgen Program	3-12
Create an Oracle Database for Oracle SOA Suite on Marketplace	3-13
Create an Oracle Cloud Infrastructure Database for Oracle SOA Suite on Marketplace	3-15
Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Suite on Marketplace	3-16

## 4 Create and View Oracle SOA Suite on Marketplace Instances

---

Provision an Oracle SOA Suite on Marketplace Instance	4-1
Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console	4-2
Provision an Oracle SOA Suite on Marketplace Quick Start Instance	4-20
Provision an Oracle SOA Suite on Marketplace Instance Using the Oracle Cloud Infrastructure Command Line Interface	4-25
Install the Command Line Interface	4-25
Configure the Command Line Interface	4-29
Start the Command Line Interface	4-29
Use CLI Commands to Provision an Oracle SOA Suite on Marketplace Instance	4-29
Provision an Oracle SOA Suite on Marketplace Instance Using Oracle Cloud Infrastructure REST APIs	4-34
Create a Database	4-34
Create a Stack	4-35
Create a Plan Job	4-37
Create an Apply Job	4-38
Complete Post-Provisioning Tasks	4-39
Add Ingress Rules to Access WebLogic Server Administration and Other Consoles	4-40
Add an Ingress Rule to Allow ssh Access to SOA Servers	4-42
Restart Servers for a Multinode Cluster	4-43
Add a Managed Server IP in a Non-Proxy Host to Enable Deployment from Fusion Middleware Control	4-43
Complete Post-Provisioning Tasks for an MFT Cluster Service Type	4-46
Add an Ingress Rule to Allow sFTP Traffic to sFTP Servers	4-47
Configure the SSH Keystore for the MFT sFTP Server	4-47
Enable and Start the MFT sFTP Server	4-48
Connect to MFT Embedded Servers Using the Load Balancer	4-50
Configure Scheduled Backups	4-51
Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure	4-51
Register a Custom Domain Name with a Third-Party Registration Vendor	4-55
View Oracle SOA Suite on Marketplace Instance Details	4-55
Access an Oracle SOA Suite on Marketplace Instance	4-56
Migrate or Upgrade to an Oracle SOA Suite on Marketplace Instance	4-58
Migrate Oracle SOA Cloud Service Instances to Oracle SOA Suite on Marketplace Using the Migration Manager	4-59

Prerequisites for Migration	4-59
Generate the Migration Report	4-61
Run the Migration Manager	4-64
Delete the Oracle SOA Suite on Marketplace RCU Schemas	4-67
Update Oracle SOA Suite on Marketplace Stack Variables	4-67
Rollback Migration	4-68
Frequently Asked Questions About the Oracle SOA Suite Migration Manager	4-69

## 5 Deploy Applications for Oracle SOA Suite on Marketplace

---

Deploy and Undeploy Applications for an Oracle SOA Suite on Marketplace Instance	5-1
Overview of Deployment Tasks for an Oracle SOA Suite on Marketplace Instance	5-1
Use Oracle JDeveloper to Deploy Applications	5-2
Add an Ingress Rule to Allow the JDeveloper Connection	5-2
Create an Application Server Connection in JDeveloper	5-4
Deploy a SOA Composite Application to Oracle SOA Suite on Marketplace from JDeveloper	5-8
Deploy an Oracle Service Bus Application to Oracle SOA Suite on Marketplace from JDeveloper	5-11
Use Oracle Enterprise Manager Fusion Middleware Control to Deploy an Application	5-13
Use the WebLogic Server Administration Console to Deploy and Undeploy an Application	5-13
Use the WebLogic Server Administration Console to Start an Application	5-13
Use the WebLogic Server Administration Console to Undeploy an Application	5-14
Use WLST Commands to Deploy and Undeploy an Application	5-14
Access an Application Deployed to an Oracle SOA Cloud Service Instance	5-14
Use a Shared File System	5-15
Access the WSDL of a Composite Deployed to a SOA Server	5-17
Use the Frontend Host and HTTPS Port Values in the WSDL URL for Inbound Cloud Adapters	5-17

## 6 Manage Oracle SOA Suite on Marketplace Instances

---

Edit an Oracle SOA Suite on Marketplace Instance	6-1
Add or Delete a Load Balancer Post-Provisioning	6-2
Configure an Existing Load Balancer for a Provisioned Instance	6-3
Add a New Load Balancer in a New Subnet	6-12
Add a New Load Balancer in an Existing Subnet	6-16
Delete a Load Balancer When Added in a New Subnet	6-17
Delete a Load Balancer When Added in an Existing Subnet	6-21
Access a VM Through a Secure Shell (SSH)	6-21
Connect to the Administration Server VM	6-22
Connect to a Managed Server VM	6-24

Create an SSH Tunnel	6-27
Change VM Users	6-29
Access a VM Through Virtual Network Computing (VNC)	6-30
Access a VM Through PuTTY	6-31
Run WLST Commands on a VM	6-33
Perform Lifecycle Operations on an Oracle SOA Suite on Marketplace Instance	6-34
Disable Server Restart During an Instance Reboot	6-34
Stop or Start an Oracle SOA Suite on Marketplace Instance and Servers	6-34
Stop or Start an Oracle SOA Suite on Marketplace Instance	6-35
Stop or Start WebLogic Servers	6-36
Scale an Oracle SOA Suite on Marketplace Instance Cluster Out or In	6-38
Scale Out an Oracle SOA Suite on Marketplace Instance Cluster	6-39
Scale In an Oracle SOA Suite on Marketplace Instance Cluster	6-42
Scale an Oracle SOA Suite on Marketplace Instance Up or Down	6-44
Back Up the Domain Home	6-45
Restore the Domain Home	6-46
Back Up a Block Volume	6-48
Back Up a Block Volume Manually	6-48
Configure Automatic Block Volume Backups	6-48
Restore a Block Volume	6-48
Deprovision an Oracle SOA Suite on Marketplace Instance	6-54
Perform Database Operations for an Oracle SOA Suite on Marketplace Instance	6-56
Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database	6-56
Discover the Default Database Schema Prefix and Password	6-59
Change the Database Schema and Wallet Passwords	6-60
Update the Database Schema Password	6-60
Update the DBFS Wallet Password	6-66
Create a Data Source for an Oracle Autonomous Transaction Processing Database	6-68
Download the ATP Wallet	6-69
Configure a Data Source for an ATP Database	6-70
Unmount and Mount DBFS	6-71
Increase the Domain Volume Size Post-Provisioning	6-73
Update the JVM Heap Size Parameter Values for Managed Servers	6-74
Enable OS Management for Oracle SOA Suite on Marketplace Instances	6-74
Perform a JNDI Lookup of JMS Resources Deployed on the Administration Server	6-76
Unmount and Mount File Storage Service	6-76

## 7 Secure an Oracle SOA Suite Instance

---

About Security in Oracle SOA Suite on Marketplace	7-1
Set Up Oracle SOA Suite to Use CA-Verified SSL Certificates (without load balancer)	7-1

Register a Domain Name for Oracle SOA Suite	7-2
Create Custom Identity and Custom Trust Keystores and Generate a CSR	7-2
Share the CSR with CA to Get CA-Signed Certificates	7-3
Import CA Certificates	7-4
Synchronize the Local Keystore with the Security Store	7-6
Update WebLogic Keystores with Custom Identity and Trust	7-7
Update the Node Manager and boot.properties File	7-9
Verify the Environment	7-10
Set Two-Way SSL Authentication	7-11
Import Certificates of External Web Services with HTTPS in Oracle SOA Suite	7-11
Export the Certificate Chain of the HTTPS WSDL Called in Oracle SOA Suite	7-12
Import the Certificate Chain of the HTTPS WSDL Called in the Oracle SOA Suite Trust Store	7-12
Import the Certificate Chain of the HTTPS WSDL Called in the Java Trust Store	7-14
Restart the Administration and Managed Servers	7-14
Troubleshoot Issues	7-14

## 8 Configure Mail Settings

---

Configure User Messaging Service on a Cluster	8-1
Create the User Messaging Service JMS Server	8-2
Create a Persistent Store	8-3
Create a Subdeployment	8-4
Deploy a User Messaging Service Adapter	8-4
Configure Mail Sessions	8-4
Import a CA-Issued SSL Certificate into the Oracle SOA Suite on Marketplace Instance	8-5
Configure the Mail Driver for Outgoing Mails	8-6
Update the Workflow Notification Properties	8-8
Verify Mail Configuration Settings	8-9

## 9 Troubleshoot Oracle SOA Suite on Marketplace

---

Find Diagnostic Information to Help with Troubleshooting	9-1
Use the WebLogic Server Administration Console to Find Diagnostic Information	9-1
Use the WebLogic Server Administration Console to Find Log Files	9-2
Problems Using IDCS as the Authentication Provider	9-2
Problems with Oracle Business Activity Monitoring (BAM)	9-2
Problems Accessing the Worklist Application from Enterprise Manager	9-3
Problems with Failure of a Running Service When the Schema User Password Expires	9-3
Problems with Connectivity	9-4
Problems with the Node Manager	9-4
Problems with Database File System Mounting on Second Managed Server Node	9-6

Problems with a Database Deployment	9-7
Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control	9-7

## A Patches Installed By Release

---

Patches Applied During Provisioning — 24.1.2	A-2
Patches Applied During Provisioning — 23.4.2	A-3
Patches Applied During Provisioning — 23.3.2	A-4
Patches Applied During Provisioning — 23.2.2	A-4
Patches Applied During Provisioning — 23.1.1	A-5
Patches Applied During Provisioning — 22.4.1 and 22.4.2	A-7
Patches Applied During Provisioning — 22.3.1	A-8
Patches Applied During Provisioning — 22.2.2.1 and 22.2.3.1	A-9
Patches Applied During Provisioning — 22.1.2.1 and 22.2.1.1	A-10
Patches Applied During Provisioning — 22.1.1.2	A-11
Patches Applied During Provisioning — 21.4.5	A-12
Patches Applied During Provisioning — 21.4.1 and 21.4.3	A-13
Patches Applied During Provisioning — 21.3.2 and 21.3.2.1	A-14
Patches Applied During Provisioning — 21.2.2 and 21.2.3	A-15
Patches Applied During Provisioning — 21.2.1	A-16
Patches Applied During Provisioning — 21.1.2 and 21.1.3	A-17
Patches Applied During Provisioning — 21.1.1	A-18
Patches Applied During Provisioning — 20.4.3	A-19
Patches Applied During Provisioning — 20.4.2 and 20.4.2.1	A-20
Patches Applied During Provisioning — 20.3.3 and 20.3.3.1	A-21
Patches Applied During Provisioning — 20.3.2	A-22
Patches Applied During Provisioning — 20.3.1.1	A-23
Patches Applied During Provisioning — 20.3.1	A-23
Patches Applied During Provisioning — 1.0.11.1	A-24



# Preface

*Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure* describes how to provision and administer Oracle SOA Suite 12c (12.2.1.4) on Marketplace in Oracle Cloud Infrastructure.

## 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**

## Audience

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

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <https://www.oracle.com/corporate/accessibility/>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <https://support.oracle.com/portal/> or visit [Oracle Accessibility Learning and Support](#) if you are hearing impaired.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Related Resources

For more information, see:

- Oracle SOA Suite documentation for 12c (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.

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

# 1

## What's New in Oracle SOA Suite on Marketplace

Learn about the new and changed features in Oracle SOA Suite on Marketplace.

For information about the patches that are installed when you provision a new Oracle SOA Suite on Marketplace instance, see [Patches Installed By Release](#).

### March 2024 — Release 24.1.2

Features and Updates	Description
January 2024 CPU patch updates.	This release includes the January 2024 CPU patch updates.
Support for choosing the load balancer compartment during provisioning.	During provisioning of a new Oracle SOA Suite on Marketplace instance, if you selected <b>Provision Load Balancer</b> , you can select the compartment to create a new load balancer or choose an existing load balancer. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
No longer support Oracle Database 12c.	The Oracle SOA Suite on Marketplace will no longer support Oracle Database 12c. See <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a> .

### December 2023 — Release 23.4.2

Features and Updates	Description
October 2023 CPU patch updates.	This release includes the October 2023 CPU patch updates.
New tab added to the Stack Details page.	A new tab named <b>Application Information</b> is added to the Stack Details page. The tab displays the Oracle SOA Suite on Marketplace instance details such as Service Type, SOAMP Cluster Size, SOAMP Stack Version, and so on. See <a href="#">View Oracle SOA Suite on Marketplace Instance Details</a> .
Support for adding multiple tags to the instance during provisioning.	During provisioning of a new Oracle SOA Suite on Marketplace instance, you can create and add multiple tags to the instance. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Support for editing tags post-provisioning.	You can update or delete tags of a Oracle SOA Suite on Marketplace instance post-provisioning. See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a> .

Features and Updates	Description
When provisioning in a private subnet, if you choose to create a Bastion VM, it will use an Oracle Linux 7.x image.	See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .

 **Note:**

The Oracle Linux 7.x image is free to use. Customers are charged only for the OCPU and the memory resources provisioned.

### August 2023 — Release 23.3.2

Features and Updates	Description
July 2023 CPU patch updates.	This release includes the July 2023 CPU patch updates.

### June 2023 — Release 23.2.2

Features and Updates	Description
New provisioning option for adding custom ATP service level.	<p>A new option <b>Custom Service Level</b> is available in the <b>Autonomous Database Service Level</b> drop-down list.</p> <p>A new field <b>Custom Autonomous Database Service Level</b> is exposed when you select <b>Custom Service Level</b> which allows you to add the custom ATP service level name.</p> <p>See <b>Autonomous Database Service Level</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
Support for <i>SOA Stack Patch Bundles</i> (SPBs).	Oracle SOA Suite on Marketplace supports <i>SOA Stack Patch Bundles</i> (SPBs).
Update in Oracle Home Path.	<p>Beginning with this release, the Oracle Home path has been updated to: <code>/u01/app/oracle/middleware</code></p> <p>This impacts the command to list the applied patches. The command to list the applied patches has been updated to: <code>/u01/app/oracle/middleware/OPatch/opatch lsinventory</code></p>

---

## March 2023 — Release 23.1.1

Features and Updates	Description
New provisioning options for enabling backup and restore configuration.	<p>A new section <b>Backup/Restore Configuration (enabled with KMS Configuration)</b> is exposed during provisioning when you select <b>Use KMS Vault Secrets for Passwords</b>. When you select <b>Enable Backup/Restore configuration</b>, the following configuration fields are exposed:</p> <ul style="list-style-type: none"> <li>• <b>KMS Vault Compartment</b></li> <li>• <b>KMS Vault</b></li> <li>• <b>KMS Encryption Key</b></li> <li>• <b>Object Storage Bucket Name</b></li> </ul> <p>See <b>Backup/Restore Configuration (enabled with KMS Configuration)</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
Backup and restore the domain home.	<p>When <b>Enable Backup/Restore configuration</b> is selected (either in the provisioning wizard or when editing an Oracle SOA Suite on Marketplace instance instance), you can back up and restore the domain homes for all nodes in an Oracle SOA Suite on Marketplace instance cluster.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <a href="#">Back Up the Domain Home</a></li> <li>• <a href="#">Restore the Domain Home</a></li> </ul>
When scaling out a cluster, a new option to copy Middleware Home and Oracle Home from the Administrator Server VM to the newly added node.	<p>When editing an Oracle SOA Suite on Marketplace instance to scale out a cluster, you can select <b>Copy Middleware Home and Oracle Home from Admin VM</b>. When selected, the newly added node automatically receives all the patches that are manually applied post-provisioning on the Administrator Server VM. However, the copy operation takes time, so the scale out operation will take more time. Additionally, you must make sure that there is enough storage in the boot volume of the Administration Server to create the binaries ZIP.</p> <p>See <a href="#">Scale Out an Oracle SOA Suite on Marketplace Instance Cluster</a>.</p>

---

## December 2022 — Release 22.4.1

Features and Updates	Description
Replacement of compute shapes.	<p>Beginning with this release, older generation shapes are no longer supported. Only the following compute shapes are supported:</p> <ul style="list-style-type: none"> <li>• <b>VM.Standard3.Flex</b></li> <li>• <b>VM.Standard.E4.Flex</b></li> <li>• <b>VM.Optimized3.Flex</b></li> </ul> <p>See <b>Compute Shape</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>

---

Features and Updates	Description
New provisioning options to enable secure boot and measured boot for Oracle SOA Suite on Marketplace VMs.	Enabling boot security options shield the compute instances from malicious boot level attacks. For more information, see <a href="#">Shielded Instances</a> in the <i>Oracle Cloud Infrastructure documentation</i> . See <b>Enable Secure Boot</b> and <b>Enable Measured Boot</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning option for specifying a custom ATP database wallet under <b>Service Instance Advanced Configuration</b> .	Select <b>Specify custom ATP wallet Password</b> to specify a custom ATP database wallet password. If not selected, the ATP database wallet password is auto-generated during provisioning. See <b>Service Instance Advanced Configuration</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning options for using an existing load balancer.	If you select <b>Provision Load Balancer</b> , you can now select an existing load balancer. See <b>Load Balancer Strategy</b> and <b>Existing Load Balancer</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .

---

Features and Updates	Description
Revised KMS configuration to use KMS secrets instead of KMS encrypted password.	<p>The <b>Use KMS Decryption</b> check box has been replaced, along with associated fields <b>Key Management Service Key Id</b> and <b>Key Management Service Cryptographic Endpoint</b>, with two options:</p> <ul style="list-style-type: none"> <li>• <b>Use KMS Vault Secrets for passwords:</b> Select this option to enable KMS vault secrets for passwords. The KMS secrets must be created prior to provisioning an Oracle SOA Suite on Marketplace instance. When selected, provisioning fields show selections for KMS secrets for passwords: <ul style="list-style-type: none"> <li>– For WebLogic Server administration: <b>WebLogic Server Admin Secret Compartment and Validated Secrets OCID for Nodemanager password</b></li> <li>– For WebLogic Server nodemanager: <b>WebLogic Server Nodemanager Secret Compartment and Validated Secrets OCID for Nodemanager password</b></li> <li>– For OCI database: <b>OCI DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>– For ATP database: <b>ATP DB Secret Compartment and Validated Secrets OCID for Autonomous Database ADMIN password</b></li> <li>– For Exadata database: <b>Exadata DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>– For database connection string: <b>External DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>– For RCU schema: <b>RCU Schema Secret Compartment and Validated Secrets OCID for Custom RCU Schema Password</b></li> <li>– For ATP DB wallet: <b>ATP DB Wallet Secret Compartment and Validated Secrets OCID for ATP DB Wallet Password</b></li> </ul> </li> <li>• <b>OCI Policies:</b> Select this option to create required OCI policies to access the KMS secrets from the vault during provisioning.</li> </ul> <p>For more information, see the <i>Oracle Cloud Infrastructure documentation</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">Managing Secrets</a></li> <li>• <a href="#">Managing Vaults</a></li> </ul> <p>See <b>Key Management Service Configuration in Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</b>.</p>

## August 2022 — Release 22.3.1

## Features and Updates

Support for creating a file system and mount target when provisioning a new Oracle SOA Suite on Marketplace instance using the ATP database. This configuration creates a new file system, mounted on all the nodes of the cluster. Subsequent scale out operations handle mounting the file system on the newly added node. When configured, FSS will be used as an alternative to DBFS.

## Description

When the **Service Type** is **MFT Cluster** and the **Database Strategy** is **Autonomous Transaction Processing Database**, the provisioning wizard exposes a new section titled **File Storage**, where you can choose to create a new mount target or reuse an existing mount target. This configuration is mandatory for an MFT Cluster service type on an Autonomous Transaction Processing (ATP) database.

The screenshot shows the 'Create stack' wizard with the 'File Storage' section expanded. On the left, there are three steps: 'Check information', 'Configure variables', and 'Execute'. The 'File Storage' section contains several configuration options:

- File System Compartment:** A dropdown menu with 'SOACompartment' selected.
- File Storage Availability Domain:** A dropdown menu with 'US-EAST-1' selected.
- Mount Target Strategy:** A dropdown menu with 'Create New Mount Target' selected.
- Mount Target Compartment:** A dropdown menu with 'SOACompartment' selected.
- Mount Target Subnet:** A dropdown menu with 'mp-subnet (Regional)' selected.
- Use Network Security Group for Mount Target:** An unchecked checkbox.

When the **Service Type** is **SOA with SB & B2B Cluster** and the **Database Strategy** is **Autonomous Transaction Processing Database**, you can optionally select a new check box labeled **Configure File Storage for shared location in cluster nodes** to expose the **File Storage** configuration settings in the provisioning wizard. By default, this setting is not selected.

The screenshot shows the 'Create stack' wizard with the 'File Storage' section expanded. On the left, there are three steps: 'Check information', 'Configure variables', and 'Execute'. The 'File Storage' section contains a checkbox:

- Configure File Storage for shared location in cluster nodes:** An unchecked checkbox.

Below this, there are sections for 'Service Instance Advanced' (with an unchecked checkbox for 'Service Instance Advanced Configuration') and 'Email Notification'.

See **File Storage** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).



July 2022 — Release 22.2.3.1

**Features and Updates**

Support for Oracle Cloud Infrastructure Resource Manager private endpoints

**Note:** To use this feature, you must add security policies to your tenancy. See [Manage Private Endpoints](#) in the *Oracle Cloud Infrastructure documentation*.

**Description**

In the **Bastion Instance Strategy** list, you can select a new option: **Use Private Endpoint**. This is the now the default selection, enabling private SSH access to compute instances created during provisioning of Oracle SOA Suite on Marketplace instances on a private subnet.

This selection exposes additional private endpoint settings in the provisioning screen, described in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#):

- **Private Endpoint Strategy**
- **Private Subnet Compartment**
- **Private Endpoint Subnet**
- **Private Endpoint Display Name**
- **Use Network Security Group for Private Endpoint**
  - **Network Security Group Compartment**
  - **Private Endpoint Network Security Group**
- **Existing Private Endpoint**

Bastion Instance Strategy

Use Private Endpoint

Create or use an existing Bastion compute instance.

Private Endpoint Strategy

Create New Private Endpoint

Create or use an existing private endpoint.

Private Endpoint Compartment

oicdev

Choose the compartment of the private endpoint.

Private Subnet Compartment

oicdev

Choose the compartment of the private endpoint subnet.

Private Endpoint Subnet

-

Choose a private subnet for creating the private endpoint

This variable is required.

Private Endpoint Display Name

Name of the private endpoint

This variable is required.

Use Network Security Group for Private Endpoint

Use a network security group (NSG) for controlling traffic to the private endpoint.

Network Security Group Compartment

oicdev

Choose the compartment of the network security group (NSG).

Private Endpoint Network Security Group

-

Network security group (NSG) to be used for controlling traffic to the private endpoint.

This variable is required.

See **Bastion Instance Strategy** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

## April 2022 — Release 22.2.1.1

Features and Updates	Description
Support for Oracle Enterprise Scheduler (ESS) on the Autonomous Transaction Processing (ATP) database.	If you use the Oracle Autonomous Transaction Processing (ATP) database for your Oracle SOA Suite on Marketplace instances, you can now use Oracle Enterprise Scheduler to define, schedule, and run jobs.  See <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a> .
Support for VM.Standard3 compute shapes.	When provisioning an Oracle SOA Suite on Marketplace instance, the <b>Compute Shape</b> list includes VM.Standard3 shapes.  See <b>Compute Shape</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .

## February 2022 — Release 22.1.1.2

Features and Updates	Description
Support for providing the database connection string when provisioning a new Oracle SOA Suite on Marketplace instance.	In the <b>Database Strategy</b> list, you can select the new option <b>Database Connection String</b> . This option is only for advanced users, and not recommended. Syntax: <i>host:port/serviceName</i> .

See **Database Strategy** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

Features and Updates	Description
Support for customizing the name of a cluster, domain, or servers when provisioning a new Oracle SOA Suite on Marketplace instance.	<p>When <b>Service Instance Advanced Configuration</b> is selected, optionally enter values for:</p> <ul style="list-style-type: none"> <li>• <b>Custom Cluster Name</b></li> <li>• <b>Custom Domain Name</b></li> <li>• <b>Custom Admin Server Name</b></li> <li>• <b>Custom Managed Server Name Prefix</b></li> <li>• <b>Custom Machine Name Prefix</b></li> </ul>

See **Service Instance Advanced Configuration** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

## December 2021 — Release 21.4.5

Features and Updates	Description
Uptake of Apache Log4j 2.16 to fix CVE-2021-44228 and CVE-2021-45046.	<p>With this release, an Apache Log4j security vulnerability is addressed in newly provisioned Oracle SOA Suite on Marketplace instances.</p> <p>For existing instances, you must apply the 21.4.5 patches to update the instances with this fix.</p> <p>See <a href="#">Patches Applied During Provisioning — 21.4.5</a> and <a href="#">About Managing Patches for Instances Provisioned With Earlier Releases</a>.</p>

## November 2021 — Release 21.4.3

Features and Updates	Description
Support for optionally selecting a network security group (NSG) in the provisioning screens to control network traffic.	<p>Oracle SOA Suite on Marketplace allows NSGs for the following resources:</p> <ul style="list-style-type: none"> <li>• Oracle SOA Suite on Marketplace compute instances</li> <li>• Bastion host</li> <li>• Load balancer</li> </ul> <p>If you do not select to use network security groups (NSGs), the compute instances and load balancer use the security lists of the respective subnets.</p> <p>See <b>Instance Network</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>

## November 2021 — Release 21.4.1

## Features and Updates

Support for new flexible compute shapes (flex shapes) when provisioning a new Oracle SOA Suite on Marketplace instance.

**Note:** Flexible compute shapes are not supported for a Bastion instance.

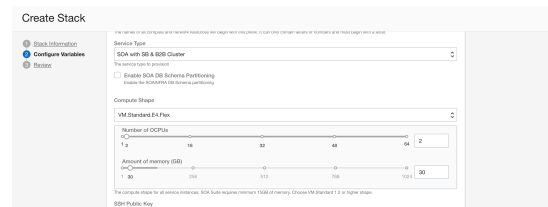
## Description

In the **Compute Shape** list, you can select the following new flex shapes:

- **VM.Standard.E3.Flex**
- **VM.Standard.E4.Flex**
- **VM.Optimized3.Flex**

These flex shapes allow you to customize the following values for Oracle SOA Suite on Marketplace instances:

- **OCPUs count:**
  - Minimum: 2
  - Maximum: 18
- **Memory size:**
  - Minimum: 15GB
  - Maximum: 256GB

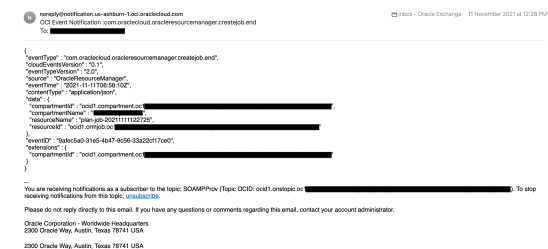


See **Compute Shape** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

New provisioning selections to support email notifications:

- **Enable Email notifications**
- **ONS Topic Strategy**
- **Existing ONS Topic OCID**
- **Notification Email ID**

During provisioning of a new Oracle SOA Suite on Marketplace instance, you can configure the OCI Notification Service (ONS) to send an email notification upon completion of the Terraform job in the stack, containing information about the job. Example email:



See **Email Notification** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

---

### October 2021 — Release 21.3.2.1

Features and Updates	Description
Support for the Exadata database when provisioning a new Oracle SOA Suite on Marketplace instance.	<p>A <b>Database Strategy</b> of <b>Exadata Database</b> requires the following configuration values:</p> <ul style="list-style-type: none"> <li>• Exadata SCAN DMS name</li> <li>• Pluggable database (PDB) service name</li> <li>• Database administrator and password</li> <li>• Database listener port</li> </ul> <p>See <b>Database Strategy</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>

---

### September 2021 — Release 21.3.2

Features and Updates	Description
New provisioning selection under <b>Service Instance Advanced Configuration: Coherence Cluster Port</b> .	<p>Use this field to specify the cluster listen port used by Coherence.</p> <p>See <b>Service Instance Advanced Configuration</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>

---

### May 2021 — Release 21.2.2

Features and Updates	Description
New provisioning selection for specifying the load balancer shape: <b>Flexible</b> .	<p>When you select a <b>Load Balancer Shape</b> of <b>Flexible</b>, the provisioning wizard exposes two fields to specify the minimum and maximum bandwidth for the load balancer, or set a fixed load balancer shape by specifying the same value for both the minimum and maximum bandwidth.</p> <p>See <b>Load Balancer Shape</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
New automation script to simplify enabling the WebLogic Plug-In at the cluster level.	<p>The following script is provided in <code>/opt/scripts/runbooks</code> to enable the WebLogic Plug-In in a cluster:</p> <ul style="list-style-type: none"> <li>• <code>enableWeblogicPlugin.sh</code></li> </ul> <p>See step 12 in <a href="#">Configure an Existing Load Balancer for a Provisioned Instance</a>.</p>

---

### March 2021 — Release 21.1.3

Features and Updates	Description
Oracle Cloud Infrastructure Console navigation menu changes.	The navigation menu for accessing Oracle SOA Suite on Marketplace has changed. Topics in this guide have been updated with the new navigation.

Features and Updates	Description
New editable field in the Edit Stack wizard: <b>Domain Volume Size (GB)</b> .	In the Edit Stack wizard, you can increase the domain volume size defined during provisioning of an instance. You cannot decrease the domain volume size.  See <a href="#">Increase the Domain Volume Size Post-Provisioning</a> .
New automation scripts to simplify tasks.	The following scripts are provided in <code>/opt/scripts/runbooks</code> : <ul style="list-style-type: none"> <li>• <code>resizeDomainVolume.sh</code> (see <a href="#">Increase the Domain Volume Size Post-Provisioning</a>)</li> <li>• <code>updateDBPassword.sh</code> (see <a href="#">Update the Database Schema Password</a>)</li> <li>• <code>updateDBFSWallet.sh</code> (see <a href="#">Update the DBFS Wallet Password</a>)</li> <li>• <code>updateJVMHeapSizeParameters.sh</code> (see <a href="#">Update the JVM Heap Size Parameter Values for Managed Servers</a>)</li> <li>• <code>updateFrontEndHostPort.sh</code> (see step 11 in <a href="#">Configure an Existing Load Balancer for a Provisioned Instance</a>)</li> </ul>

### March 2021 — Release 21.1.2

Features and Updates	Description
Support for the OCI Storage Cloud Service source and target type for Oracle Managed File Transfer in Oracle SOA Suite on Marketplace.	When provisioned to use the <b>MFT Cluster</b> service type, Oracle SOA Suite on Marketplace supports the OCI Storage Cloud Service source and target type to transfer data to and from Oracle Cloud Infrastructure. See <a href="#">OCI Storage Cloud Service Source Type</a> and <a href="#">OCI Storage Cloud Service Target Type</a> in <i>Using Oracle Managed File Transfer</i> . <b>Note:</b> For instances provisioned prior to 2 March 2021, this feature is available only if you have installed 12.2.1.4 patch 32395225. Additionally, to update the MFT Composer online help to reflect these changes, you must install patch 32463347. Sign in to <a href="#">My Oracle Support</a> and search for the patch numbers to locate and download the patches.
New provisioning option for the Node Manager password under <b>Service Instance Advanced Configuration: Specify Custom WLS Nodemanager Password</b> .	You can select this check box to specify a custom Node Manager password that is different from the WebLogic Server administration password. If not selected, the Node Manager and WebLogic Server administration passwords are the same.  See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .

## February 2021 — Release 21.1.1

Features and Updates	Description
<p>Changed purpose for provisioning option to select the name of the availability domain in which to create instances: <b>Availability Domain</b>.</p>	<p>The selection of an availability domain for an Oracle SOA Suite on Marketplace instance is moved from its prior location in the provisioning wizard to a new location only visible when the <b>Subnet Strategy</b> is set to <b>Create New Subnet</b> and the <b>Subnet Span</b> is set to <b>AD Specific Subnet</b>. In prior releases, all nodes in Oracle SOA Suite on Marketplace cluster were created in same availability domain even if there were multiple availability domains in the region. With this change, the nodes in an Oracle SOA Suite on Marketplace cluster are distributed evenly across all available availability domains. You can no longer select an availability domain during provisioning unless you choose to create a new <b>AD Specific Subnet</b>.</p> <p>See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
<p>Expanded provisioning options to create new subnets in a selected compartment: <b>Subnet Compartment</b> and <b>Load Balancer Subnet Compartment</b>.</p>	<p>You can create both new and existing Oracle SOA Suite on Marketplace instance or load balancer subnets in the compartment of your choice. In prior releases, you could select a compartment only for an existing subnet.</p> <p>See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
<p>New provisioning option for selecting a Bastion subnet compartment: <b>Bastion Host Subnet Compartment</b>.</p>	<p>You can create a new Bastion instance in an existing private subnet in the compartment of your choice.</p> <p>See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>
<p>RCU database profile password expiration set to 365 days.</p>	<p>Oracle SOA Suite on Marketplace RCU schemas are created with a new RCU database profile, where the password expiration limit is set to 365 days. All RCU schemas created during provisioning of new Oracle SOA Suite on Marketplace instances will be set to use the new RCU database profile. In prior releases, the Oracle SOA Suite on Marketplace RCU schemas were created with a default database profile.</p>

## November 2020 — Release 20.4.2.1

Features and Updates	Description
<p>New provisioning option for entering a custom domain block volume size: <b>Domain Volume Size (GB)</b>.</p>	<p>You can specify a custom domain block volume size for an Oracle SOA Suite on Marketplace instance. The default (minimum) value is 50GB. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>.</p>

## November 2020 — Release 20.4.2

Features and Updates	Description
Increased character limit for an Oracle SOA Suite on Marketplace instance name prefix.	The character limit for an Oracle SOA Suite on Marketplace instance name prefix is increased from 8 to 15 characters. See <b>Instance Name Prefix</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New topic added to this guide for the division of roles and responsibilities between Oracle and customers.	See <a href="#">About Oracle SOA Suite on Marketplace Roles and Responsibilities between Oracle and Customer</a> .
New topic added to this guide for creating a data source for an Oracle Autonomous Transaction Processing (ATP) database.	See <a href="#">Create a Data Source for an Oracle Autonomous Transaction Processing Database</a> .
New topic added to this guide for disabling the default automatic restart of the Administration Server and Managed Servers during an Oracle SOA Suite on Marketplace instance reboot.	See <a href="#">Disable Server Restart During an Instance Reboot</a> .

## October 2020 — Release 20.3.3.1

Features and Updates	Description
Support for multinode BAM clusters.	Multinode BAM clusters provide high availability for Oracle BAM Composer and dashboards. See <b>Oracle Business Activity Monitoring (BAM)</b> in <a href="#">About the Components of Oracle SOA Suite on Marketplace</a> .

## September 2020 — Release 20.3.3

Features and Updates	Description
When provisioning in a private subnet, new provisioning options for choosing an existing Bastion host instead of creating a new Bastion host for every SOA cluster: <b>Bastion Instance Strategy</b> , <b>Public IP of Bastion Instance</b> , and <b>SSH Private Key Bastion Instance</b> .	When you choose an existing VCN and existing private subnet during provisioning, you must provide the public IP of the existing Bastion host, along with an SSH private key as input. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning option for entering the database listener port: <b>Database Listener Port</b> .	You can specify a custom listener port for your database. The default value is 1521. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning option for entering an RCU schema password: <b>Specify RCU Schema custom Password</b> .	You can select to specify a custom password for the RCU schema. If this option is not selected, the provisioning process generates a random password for the RCU schema. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .



Features and Updates	Description
Support for providing an SSH key file to enter the value for <b>SSH Public Key</b> .	You can enter the public key for the secure shell (SSH), either by providing an SSH key file or pasting the SSH key. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Added security for the WebLogic Server administration password.	During provisioning, the <b>Administration Password</b> value must be entered twice for confirmation.
Oracle SOA Suite on Marketplace provisioned with the Oracle Cloud Infrastructure database supports both <b>Oracle Grid Infrastructure</b> and <b>Logical Volume Manager (LVM)</b> storage management software.	Previously, Oracle SOA Suite on Marketplace provisioned with the Oracle Cloud Infrastructure database supported only <b>Oracle Grid Infrastructure</b> storage management software.

### September 2020 — Release 20.3.2

Features and Updates	Description
New Quick Start option to provision an Oracle SOA Suite on Marketplace instance quickly, along with underlying Oracle Cloud Infrastructure network resources.	A quick start instance is useful for testing integrations with minimal knowledge required to set up Oracle Cloud Infrastructure network resources. The Quick Start option helps you to provision an instance with default values and fewer clicks than going through the full provisioning wizard. See <a href="#">Provision an Oracle SOA Suite on Marketplace Quick Start Instance</a> .
New provisioning options for configuring a load balancer during provisioning: <b>Load Balancer Subnet Type</b> and <b>Load Balancer Subnet Compartment</b> .	A load balancer can be in a public or private subnet, and you can select the load balancer subnet compartment. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning options for specifying an RCU schema prefix: <b>Specify Custom RCU Schema Prefix</b> and <b>Custom RCU Schema Prefix</b> .	You can select <b>Specify Custom RCU Schema Prefix</b> , then enter an RCU schema prefix. Note that it is your responsibility to make sure that the prefix name is unique in the selected database. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Support for cluster sizes up to 16 nodes.	During provisioning, the maximum allowable cluster size is 8 nodes. If you want to create a cluster of a larger size, you can create a 8-node cluster during provisioning and then <a href="#">scale out</a> the cluster to increase the cluster size to a maximum size of 16 nodes. See <b>Cluster Node Count</b> in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .

Features and Updates	Description
Reduced number of editable fields in the Edit Stack wizard.	In the Edit Stack wizard, only the following fields are editable: <ul style="list-style-type: none"> <li>• <b>Compute Shape</b></li> <li>• <b>Cluster Node Count</b></li> <li>• <b>Load Balancer Subnet Compartment</b></li> <li>• <b>Existing Subnet for Load Balancer</b></li> <li>• <b>Load Balancer Shape</b></li> </ul> See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a> .
Support for OS Management service in Oracle Cloud Infrastructure.	You can enable OS Management for all Oracle SOA Suite on Marketplace instances to manage OS patches and security fixes. See <a href="#">Enable OS Management for Oracle SOA Suite on Marketplace Instances</a> .

### August 2020 — Release 20.3.1

Features and Updates	Description
Provisioning of new Oracle SOA Suite on Marketplace instances will include July 2020 Patch Set Updates (PSUs).	See <a href="#">Oracle Critical Patch Update Advisory - July 2020</a> .
New topic added to this guide for adding access rules if you are not able to access the WebLogic Server Administration Console or other console URLs from your browser after provisioning an Oracle SOA Suite on Marketplace instance after 1 August 2020.	See <a href="#">Add Ingress Rules to Access WebLogic Server Administration and Other Consoles</a> .
New topic added to this guide for replacing an existing Oracle Cloud Infrastructure database with a new Oracle Cloud Infrastructure database.	See <a href="#">Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database</a> .
New provisioning options for selecting the database compartment: <b>DB System Compartment</b> and <b>Autonomous DB System Compartment</b> .	The database can be provisioned in the same compartment as the Oracle SOA Suite on Marketplace instance, or a different compartment. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
New provisioning selection: <b>Subnet Compartment</b> .	If you choose to create an Oracle SOA Suite on Marketplace instance in an existing subnet, you can select the compartment for the subnet. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Support for Oracle Real Application Clusters (RAC) during Oracle Cloud Infrastructure database provisioning.	See <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a> .
Support for ATP-D during Oracle Autonomous Transaction Processing (ATP) database provisioning.	Oracle SOA Cloud Service supports both <i>serverless deployments</i> and <i>dedicated deployments</i> (ATP-D) of the ATP database.
Support for the Database Adapter for the Oracle Autonomous Transaction Processing (ATP) database.	See <a href="#">Oracle JCA Adapter for Database</a> .

Features and Updates	Description
Support for Oracle Exadata Database Service as a backend database to create SOAINFRA schemas.	See <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a> .
<b>June 2020 — Release 1.0.11.1</b>	
Features and Updates	Description
New Marketplace offerings: <ul style="list-style-type: none"> <li>• Oracle SOA Suite on Oracle Cloud Infrastructure (PAID)</li> <li>• Oracle SOA Suite with B2B EDI Adapter on Oracle Cloud Infrastructure (PAID)</li> </ul>	In addition to the BYOL offering, Oracle SOA Suite on Marketplace is available as a PAID offering. See <a href="#">About the Oracle SOA Suite on Marketplace License</a> .
New provisioning selection to enable SOAINFRA schema partitioning: <b>Enable SOA DB Schema Partitioning</b>	When provisioning an Oracle SOA Suite on Marketplace instance for service type <b>SOA with SB &amp; B2B Cluster</b> , you can select <b>Enable SOA DB Schema Partitioning</b> to enable SOAINFRA schema partitioning. By default, this setting is not selected. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Change to ports in an existing subnet	If you provision your Oracle SOA Suite on Marketplace instance in an existing subnet, the ports that you must open explicitly before provisioning changed: <ul style="list-style-type: none"> <li>• Administration Server: from 7001/7002 to 9071/9072</li> <li>• Managed Servers to load balancer subnet from 7003/7004 to 9073/9074</li> </ul> See <a href="#">Configure Security Lists</a> .

# 2

## Get 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](#)
- [Migrate or Upgrade to an Oracle SOA Suite on Marketplace Instance](#)
- [About the Oracle SOA Suite on Marketplace License](#)
- [About the Components of Oracle SOA Suite on Marketplace](#)
- [About the Components of Oracle Cloud Infrastructure Used By 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 Managing Oracle SOA Suite on Marketplace Instances](#)
- [About Security for Oracle SOA Suite on Marketplace Instances](#)
- [About Managing Patches for Instances Provisioned With Earlier Releases](#)
- [About Oracle SOA Suite on Marketplace Roles and Responsibilities between Oracle and Customer](#)

## About Oracle SOA Suite on Marketplace

Oracle SOA Suite on Marketplace supports Oracle SOA Suite 12c (12.2.1.4) and its components. It is provided as a VM-based solution on Oracle Cloud Infrastructure.

Oracle SOA Suite on Marketplace is available in two types of Marketplace offerings: PAID and BYOL. See [About the Oracle SOA Suite on Marketplace License](#).

Oracle SOA Suite on Marketplace provides a Platform as a Service (PaaS) computing platform solution for running applications in the cloud. It includes a complete set of service infrastructure components for designing, deploying, and managing composite applications. See [About the Components of Oracle SOA Suite on Marketplace](#).

The rich variety of features of Oracle SOA Suite on Marketplace 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, which means that 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 Fusion Cloud Sales Automation new customer account with a Siebel application. This enables a customer that purchases a product through Oracle Fusion Cloud Sales Automation to receive support for that product through the Siebel system. For this same Oracle Fusion Cloud Sales Automation 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](#).

### Topics:

- [Differences Between Oracle SOA Cloud Service and Oracle SOA Suite on Marketplace](#)
- [Differences Between Oracle SOA Suite On-Premises and Oracle SOA Suite on Marketplace](#)

## Differences Between Oracle SOA Cloud Service and Oracle SOA Suite on Marketplace

Review the differences between Oracle SOA Cloud Service and Oracle SOA Suite on Marketplace.

Oracle SOA Cloud Service	Oracle SOA Suite on Marketplace
Provisioned using the Oracle SOA Cloud Service Console. Uses the Oracle SOA Cloud Service Console for all operations.	Provisioned using the Oracle Cloud Infrastructure Console. Uses the Oracle Cloud Infrastructure Console for all operations. See <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
SOA URLs are displayed in the Oracle SOA Cloud Service Console.	SOA URLs are displayed in the job details, either from the job outputs view or the log file. See <a href="#">Access an Oracle SOA Suite on Marketplace Instance</a> .
Cluster size during initial provisioning is restricted to 1, 2, 4, or 8.	Cluster size during initial provisioning can be any value from 1 to 8, and you can scale out a cluster up to 16 nodes.
Supports only <i>serverless deployments</i> of the Oracle Autonomous Transaction Processing (ATP) database. Does not support <i>dedicated deployments</i> .	Supports both <i>serverless deployments</i> and <i>dedicated deployments</i> of the Oracle Autonomous Transaction Processing (ATP) database.
Requires a patch for Database Adapter connectivity with the Oracle Autonomous Transaction Processing (ATP) database.	Supports the Database Adapter with the Oracle Autonomous Transaction Processing (ATP) database out of the box.
Does not support database schema partitioning during provisioning.	Supports database schema partitioning during provisioning.

Oracle SOA Cloud Service	Oracle SOA Suite on Marketplace
All Oracle Cloud Infrastructure resources must be in the same compartment.	Security lists and subnets can be defined in parent compartment subnets.
Supports provisioning with Oracle Cloud Infrastructure database and Autonomous Transaction Processing (ATP) database. Does not support Exadata Cloud Service on Oracle Cloud Infrastructure.	Supports provisioning with Oracle Cloud Infrastructure database, Autonomous Transaction Processing (ATP) database, and Exadata Cloud Service on Oracle Cloud Infrastructure. See <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a> for supported Oracle Database versions.
Supports the Oracle Traffic Director (OTD) load balancer during provisioning. Also supports Oracle Cloud Infrastructure load balancer, which must be configured manually post-provisioning.	Supports the Oracle Cloud Infrastructure load balancer in both private and public subnets. The load balancer can be configured during provisioning or post-provisioning. See <a href="#">Add or Delete a Load Balancer Post-Provisioning</a> .
Does not include the option to specify a custom schema prefix.	Supports configuring a custom schema prefix during provisioning. See SPECIFY_CUSTOM_RCU_SCHEMA_PREFIX in <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a> .
Backups and restores of the WebLogic Server domain configuration are performed using the Oracle SOA Cloud Service Console.	Backups and restores of data volumes are performed using the Oracle Cloud Infrastructure Console/terminal.

## Differences Between Oracle SOA Suite On-Premises and Oracle SOA Suite on Marketplace

Review the high-level differences between Oracle SOA Suite on-premises and Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure.

Oracle SOA Suite On-Premises	Oracle SOA Suite on Marketplace
Installed on your own hardware.	Provisioned on Oracle Cloud.
You create the complete domain.	Provisioning an Oracle SOA Suite on Marketplace instance automatically creates an Oracle WebLogic Server domain.
You must install a database.	During Oracle SOA Suite on Marketplace provisioning, you select the database to use. <b>Note:</b> You must provision a <a href="#">database</a> prior to provisioning a Oracle SOA Suite on Marketplace instance.
You must set up an environment based on your high availability requirements.	High availability functionality is provided by default using a virtual machine.
Oracle HTTP Server serves as the load balancer.	Load balancing is provided by the Oracle Cloud Infrastructure load balancer.

Oracle SOA Suite On-Premises	Oracle SOA Suite on Marketplace
You typically use shared storage.	<ul style="list-style-type: none"> <li>Shared storage is available through Database File System (DBFS) or OCI File Storage Service (FSS) in the cloud.</li> <li>You can use a combination of database direct configuration for JMS and JTA logs and use DBFS for other shared file use cases.</li> <li>Log files are local to each virtual machine.</li> <li>Managed Servers by default will write to a file on their own local disks. Optionally, you can configure adapters to read/write files from shared storage (DBFS/FSS).</li> </ul>
Additional memory and storage must be manually added to address high load.	Supports scaling up and adding storage to add more memory and storage when needed.
Stopping and starting the servers requires many manual steps.	Supports stop and start operations to reboot the VMs, node manager, load balancer, and SOA servers.
The domain must be manually extended to add a new Managed Server or add a new node.	Supports scaling out to add a new node and complete required configuration changes, and scaling in to remove a node from a cluster.
Network access for on-premises networks varies from site to site, as well as logic processes. Usually it is completely open to employees, as long as they have the right credentials.	<ul style="list-style-type: none"> <li>External network access must be configured at the virtual machine level and the load balancer level.</li> <li>Logins to the virtual machine can be done through an SSH tunnel.</li> </ul>
There should not be any connectivity issues blocking Oracle SOA Suite and your on-premises applications.	Connectivity between Oracle SOA Suite on Marketplace adapters and on-premises applications may be blocked by your corporate firewall. Connections can be established by setting up a VPN connection between Oracle Cloud and your on-premises network.
The SOA debugger and automatic SOA composite application tester (unit tester) in Oracle JDeveloper are supported when connecting to on-premises SOA Server.	The SOA debugger and automatic SOA composite application tester (unit tester) in Oracle JDeveloper are not supported when connecting to SOA Server in the cloud.
JMS store and JTA transaction logs can use either Oracle database or file stores.	JMS store and JTA transaction logs will use Oracle database instead of file stores.
Supports Oracle SOA for Healthcare.	Oracle SOA for Healthcare is not available.
After installing Oracle SOA Suite you can install Oracle Business Process Management Suite on top of it.	Oracle Business Process Management Suite is not available.

## About the Oracle SOA Suite on Marketplace License

Oracle SOA Suite on Marketplace is based on Oracle SOA Suite 12c (12.2.1.4).

Oracle SOA Suite on Marketplace is available in two types of Marketplace offerings:

- PAID:** Use one of the following Oracle SOA Suite (PAID) listings to use Universal Credits pricing:
  - Oracle SOA Suite for Oracle Cloud Infrastructure (PAID)
  - Oracle SOA Suite for Oracle Cloud Infrastructure - with B2B Adapter for EDI (PAID)

See [Oracle Universal Credits](#).

- **BYOL:** Use the Oracle SOA Suite (BYOL) listing to Bring Your Own License using your existing Oracle SOA Suite 12c (12.2.1.4) on-premises license, or you can purchase a new license for Oracle SOA Suite 12c (12.2.1.4).

When you activate Oracle SOA Suite on Marketplace using the BYOL listing, you are charged only for the Oracle Cloud Infrastructure resources consumed. You must 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 for the BYOL offering, go to the [Cloud Services Service Descriptions page](#) and click the link to the *Oracle PaaS and IaaS Universal Credits Service Descriptions* PDF. In particular, note the following conversion ratios for BYOL:

- For each supported Processor license you may activate up to 2 OCPUs of the BYOL Cloud Service.
- For every 25 supported Named User Plus licenses you may activate 1 OCPU of the BYOL Cloud Service.

Once you have selected one of these options, you cannot later change it. For example, if you selected BYOL and later want to use PAID, then you need to delete the BYOL instance and re-create a new PAID instance.

 **Note:**

If Oracle B2B is used, you need to have or purchase B2B (B2B for EDI, B2B for Rosettanet, or B2B for ebXML).

## About the Components of Oracle SOA Suite on Marketplace

Oracle SOA Suite on Marketplace supports Oracle SOA Suite 12c (12.2.1.4) and its constituent 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 be rapidly modeled for mobile devices such as smart phones and tablets using Oracle SOA Suite.

Oracle SOA Suite includes the following core components:

- **BPEL** (Business Process Execution Language) — Orchestrates integration processes.
- **Human Workflow** — Creates interactions that require human input, such as 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.

 **Note:**

Oracle SOA Suite on Marketplace uses a *Reference Configuration domain*. For more information, see *Selecting the Configuration Template for Oracle SOA Suite in Installing and Configuring Oracle SOA Suite and Business Process Management*.

See:

- [Understanding Oracle SOA Suite](#)
- [Developing SOA Applications with Oracle SOA Suite](#)

- **Oracle WebLogic Suite.** Oracle WebLogic Suite is the flagship Oracle WebLogic Server edition. It is included with Oracle SOA Suite on Marketplace.

For details about the components of Oracle WebLogic Suite, see [Oracle WebLogic Server](#) in *Oracle Fusion Middleware Licensing Information User Manual*.

- **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 Administration Server and the clustered Managed Server. Management features are deployed on the Administration 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. Note that Oracle B2B with Oracle SOA Suite on Marketplace does not support 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.

Oracle SOA Suite on Marketplace supports multinode BAM clusters, providing high availability for Oracle BAM Composer and dashboards. In the event of a node failure:

- You are prompted to log in again to continue working with the Oracle BAM Composer or dashboards on an active node.
- Time-based and KPI alerts do not trigger. As soon as all nodes are available again, all alerts will trigger.

To take advantage of high availability in a multinode BAM cluster, note the following requirements:

- Use Chrome or Internet Explorer 11+ as your browser. Other browsers, such as Firefox, are not certified for a multinode BAM cluster.
- Access BAM Composer and dashboards using the load balancer IP address in the URL, rather than a direct URL to a specific Managed Server. See [Access an Oracle SOA Suite on Marketplace Instance](#).
- Create and use ADF-based BAM dashboards. JET-based dashboards are not certified for a multinode BAM cluster.

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.

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

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.

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

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

- **Oracle Enterprise Scheduler.** Oracle Enterprise Scheduler is installed with Oracle SOA Suite on Marketplace. It 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](#)

- **Oracle Web Services Manager (OWSM).** OWSM provides the policy manager for securing web services, including authentication and authorization. OWSM is installed by default when you install Oracle Fusion Middleware Infrastructure. It is licensed only through Oracle SOA Suite; a standalone license is not available.

See:

- [Enabling Security with Policies and Message Encryption](#) in *Developing SOA Applications with Oracle SOA Suite*.
- [Administering Web Services](#)
- [Securing Web Services and Managing Policies with Oracle Web Services Manager](#)

## About the Components of Oracle Cloud Infrastructure Used By Oracle SOA Suite on Marketplace

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:

- [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#)
- [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:

- [Set 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:  
– [Create an Oracle Database for Oracle SOA Suite on Marketplace](#)  
– [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.

Resources	Description
Administration Server	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 domain has one server instance that hosts the Administration Server.
Managed Servers	Host business applications, application components, Web services, and their associated resources. When creating an Oracle SOA Suite on Marketplace instance, you can configure up to four Managed Servers, then scale out, as needed. Each Oracle SOA Suite on Marketplace 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: <i>first8charsOfDomainName_server_n</i> (where <i>n</i> starts with 1 and is incremented by 1 for each additional Managed Server to guarantee unique names).
Cluster	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 on Marketplace Managed Server instance name using the following format: <i>first8charsOfServiceInstanceName_cluster</i> .

Resources	Description
Load Balancer	<p>Employs the Oracle Cloud Infrastructure load balancer to manage routing requests across all Managed Servers and provide failover and replication.</p> <p>Using the load balancer is optional. It is recommended that you use the load balancer when you configure more than one Managed Server in your environment. You can enable the load balancer during provisioning (see <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>) or add it after provisioning (see <a href="#">Add or Delete a Load Balancer Post-Provisioning</a>).</p>

If you want more information about Oracle WebLogic Server domains, see [WebLogic Server Domains](#) in *Understanding Oracle WebLogic Server*.

After the Oracle SOA Suite on Marketplace 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.

## Typical Workflow for Managing the Life Cycle of Oracle SOA Suite on Marketplace Instances

To manage the life cycle of Oracle SOA Suite on Marketplace instances, follow the typical workflow shown in the following table.

Task	Description	More Information
Create an Oracle SOA Suite on Marketplace instance.	Create a new Oracle SOA Suite on Marketplace instance by stepping through the provisioning wizard in Oracle Cloud Infrastructure.	<a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>
View information about Oracle SOA Suite on Marketplace instances.	View status, resource allocation, and other details for Oracle SOA Suite on Marketplace instances.	<a href="#">View Oracle SOA Suite on Marketplace Instance Details</a>
Deploy and undeploy applications to an Oracle SOA Suite on Marketplace instance.	Deploy and undeploy applications to an Oracle SOA Suite on Marketplace instance using JDeveloper, Fusion Middleware Control, the WebLogic Server Administration Console, and WLST commands.	<a href="#">Deploy and Undeploy Applications for an Oracle SOA Suite on Marketplace Instance</a>
Stop, start, or restart an Oracle SOA Suite on Marketplace instance and individual servers.	Stop an Oracle SOA Suite on Marketplace instance, Administration Server, and Managed Servers. Restart the Administration Server or individual Managed Servers if reboot is needed.	<a href="#">Stop or Start an Oracle SOA Suite on Marketplace Instance and Servers</a>

Task	Description	More Information
Scale an Oracle SOA Suite on Marketplace instance.	Scale an Oracle SOA Suite on Marketplace instance cluster out or in to add or remove nodes in response to changes in the load on the cluster. Scale an Oracle SOA Suite on Marketplace instance up or down to change its compute shape in response to changes in workload or to add storage to a node that is running out of storage.	<a href="#">Scale an Oracle SOA Suite on Marketplace Instance Cluster Out or In</a> <a href="#">Scale an Oracle SOA Suite on Marketplace Instance Up or Down</a>
Back up and restore a block volume.	Back up a block volume to preserve Oracle SOA Suite on Marketplace instance data in a particular state. If necessary, undo changes by restoring the data from a block volume backup.	<a href="#">Back Up a Block Volume</a> <a href="#">Restore a Block Volume</a>
Deprovision an Oracle SOA Suite on Marketplace instance.	Manage access to an Oracle SOA Suite on Marketplace instance by deprovisioning the instance.	<a href="#">Deprovision an Oracle SOA Suite on Marketplace Instance</a>

## 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:

- Add Users to a Cloud Account with Identity Cloud Service in *Getting Started with Oracle Cloud*.
- [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.

## 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 adapter certification information.

### 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 on-premises and cloud SOA 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 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 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 along with Oracle SOA Suite on Marketplace OCPUs at the instance level during provisioning. After provisioning, the B2B Adapter for EDI cannot be disabled from an existing Oracle SOA Suite on Marketplace instance. The adapter can only be removed by deleting the instance. Billing can be paused by stopping the instance, which stops the entire Oracle SOA Suite on Marketplace VM. Another option is to create a new Oracle SOA Suite on Marketplace instance without the B2B Adapter for EDI and migrate Oracle SOA Suite on Marketplace projects and artifacts to the new instance. To migrate from an old Oracle SOA Suite on Marketplace instance to a new instance, see *Migrating to the Cloud and Side-by-Side Upgrade in the Cloud for SOA on Marketplace, SOA Cloud Service, and MFT Cloud Service*

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 Suite on Marketplace instances, the recommended path forward for using the B2B Adapter for EDI, is to provision a new Oracle SOA Suite on Marketplace instance, and then use that instance exclusively for B2B processing. This allows you to run an existing Oracle SOA Suite on Marketplace 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**.
3. Under **Additional Components**, click **Download** next to the B2B Document Editor components.

## About Managing Oracle SOA Suite on Marketplace Instances

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

Reliable management of Oracle SOA Suite on Marketplace instances requires a specific software environment that includes 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 instances manageable, follow these guidelines:

- To ensure that you can restore the database for an Oracle SOA Suite on Marketplace instance without risking data loss for other instances, do **not** use the same Oracle Cloud Infrastructure database with multiple Oracle SOA Suite on Marketplace instances. Backups of an Oracle Cloud Infrastructure database instance that are used with multiple Oracle SOA Suite on Marketplace instances contain data for all the instances. If you restore the database while restoring an Oracle SOA Suite on Marketplace instance, data for all the instances is restored.
- Apply the latest software bundle patches. See [About Managing Patches for Instances Provisioned With Earlier Releases](#).
- Use only the default domain that was provisioned when an Oracle SOA Suite on Marketplace instance was created. Do not add any Oracle WebLogic Server domains to the instance.
- If you plan to integrate multi-domain environments, ensure that the first eight characters of your Oracle SOA Suite on Marketplace 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 on Marketplace instance are generated from the first eight characters of the instance name, and use the following formats, respectively:

- `first8charsOfServiceInstanceName_domain`
- `first8charsOfServiceInstanceName_cluster`

- For any disk volume that an Oracle SOA Suite on Marketplace Managed Server attaches to an instance's VMs during creation of the instance:
  - Do not detach, change file access permissions for, or change the *mount point* of a disk volume.
  - Except for the `DOMAIN_HOME` volume, do not change the *content* of a disk volume.

For details about these volumes, see [About the Storage Volumes Attached to the WebLogic Server Nodes in Administering Oracle Java Cloud Service](#).

- Do not change the egress and ingress network and security settings of any infrastructure resources that the instance uses.
- If you close any ports or protocols post-provisioning, you may end up in blocking your server endpoint URLs. You must ensure that you have valid ingress rules allowing traffic from known sources only.

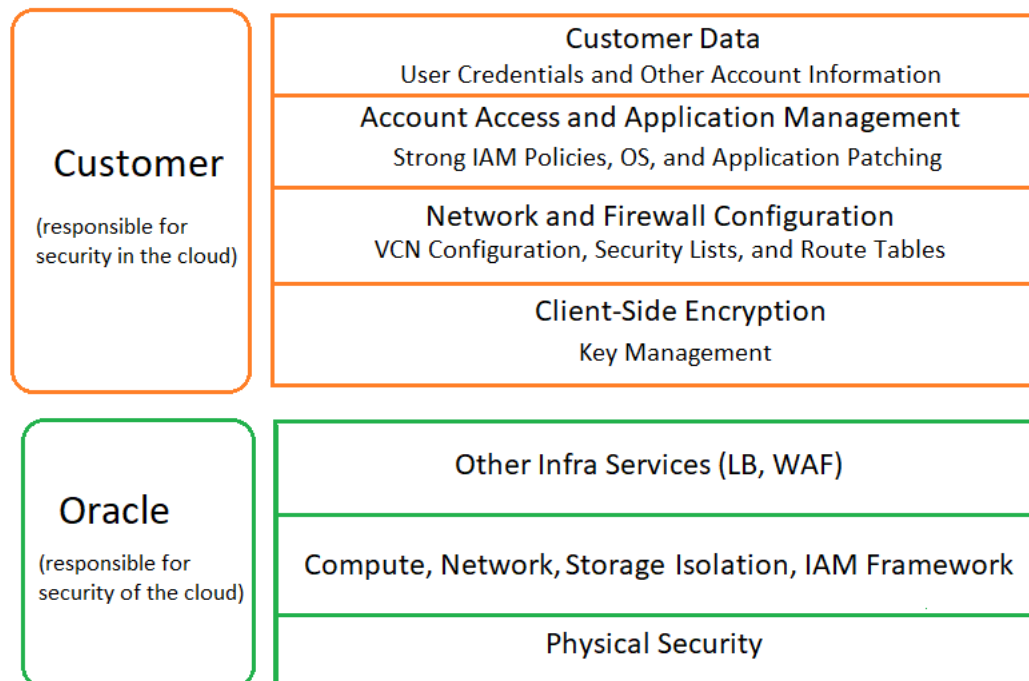


You can open new ports and protocols, but closing existing ports and protocols may impair the functioning of an instance.

- Do not detach NAT IP addresses from any of an instance's VMs.
- Do not change the Oracle Fusion Middleware component schemas with which an instance was provisioned.
- After provisioning, 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 an Oracle SOA Suite on Marketplace Managed Server configured during creation of an instance.

## About Security for Oracle SOA Suite on Marketplace Instances

Security in the cloud is a shared responsibility between you and Oracle. In a shared, multitenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data center facilities, hardware, and software) and you are responsible for securing your workloads and configuring your services (such as compute, network, storage, and database) securely.



The following principles are fundamental to using any application securely:

- Keep patches up-to-date. This includes all product patches that are applicable. For more information, see [About Managing Patches for Instances Provisioned With Earlier Releases and Patches Installed By Release](#).
- Limit privileges as much as possible. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Learn about and use the Oracle Cloud Infrastructure security features.

- Use secure best practices. For more information, see [Security Best Practices](#) in the Oracle Cloud Infrastructure documentation.
- Keep up-to-date on security information. Oracle regularly issues security-related patch updates and security alerts. Install all security patches as soon as possible. See the [Critical Patch Updates and Security Alerts](#) website.
- If you're creating a Linux instance, then try to determine how many users you expect to access the instance and plan for a separate SSH key pair for each user.
- Keep your SSH keys secure. Lay down policies to ensure that the keys aren't lost or compromised when employees leave the organization or move to other departments. If you lose your private key, then you can't access your instances. For business continuity, ensure that the SSH keys of at least two IT system administrators are added to your instances.
- If you need to edit the `~/.ssh/authorized_keys` file of a user on your instance, then before you make any changes to the file, start a second `ssh` session and ensure that it remains connected while you edit the `authorized_keys` file. This second `ssh` session serves as a backup. If the `authorized_keys` file gets corrupted or you inadvertently make changes that result in your getting locked out of the instance, then you can use the backup `ssh` session to fix or revert the changes. Before closing the backup `ssh` session, test the changes you made in the `authorized_keys` file by logging in with the new or updated SSH key.
- Ensure instance isolation by creating security lists and adding instances to the appropriate security lists. For more information, see [Configure Security Lists](#).
- To monitor network traffic on Oracle Cloud Infrastructure, enable VCN flow logs. For more information, see [VCN Flow Logs](#) in the Oracle Cloud Infrastructure documentation.
- WebLogic Server includes a set of demonstration private keys, digital certificates, and trusted certificate authorities that are for development only. Oracle highly recommends that you use third-party Certificate Authority (CA) signed certificates in a production environment.

## About Managing Patches for Instances Provisioned With Earlier Releases

It is your responsibility to keep your Oracle SOA Suite on Marketplace instances up-to-date with the latest software bundle patches.

The following types of patches apply to your Oracle SOA Suite on Marketplace instances:

- [SOA Bundle Patches](#)
- [Quarterly Security Patches](#)
- [Operating System Patches](#)

## SOA Bundle Patches

### Note:

- Oracle SOA Suite on Marketplace 23.2.2 and later versions support *SOA Stack Patch Bundles* (SPBs).
- Oracle SOA Suite on Marketplace 23.1.1 or earlier versions do not support *SOA Stack Patch Bundles* (SPBs). Use the *SOA bundle patch* instead of the SOA SPB to patch your existing Oracle SOA Suite on Marketplace instances.

When you provision a new Oracle SOA Suite on Marketplace instance, it contains all of the latest patches associated with the product. However, once instances are created, they are not automatically updated with the latest bundle patches from subsequent releases. You are responsible for keeping the instance patch levels current.

To retrieve a list of bundle patches that have been applied to your Oracle SOA Suite on Marketplace instance:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Enter the following command based on your Oracle SOA Suite on Marketplace instance version.

- For Oracle SOA Suite on Marketplace instances created on 23.2.2 and later versions:

```
/u01/app/oracle/middleware/OPatch/opatch lsinventory
```

- For Oracle SOA Suite on Marketplace instances created on 23.1.1 or earlier versions:

```
/u01/app/oracle/suite/OPatch/opatch lsinventory
```

Applying bundle patches to existing instances may involve multiple Oracle SOA Suite on Marketplace instances that were provisioned at different times that may include different bundle patches. Contact Oracle Support for information about the latest Oracle SOA Suite on Marketplace certified patches and instructions on how to apply the patches.

If a `FUSER could not be located` error occurs while applying a patch to Oracle SOA Suite on Marketplace, perform the following steps:

1. Set the environment variable: `export OPATCH_NO_FUSER=TRUE`.
2. In the Unix shell where step 1 is executed or `OPATCH_NO_FUSER=TRUE` is set, apply the patch.

**Note:**

You can find the current list of Oracle SOA Suite on Marketplace bundle patches in [Patches Installed By Release](#).

**Quarterly Security Patches**

Oracle recommends that you subscribe to security updates and apply quarterly security patches that are available for your release. For more information, see [Step1: Apply the Latest Patch Set Update for WebLogic Server](#).

**Operating System Patches**

To assist you with managing operating system patches, Oracle SOA Suite on Marketplace supports the Oracle Cloud Infrastructure OS Management service. OS Management offers the capability to view and install the available CPU fixes, security patches, and bug fixes on your compute instances. You can create instance groups and add all the nodes of a SOA cluster to a group and manage all the patches and updates of all the instances in the group. To enable OS Management for Oracle SOA Suite on Marketplace, see [Enable OS Management for Oracle SOA Suite on Marketplace Instances](#).

**Recommendations:**

- Before applying an operating system patch, stop the SOA servers from the command line. After the patch is applied, [start the SOA servers](#).
- For major version patching (for example, OEL6 to OEL8), consult the Linux upgrade documentation if your operating system version has a supported upgrade path. While it is possible to upgrade the Linux version of current nodes to OEL8, the base image continues to remain on OEL7, and any subsequent scale-out operations creates a new node on OEL7 with potential issues.
- Always test the patch on a non-production environment before applying it to a production environment.
- If you need help with issues in applying Linux patches, file a service request (SR) at [My Oracle Support](#) (click the Service **Requests** tab, and click **Create Technical SR**) on the Oracle Linux product.

## About Oracle SOA Suite on Marketplace Roles and Responsibilities between Oracle and Customer

This table summarizes the division of roles and responsibilities for Oracle SOA Suite on Marketplace.

**R=Responsible, A=Accountable, C=Consulted, I=Informed**

Task	Oracle's Role	Customer's Role	Comments
All lifecycle operations: <ul style="list-style-type: none"> <li>• Instance provisioning and deprovisioning</li> <li>• Backup and restore</li> <li>• Scale out, scale in, scale up, scale down</li> <li>• Start and stop</li> <li>• Patching</li> </ul>	A	R, A	Customer provisions the Oracle SOA Suite on Marketplace instance and is responsible for all lifecycle operations.  Customer manually applies operating system, Oracle SOA Suite on Marketplace, and MFT patches.
High availability	C	R, A	Oracle provides necessary capabilities for HA/DR/replication. Customer is responsible for incorporating them into their solution.
Disaster recovery	C	R, A	Oracle provides necessary capabilities for HA/DR/replication. Customer is responsible for incorporating them into their solution.
Security and compliance	R, A	R, A	Oracle is responsible for security and compliance of the underlying shared infrastructure.  Customer is responsible for securing the service endpoints and console URLs exposed by the individual services.
VPN configuration	C	R, A	
VPN monitoring	C	R, A	
Service monitoring	C	R, A	
User setup, roles and permissions	C	R, A	Customer is responsible for user credentials. Applications are maintained and managed by the customer.
Maintenance notifications	R, A	I	Customer must subscribe to Oracle security notifications.  Oracle publishes security notifications to subscribed customers.
Source control and continuous delivery	C	R, A	
Customer composites and projects	C	R, A	
Overage tracking and management	C	R, A	

# 3

## Before You Begin

Before provisioning Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure, it is helpful to have an understanding of how your topology is configured. Make sure you can sign in to the Oracle Cloud Infrastructure Console and complete the prerequisites.

### Topics:

- [Understand Oracle SOA Suite on Marketplace Topologies](#)
- [Sign in to the Oracle Cloud Infrastructure Console](#)
- [Prerequisites](#)

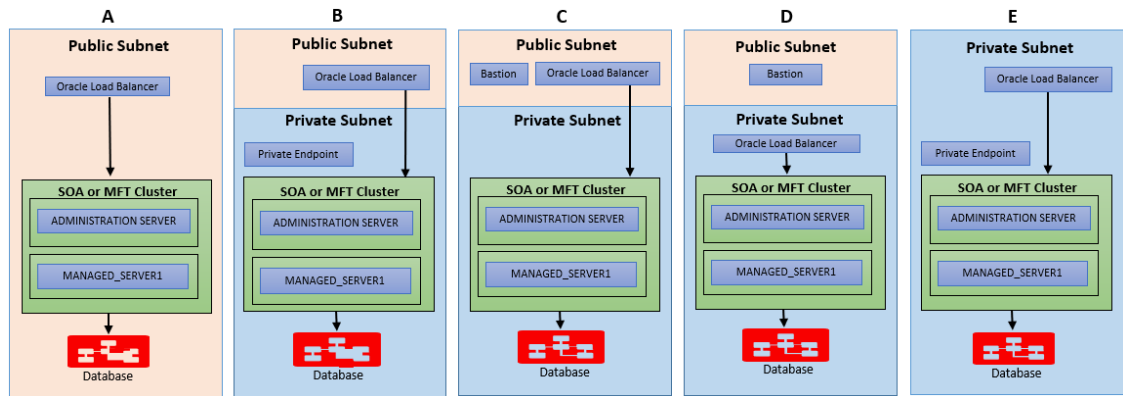
## Understand Oracle SOA Suite on Marketplace Topologies

You can create a virtual cloud network (VCN) with a *public subnet* or a *private subnet* to extend your on-premises network into the cloud.

- **Public subnet:** Instances created in a public subnet have both a public IP address and a private IP address. These instances have direct access to the internet through an *internet gateway*. Traffic can initiate from both the internet and public subnet instances.
- **Private subnet:** Instances created in a private subnet need only a private IP address with no internet access. These instances can initiate connections to the internet through a *NAT gateway* (for example, to get software updates), but cannot receive inbound connections from the internet through that gateway. When you provision an Oracle SOA Suite on Marketplace instance with a private subnet, you must select to create or use an existing private endpoint or to create or use an existing Bastion VM.

You can configure Oracle SOA Suite on Marketplace across a public and private subnet in several ways. As illustrated in the figure below, the scenarios for an Oracle SOA Suite on Marketplace topology are:

- Scenario A: All components in a public subnet.
- Scenario B: Load balancer in a public subnet, and remaining components in a private subnet.
- Scenario C: Bastion VM and load balancer in a public subnet, and remaining components in a private subnet.
- Scenario D: Bastion VM in a public subnet, and remaining components in a private subnet.
- Scenario E: All components in a private subnet.



### Scenario A: Public Subnet

In this scenario, the VCN is directly connected to the internet through an *internet gateway*. The gateway is also used for connectivity to your on-premises network. Any resource in the on-premises network that needs to communicate with resources in the VCN must have access to the internet. A SOA server, Database server, and optional load balancers are created in a public subnet. All these resources are assigned a public IP address and can be accessible from the internet. Your on-premises resources will communicate to cloud resources over the public internet. After creating an instance, you can use SSH to connect to it over the internet from your on-premises network or other location on the internet. This setup has default routing rules that are designed to make it easy to get started with Oracle Cloud Infrastructure. When you set up a load balancer or SOA server in a public subnet, you allow SOA runtime traffic from the internet.

### Scenario B, C, and D: Public and Private Subnet

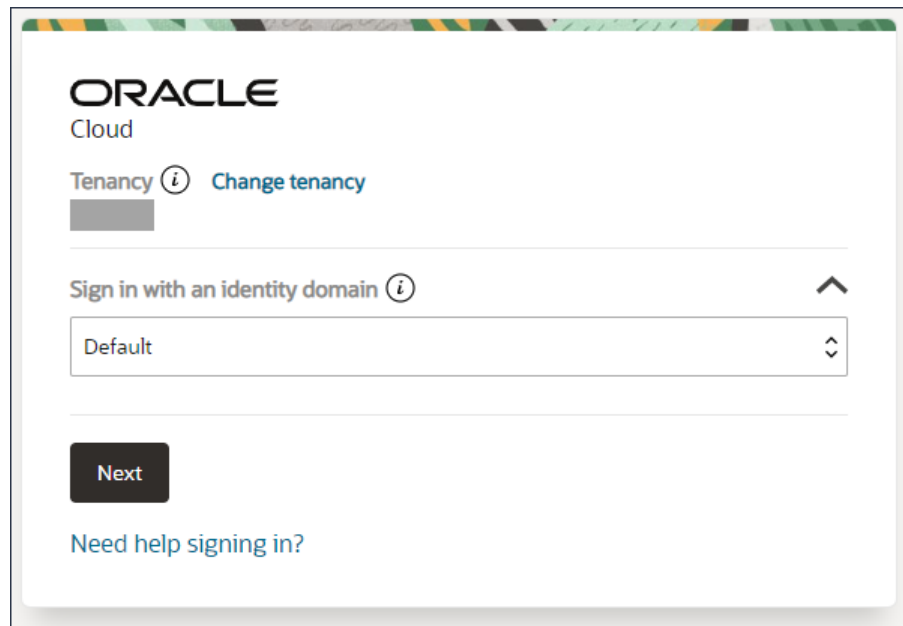
This scenario consists of a virtual cloud network (VCN) with a regional public subnet to hold public servers (such as load balancers) and a regional private subnet to hold private servers (such as a SOA server and Database server). Optionally, you can set up a load balancer and a SOA server on a public subnet and a Database server on a private subnet. Your on-premises resources communicate to cloud resources over the public internet. After creating an instance, you can connect to instances in a public subnet over the internet. The VCN has a *dynamic routing gateway (DRG)* and *IPSec VPN* for connectivity to your on-premises network. After creating an instance, you can use SSH to connect to instances in a private subnet over a DRG/IPSecVPN. You cannot connect to instances in a private subnet over the internet. You need to set up additional routing rules to route traffic from a private subnet to a DRG that allows communication with an on-premises network. When you set up a load balancer or a SOA server in a public subnet, you allow SOA runtime traffic from the internet.

### Scenario E: Private Subnet

This scenario consists of a virtual cloud network (VCN) with a regional private subnet to hold private servers (such as a SOA server, Database server, and load balancers). The VCN has a *dynamic routing gateway (DRG)* and *IPSec VPN* for connectivity to your on-premises network. The VCN has no direct connection to the internet. Any connection to the internet would need to come indirectly through the on-premises network. You cannot connect to instances in a private subnet over the internet. After creating an instance, you can use SSH to connect to instances in a private subnet over a DRG/IPSecVPN. You need to set up additional routing rules to route traffic from a private subnet to a DRG that allows communication with an on-premises network. When you set up a load balancer or SOA server in a private subnet, you allow SOA runtime traffic from your on-premises network only and not from the internet.

## Sign in to the Oracle Cloud Infrastructure Console

1. Go to <http://cloud.oracle.com>.
2. Enter your cloud account name and click **Next**.
3. Sign in to the Oracle Cloud Infrastructure Console:
  - If your cloud account uses identity domains, sign in to the Oracle Cloud Infrastructure Console as a user configured in Oracle Cloud Infrastructure Identity and Access Management (IAM).  
Select the **default** domain.



- If your cloud account does *not* use identity domains, sign in to the Oracle Cloud Infrastructure Console as a user federated through Oracle Identity Cloud Service. Under Single Sign-On (SSO) options, note the identity provider selected in the **Identity Provider** field and click **Continue**.



oic2 Change Tenant

## Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

Identity Providers

oracleidentitycloudservice

**Continue**

---

### Oracle Cloud Infrastructure Direct Sign-In ⓘ

This login is uncommon for federated accounts. If you have questions, please review the [FAQ](#) or contact your tenancy administrator.

User Name

Password

**Sign In** [Forgot Password?](#)

4. Enter the user name and password provided in the welcome email, and click **Sign In**. The Oracle Cloud Infrastructure Console is shown.

## 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.

Prerequisites	Details
License	<ul style="list-style-type: none"> <li>For BYOL, an Oracle SOA Suite 12c (12.2.1.4) license. See <a href="#">About the Oracle SOA Suite on Marketplace License</a>.</li> <li>If Oracle B2B is used, an Oracle B2B license.</li> </ul>
Oracle Cloud Infrastructure resources	<ul style="list-style-type: none"> <li>A compartment for your Oracle SOA Suite on Marketplace instances. See <a href="#">Create a Compartment</a>.</li> <li>A virtual cloud network (VCN) with at least one public subnet. See <a href="#">Set Up a Virtual Cloud Network</a>.</li> <li>If provisioning an Oracle SOA Suite on Marketplace instance in an existing subnet, configure security lists. See <a href="#">Configure Security Lists</a>.</li> <li>A secure shell (SSH) public/private key pair. See <a href="#">Generate a Secure Shell (SSH) Public/Private Key Pair</a>.</li> <li>If using Key Management Service Vault Secrets during provisioning, create vault secrets for storing the passwords. See <a href="#">Creating a Secret in a Vault</a>.</li> </ul>
Database	<ul style="list-style-type: none"> <li>An Oracle Cloud Infrastructure, Autonomous Transaction Processing (ATP), or Oracle Exadata Database Service database that is preprovisioned and provided as an input when configuring an 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 <a href="#">Create an Oracle Database for Oracle SOA Suite on Marketplace</a>.</li> </ul>
(optional) JDeveloper, to deploy SOA projects post-provisioning	<ul style="list-style-type: none"> <li>Oracle JDeveloper 12.2.1.4.0, available from the <a href="#">Oracle JDeveloper Software</a> page.</li> </ul>

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

Oracle Cloud	Create and configure your account on Oracle Cloud. See <a href="#">Overview of Oracle Cloud Subscriptions</a> in <i>Getting Started with Oracle Cloud</i> .
Oracle Compute VMs	Oracle SOA Suite on Marketplace runs on Oracle Compute VMs. See <a href="#">Overview of the Compute Service</a> in the Oracle Cloud Infrastructure documentation.

Oracle WebLogic Server	Applications are deployed to Oracle WebLogic Server. Oracle SOA Suite on Marketplace supports <a href="#">Oracle WebLogic Server 12.2.1.4.0</a> .
Oracle Cloud Infrastructure Load Balancing service	<p>To provide load balancing for applications, Oracle SOA Suite on Marketplace uses the Oracle Cloud Infrastructure load balancer. See <a href="#">Overview of Load Balancing</a> in the Oracle Cloud Infrastructure documentation.</p> <p>Using the load balancer is optional. It is recommended that you use the load balancer when you configure more than one Managed Server in your environment. You can enable the load balancer during provisioning (see <a href="#">Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console</a>) or add it after provisioning (see <a href="#">Add or Delete a Load Balancer Post-Provisioning</a>).</p>

## Create a Compartment

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



### Note:

To create a compartment, your administrator must first add the following policy for your group:

```
allow group groupName to manage compartments in tenancy
```

To create a compartment in Oracle Cloud Infrastructure:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**.  
A list of the existing compartments in your tenancy is displayed.
3. Click **Create Compartment**.
4. 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.
  - **Description:** A friendly description.
5. Click **Create Compartment**.
6. Once the compartment is created, ask your administrator to grant the following `manage` and `use` permissions in the compartment:

- allow group *groupName* to manage instance-family in compartment *compartmentName*
- allow group *groupName* to manage virtual-network-family in compartment *compartmentName*
- allow group *groupName* to manage volume-family in compartment *compartmentName*
- allow group *groupName* to use database-family in compartment *compartmentName*
- allow group *groupName* to use autonomous-database-family in compartment *compartmentName*

where *groupName* is the name of the group to which you belong and *compartmentName* is the name of the compartment where Oracle SOA Suite on Marketplace instances will be created.

## Set Up a Virtual Cloud Network

Set up a Virtual Cloud Network (VCN) for your Oracle SOA Suite on Marketplace 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 on Marketplace 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. Open the navigation menu, click **Networking**, and then click **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.

## Configure Security Lists

If you plan to provision your Oracle SOA Suite on Marketplace instance in an existing subnet, note that the provisioning process will not create any security lists to open ports in the subnets. You must open the ports explicitly before provisioning.

For more information, see [Security Lists](#) in the Oracle Cloud Infrastructure documentation.

Open required ports for your private or public subnet as described in the following scenarios:

- [Private subnet with private endpoint and load balancer](#)
- [Private subnet with private endpoint and without load balancer](#)
- [Private subnet with Bastion instance and load balancer](#)
- [Private subnet with Bastion instance and without load balancer](#)
- [Public subnet with load balancer](#)
- [Public subnet without load balancer](#)

### Note:

- Oracle recommends not to allow traffic from the public internet (0.0.0.0/0) on ports 22, 7002, and 9073. This will expose the instance to malicious traffic. You must configure security rules to allow traffic on these ports from known CIDRs only.
  - Oracle Marketplace servers will connect (`ssh`) to the VM during provisioning and they will report the status to Resource Manager, Stack Jobs. The end user will be able to track the provisioning status.
    - You must allow traffic from Oracle Marketplace servers for provisioning to complete.
    - For Oracle Marketplace server known CIDRs:
      - \* For Government Cloud regions, file a service request (SR) to obtain IP addresses of Oracle Marketplace servers. To file an SR, log in to [My Oracle Support](#), click the **Service Requests** tab, and click **Create Technical SR**.
      - \* For non-Government Cloud regions, see [https://docs.cloud.oracle.com/en-us/iaas/tools/public\\_ip\\_ranges.json](https://docs.cloud.oracle.com/en-us/iaas/tools/public_ip_ranges.json).
- You must allow traffic from CIDRs that are tagged as `OCI`, for your region.

---

### Private subnet with private endpoint and load balancer

Private Subnet	Port Settings
Private endpoint subnet	Port 22 to same subnet CIDR.
Oracle SOA Suite on Marketplace instance subnet	Port 22 to private endpoint subnet CIDR. Port 9073 to load balancer subnet CIDR. All ports to within the same subnet CIDR.
Load balancer subnet	Port 443 to public internet (0.0.0.0/0) to allow SOA runtime traffic.
DB connectivity	Port 1521 to SOA subnet CIDR.

### Private subnet with private endpoint and without load balancer

Private Subnet	Port Settings
Private endpoint subnet	Port 22 to same subnet CIDR.
Oracle SOA Suite on Marketplace instance subnet	Port 22 to private endpoint subnet CIDR. All ports to within the same subnet CIDR.
DB connectivity	Port 1521 to SOA subnet CIDR.

### Private subnet with Bastion instance and load balancer

Private Subnet	Port Settings
Bastion instance subnet	Port 22 to Oracle Marketplace server CIDRs. See <b>Note</b> above.
Oracle SOA Suite on Marketplace instance subnet	Port 22 to Bastion subnet CIDR. Port 9073 to load balancer subnet CIDR. All ports to within the same subnet CIDR.
Load balancer subnet	Port 443 to public internet (0.0.0.0/0) to allow SOA runtime traffic.
DB connectivity	Port 1521 to SOA subnet CIDR.

### Private subnet with Bastion instance and without load balancer

Private Subnet	Port Settings
Bastion instance subnet	Port 22 to Oracle Marketplace server CIDRs. See <b>Note</b> above.
Oracle SOA Suite on Marketplace instance subnet	Port 22 to Bastion subnet CIDR. All ports to within the same subnet CIDR.
DB connectivity	Port 1521 to SOA subnet CIDR.

## Public subnet with load balancer

Public Subnet	Port Settings
<b>Oracle SOA Suite on Marketplace instance subnet</b>	Port 22 to Oracle Marketplace server CIDRs. See <b>Note</b> above.
	Port 9073 to load balancer subnet's CIDR.
	All ports to within the same subnet CIDR.
<b>Load balancer subnet</b>	Port 443 to public internet (0.0.0.0/0) to allow SOA runtime traffic.
<b>DB connectivity</b>	Port 1521 to SOA subnet CIDR.

## Public subnet without load balancer

Public Subnet	Port Settings
<b>Oracle SOA Suite on Marketplace instance subnet</b>	Port 22 to Oracle Marketplace server CIDRs. See <b>Note</b> above.
	Port 9074 to public.
	All ports to within the same subnet CIDR.
<b>DB connectivity</b>	Port 1521 to SOA subnet CIDR.

The following screen shows example ingress rules to allow traffic from Oracle Marketplace servers on port 22 in the Tokyo region:

	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	All		TCP traffic for ports: All	
<input type="checkbox"/>	No	132.145.112.0/20	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	140.238.32.0/19	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	158.101.64.0/19	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	158.101.128.0/19	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	168.138.192.0/19	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	193.123.160.0/20	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	

## Generate 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:

- [About SSH Keys](#)
- [Generate an SSH Key Pair on UNIX and UNIX-Like Platforms Using the ssh-keygen Utility](#)
- [Generate an SSH Key Pair on Windows Using the PuTTYgen Program](#)

## About 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.

## Generate 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
```

### 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.

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.



## Generate 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 download 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.

## Create an Oracle Database for Oracle SOA Suite on Marketplace

If it does not exist, you must create an Oracle database in the same or different compartment as your Oracle SOA Suite on Marketplace instance.

### Note:

For production Oracle SOA Suite on Marketplace instances, Oracle recommends to not share the database with other Oracle SOA Suite on Marketplace instances. If one database is shared across multiple instances, restoring the database will revert the data for all instances.

Oracle SOA Suite on Marketplace supports the following databases:

Database	Supported Versions	Additional Information
Oracle Cloud Infrastructure database, with or without Oracle Real Application Clusters (RAC) <b>Note:</b> If you want to use RAC, you will need to create an Oracle Cloud Infrastructure database instance using the standard service level and <b>Enterprise Edition Extreme Performance</b> for the Oracle Database software edition	<ul style="list-style-type: none"> <li>• Oracle Database 19c</li> <li>• Oracle Database 18c</li> </ul>	<p><b>Note:</b> If you plan to enable SOAINFRA schema partitioning for your Oracle Cloud Infrastructure database, be sure to choose <b>Enterprise Edition High Performance</b> or <b>Enterprise Edition Extreme Performance</b> for the Oracle Database software edition when you create the database.</p> <p>See <b>Oracle Cloud Infrastructure Database Limitations and Usage Notes</b>, below.</p>
Oracle Autonomous Transaction Processing (ATP) database	<ul style="list-style-type: none"> <li>• Oracle Database 19c</li> <li>• Oracle Database 18c</li> </ul>	See <b>Oracle Autonomous Transaction Processing (ATP) Database Limitations and Usage Notes</b> , below.
Oracle Exadata Database Service database	<ul style="list-style-type: none"> <li>• Oracle Database 19c</li> <li>• Oracle Database 18c</li> <li>• Oracle Database 11g Release 2</li> </ul>	Oracle SOA Suite on Marketplace supports Exadata database as a backend database to create SOAINFRA schemas. If you are not familiar with Oracle Exadata Database Service, see <a href="#">Exadata Cloud Service</a> in the Oracle Cloud Infrastructure documentation.

### Oracle Cloud Infrastructure Database Limitations and Usage Notes

- You must have quota to provision the Oracle Cloud Infrastructure database.
- Oracle SOA Suite on Marketplace provisioned with the Oracle Cloud Infrastructure database supports both **Oracle Grid Infrastructure** and **Logical Volume Manager (LVM)** storage management software.
- If you are using Oracle Real Application Clusters (RAC) with the Oracle Cloud Infrastructure database:

- When you configure the compute shape during provisioning or scaling up a node, be sure to stay within the bounds of your available memory.
- Note that Oracle SOA Suite on Marketplace uses the GridLink data source to point to the RAC database.

The following example shows a connect string used to connect to a RAC database:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=vgad c01jjfrac1)(PORT=1522))(ADDRESS=(PROTOCOL=TCP)(HOST=DBHostRAC1)
(PORT=1522))(LOAD_BALANCE=ON)(FAILOVER=ON))
(CONNECT_DATA=(SERVICE_NAME=PDB1.sbcs.cloud.internal)))
```

Name	Type	JNDI Name	Targets
EDNDataSource	GridLink	jdbc/EDNDataSource	soaRACNo_cluster
EDNLocalTxDataSou ce	GridLink	jdbc/ EDNLocalTxDataSou ce	soaRACNo_cluster
LocalSvcTblDataSou rce	GridLink	jdbc/ LocalSvcTblDataSou rce	soaRACNo_adminserv er
mds-owsm	GridLink	jdbc/mds/owsm	soaRACNo_cluster, soaRACNo_adminserv er
mds-soa	GridLink	jdbc/mds/ MDS_LocalTxDataSou rce	soaRACNo_cluster, soaRACNo_adminserv er
opss-audit-DBDS	GridLink	jdbc/ AuditAppendDataSou rce	soaRACNo_cluster, soaRACNo_adminserv er
opss-audit-viewDS	GridLink	jdbc/ AuditViewDataSou rce	soaRACNo_cluster, soaRACNo_adminserv er
opss-data-source	GridLink	jdbc/ OpssDataSource	soaRACNo_cluster, soaRACNo_adminserv er
OraSDPMDDataSource	GridLink	jdbc/ OraSDPMDDataSource	soaRACNo_cluster
SOADataSource	GridLink	jdbc/SOADataSource	soaRACNo_cluster

### Oracle Autonomous Transaction Processing (ATP) Database Limitations and Usage Notes

- Oracle SOA Suite on Marketplace supports both *serverless deployments* and *dedicated deployments* (ATP-D) of the ATP database.
- DBFS is not configured when using the ATP database.
- Oracle SOA Suite on Marketplace supports the Database Adapter for the ATP database. See [Oracle JCA Adapter for Database](#) in *Understanding Technology Adapters*.
- A two-node Oracle SOA Suite on Marketplace cluster consumes the maximum connections supported by one OCPU ATP database. An increase in cluster size requires a

proportional increase in the OCPU count of ATP database. That is, a four-node cluster needs at least two OCPU ATP databases.

- The ATP database is *not* supported with the **Business Activity Monitoring** service type.
- Oracle SOA Suite on Marketplace does not support the Always Free Autonomous database. Instead, use the paid ATP database with Oracle SOA Suite on Marketplace.

**Topics:**

- [Create an Oracle Cloud Infrastructure Database for Oracle SOA Suite on Marketplace](#)
- [Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Suite on Marketplace](#)

## Create an Oracle Cloud Infrastructure Database for Oracle SOA Suite on Marketplace

 **Note:**

If you are using network security groups, ensure that you configure the required rules for port 1521. For more information, see [Network Security Groups](#) in the Oracle Cloud Infrastructure documentation.

To create an Oracle Cloud Infrastructure database for Oracle SOA Suite on Marketplace:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Oracle Database**, and then click **Bare Metal, VM, and Exadata**.
3. Choose the **Compartment** in which to create the database, and then click **Create DB System**.
4. In the Create DB System wizard, provide the information for the database. See the [Oracle Cloud Infrastructure documentation](#) for field descriptions.

 **Notes:**

- Oracle SOA Suite on Marketplace provisioned with the Oracle Cloud Infrastructure database supports both **Oracle Grid Infrastructure** and **Logical Volume Manager (LVM)** storage management software.
- If you plan to enable SOAINFRA schema partitioning for your Oracle Cloud Infrastructure database, be sure to choose **Enterprise Edition High Performance** or **Enterprise Edition Extreme Performance** for the Oracle Database software edition.

5. 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).
6. 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.

- Note the IP addresses. You'll need the private or public IP address, depending on network configuration, to connect to the DB system.

## Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Suite on Marketplace

### Note:

If you are using network security groups, ensure that you configure the required rules for port 1521. For more information, see [Network Security Groups](#) in the Oracle Cloud Infrastructure documentation.

To create an Oracle Autonomous Transaction Processing (ATP) database for Oracle SOA Suite on Marketplace:

- Sign in to the Oracle Cloud Infrastructure Console.
- Open the navigation menu and click **Oracle Database**. Under **Autonomous Database**, click **Autonomous Transaction Processing**.

The screenshot shows the 'Create Autonomous Database' wizard in the Oracle Cloud Infrastructure console. The form is titled 'Create Autonomous Database' and is divided into several sections:

- Provide basic information for the Autonomous Database:**
  - Compartment: SOACompartment (dropdown menu)
  - Display name: ATPDevDB (text input field)
  - Database name: DB202 (text input field)
- Choose a workload type:**
  - Data Warehouse (unselected)
  - Transaction Processing (selected, indicated by a checkmark)
- Choose a deployment type:**
  - Shared Infrastructure (unselected)
  - Dedicated Infrastructure (selected, indicated by a checkmark)
- Choose Autonomous Container Database:**
  - Compartment: FleetCompartment (dropdown menu)
  - High Availability Container Database: InternalACD (pEF:PHX-AD-3) (dropdown menu)
- Configure the database:**
  - CPU Count: (text input field)
  - Storage (TB): (text input field)

At the bottom of the form, there are two buttons: 'Create Autonomous Database' (highlighted in blue) and 'Cancel'.

- In the Create Autonomous Database wizard, provide the information for the database. See the [Oracle Cloud Infrastructure documentation](#) for field descriptions.
- Click **Create Autonomous Database**. The ATP database appears in the list with a status of **Provisioning**. The icon changes from yellow to green (or red to indicate errors).
- Wait for the ATP database's icon to turn green, with a status of **Available**, and then click the highlighted ATP database name.

Details about the ATP database are displayed.

6. Note the IP addresses; you'll need the private or public IP address, depending on network configuration, to connect to the ATP database.

# 4

## Create and View Oracle SOA Suite on Marketplace Instances

After provisioning an Oracle SOA Suite on Marketplace instance, you may need to complete post-provisioning and other administrative tasks, depending on the requirements of the instance.

### Topics:

- [Provision an Oracle SOA Suite on Marketplace Instance](#)
- [Complete Post-Provisioning Tasks](#)
- [View Oracle SOA Suite on Marketplace Instance Details](#)
- [Access an Oracle SOA Suite on Marketplace Instance](#)

## Provision an Oracle SOA Suite on Marketplace Instance

You can provision an Oracle SOA Suite on Marketplace instance in a selected compartment in Oracle Cloud Infrastructure, as a quick start, or using the command line interface.

### Topics:

- [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#)
- [Provision an Oracle SOA Suite on Marketplace Quick Start Instance](#)
- [Provision an Oracle SOA Suite on Marketplace Instance Using the Oracle Cloud Infrastructure Command Line Interface](#)
- [Provision an Oracle SOA Suite on Marketplace Instance Using Oracle Cloud Infrastructure REST APIs](#)

# Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console

You can provision an Oracle SOA Suite on Marketplace instance in a selected compartment in Oracle Cloud Infrastructure. The database and Oracle SOA Suite on Marketplace instance can be in the same or different compartment.

## Notes:

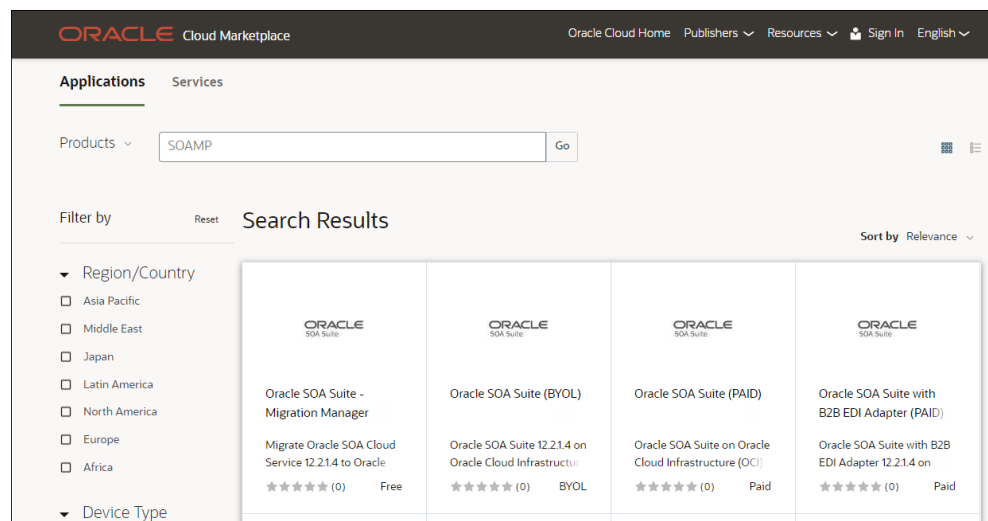
- Before you begin these steps, make sure that you have met the necessary [Prerequisites](#).
- When you provision an Oracle SOA Suite on Marketplace instance with a private subnet, you must select either an existing Private Endpoint or a Bastion VM, or create a new Bastion VM (see [Understand Oracle SOA Suite on Marketplace Topologies](#)). The newly created Bastion VM will use an Oracle Linux 7.x image, which is free to use (only the instance's OCPU and memory usage will be billed). The Bastion VM is associated with the Oracle SOA Suite on Marketplace instance stack and will be deleted when the stack is deleted (**Terraform Actions > Destroy**). You can delete just the Bastion VM once the provisioning process is completed. If you provision another instance in the same subnet, you will need to choose another Bastion VM that is associated to second stack. Note that scale out and scale in operations will create a new Bastion VM if it does not exist. You can delete this Bastion VM after scale out and scale in operations.
- With administration privileges in Oracle Cloud Infrastructure, you can deprovision compute instances from an Oracle SOA Suite on Marketplace cluster. To delete nodes from a cluster when you no longer need the cluster, it is recommended that you use **Terraform Actions > Destroy** (see [Deprovision an Oracle SOA Suite on Marketplace Instance](#)). As a best practice, use a dedicated compartment for provisioning Oracle SOA Suite on Marketplace 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.
- If provisioning of an Oracle SOA Suite on Marketplace instance fails, check for the following common causes of failure:
  - Before provisioning in an existing subnet, verify that port 1521 is open for database connectivity in the ingress rules. See [Configure Security Lists](#).
  - If you select a **Database Strategy** of **Database System** in the provisioning screens, verify that the following values are correct:
    - \* the name of the pluggable database (**PDB**)
    - \* the **Database Administrator Password**
  - Verify that the user who submitted the provisioning request is part of the Oracle Cloud Infrastructure IAM Administrator group or part of a group that is authorized to manage network and compute resources.
  - If you select **Enable SOA DB Schema Partitioning**, verify that the Oracle Database software edition is **Enterprise Edition High Performance** or **Enterprise Edition Extreme Performance**.



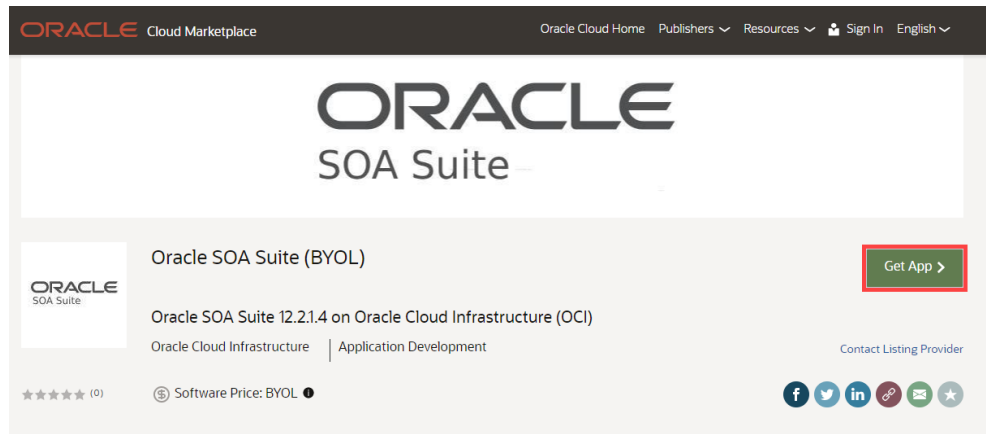
- If you use a custom DNS resolver and provisioning times out for a cluster with more than 4 nodes, verify that the custom DNS resolver is configured correctly.
- If provisioning continues to fail, file a service request (SR) at [My Oracle Support](#) (click the **Service Requests** tab, and click **Create Technical SR**):
  - \* Use the `ssh` command to [connect to the Administration Server VM](#) that failed to provision the Oracle SOA Suite on Marketplace instance and provide `/u01/logs/*.log` from all the nodes for analysis.

To provision an Oracle SOA Suite on Marketplace instance:

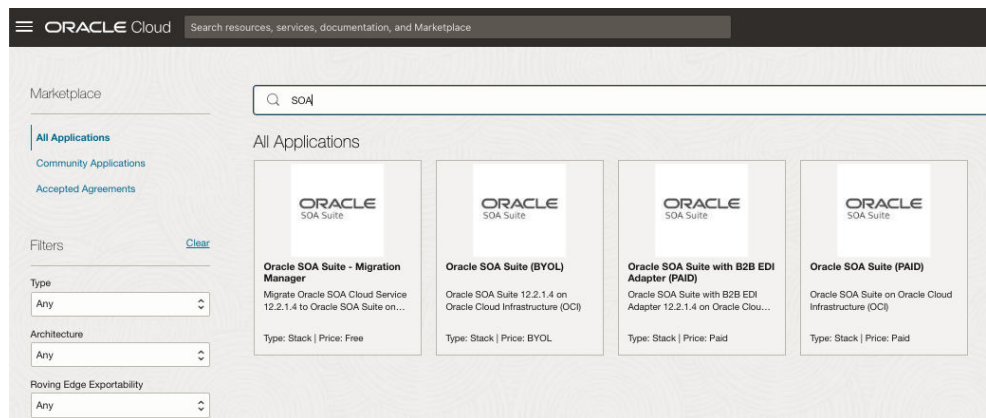
1. Navigate to the SOA Suite 12.2.1.4 listing on Marketplace by direct URL or by browsing in Oracle Cloud Infrastructure:
  - **Direct URL:**
    - a. In your browser, enter [https://cloudmarketplace.oracle.com/marketplace/en\\_US/homePage.jsp?tag=SOAMP](https://cloudmarketplace.oracle.com/marketplace/en_US/homePage.jsp?tag=SOAMP).  
The Marketplace listings for SOA Suite 12.2.1.4 are displayed.



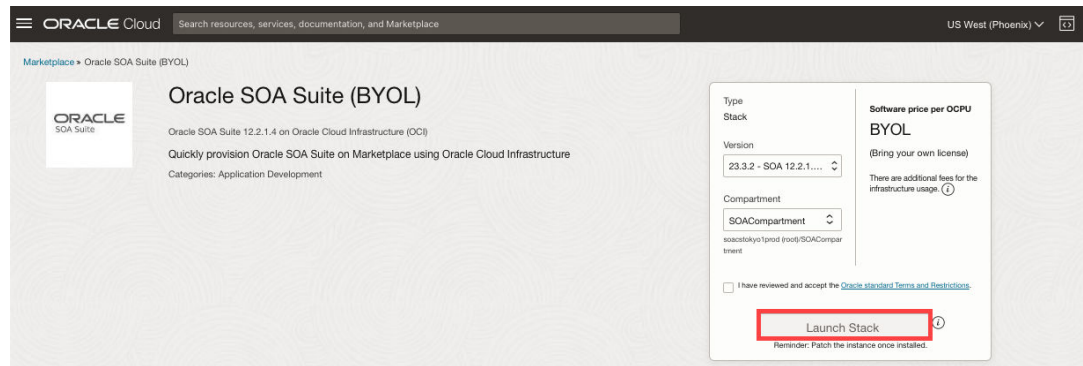
- b. Click the title for the listing you want to use to open the landing page, and review the information on the **Overview** page.
- c. Click **Get App**.



- d. Select your Oracle Cloud Infrastructure region and click **Sign In**.
- e. [Sign in to the Oracle Cloud Infrastructure Console](#).
- **Browsing:**
  - a. [Sign in to the Oracle Cloud Infrastructure Console](#).
  - b. Open the navigation menu and click **Marketplace**. Under **Marketplace**, click **All Applications**.
  - c. In the Marketplace search field, enter `SOA`. The Marketplace listings for SOA Suite 12.2.1.4 are displayed.



- d. Click the title for the listing you want to use to open the landing page, and review the information on the **Overview** page.
2. Accept the terms and restrictions, then click **Launch Stack**.



The Create Stack wizard is displayed.

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

Field Label	Description
<b>Name</b>	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).
<b>Description</b>	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.

Field Label	Description
Create in compartment	<p>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.)</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>If not already granted, you will need to ask your administrator to grant the following manage and use permissions in the compartment:</p> <ul style="list-style-type: none"> <li>• allow group <i>groupName</i> to manage instance-family in compartment <i>compartmentName</i></li> <li>• allow group <i>groupName</i> to manage virtual-network-family in compartment <i>compartmentName</i></li> <li>• allow group <i>groupName</i> to manage volume-family in compartment <i>compartmentName</i></li> <li>• allow group <i>groupName</i> to use database-family in compartment <i>compartmentName</i></li> <li>• allow group <i>groupName</i> to use autonomous-database-family in compartment <i>compartmentName</i></li> </ul> <p>where <i>groupName</i> is the name of the group to which you belong and <i>compartmentName</i> is the name of the compartment where Oracle SOA Suite on Marketplace instances will be created.</p> </div>
Terraform version	Automatically populated with the Terraform version used for the Marketplace offering.
Tags	<p>Optionally, select existing tags or add tags to associate with the stack. For more information about tagging, see <a href="#">Resource Tags</a>.</p> <p>If you do not assign tags during provisioning, you can create and manage tags after the stack is created.</p>

4. Click **Next** and configure the instance as described in the following table.

Field Label	Description
<b>Server Instance</b>	
<b>Instance Name Prefix</b>	Enter the prefix you wish to use for the instance name, up to 15 characters.
<b>Service Type</b>	<p>Select the service type you are provisioning:</p> <ul style="list-style-type: none"> <li>• <b>SOA with SB &amp; B2B Cluster</b></li> <li>• <b>MFT Cluster</b></li> <li>• <b>BAM Cluster</b></li> </ul> <p><b>Note:</b> In this guide, <i>Oracle SOA Suite</i> refers to any of the three service types.</p>
<b>Enable SOA DB Schema Partitioning</b>	<p>If you selected a <b>Service Type</b> of <b>SOA with SB &amp; B2B Cluster</b>, select this check box to enable SOAINFRA schema partitioning.</p> <p>Default: not selected.</p> <p><b>Note:</b> If you enable SOAINFRA schema partitioning for your database, be sure to choose <b>Enterprise Edition High Performance</b> or <b>Enterprise Edition Extreme Performance</b> for the Oracle Database software edition when you create the database.</p>
<b>Compute Shape</b>	<p>Select a compute shape with at least 15GB of memory. For information about compute shapes, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Compute - Virtual Machine Instances</a></li> <li>• <a href="#">Standard Shapes</a> in the Oracle Cloud Infrastructure documentation.</li> </ul> <p>The available compute shapes (<b>VM.Standard3.Flex</b>, <b>VM.Standard.E4.Flex</b>, and <b>VM.Optimized3.Flex</b>) allow you to customize the following values for Oracle SOA Suite on Marketplace instances:</p> <ul style="list-style-type: none"> <li>• OCPU count:           <ul style="list-style-type: none"> <li>– Minimum: 2</li> <li>– Miximum: 18</li> </ul> </li> <li>• Memory size:           <ul style="list-style-type: none"> <li>– Minimum: 15GB</li> <li>– Miximum: 256GB</li> </ul> </li> </ul> <p><b>Note:</b> Flexible compute shapes are not supported for a Bastion instance.</p> <p>You can change the compute shape post-provisioning by scaling up the Oracle SOA Suite on Marketplace instance. See <a href="#">Scale an Oracle SOA Suite on Marketplace Instance Up or Down</a>.</p>
<b>Enable Secure Boot</b>	<p>Select to prevent unauthorized boot loaders and operating systems from booting.</p> <p>For more information, see <a href="#">Shielded Instances</a> in the <i>Oracle Cloud Infrastructure documentation</i>.</p>

Field Label	Description
<b>Enable Measured Boot</b>	<p>Select to enhance boot security by taking and storing measurements of boot components, such as bootloaders, drivers, and operating systems. The Trusted Platform Module (TPM) securely stores boot measurements.</p> <p><b>Note:</b> Bare metal instances do not support Measured Boot.</p> <p>For more information, see <a href="#">Shielded Instances</a> in the <i>Oracle Cloud Infrastructure documentation</i>.</p>
<b>SSH Public Key</b>	<p>Enter the public key for the secure shell (SSH), either by providing an SSH key file or pasting the SSH key. This key is used for authentication when connecting to the Oracle SOA Suite on Marketplace instance using an SSH client. See <a href="#">Generate a Secure Shell (SSH) Public/Private Key Pair</a>.</p>
<b>Cluster Node Count</b>	<p>Enter the initial number of SOA Server compute instances. This is also the number of Managed Servers in the cluster.</p> <p>During provisioning, the maximum allowable cluster size is 8 nodes. If you want to create a cluster of a larger size, you can create a 8-node cluster during provisioning and then post-provisioning you can scale out the cluster to a maximum size of 16 nodes. See <a href="#">Scale Out an Oracle SOA Suite on Marketplace Instance Cluster</a>.</p>
<b>Administration Username</b>	<p>Enter the name of the SOA Server domain administrator.</p>
<b>Administration Password</b>	<p>Enter a password that meets the specifications shown below the field. Enter the password again for confirmation.</p>
<b>WebLogic Server Admin Secret Compartment Validated Secrets OCID for Administration password</b>	<p>If you selected <b>Use KMS Vault Secrets for passwords</b>:</p> <ul style="list-style-type: none"> <li>• Select the compartment for the WebLogic Server administration secret.</li> <li>• Select the OCID of the secret that contains the WebLogic Server administration password.</li> </ul>
<b>Domain Volume Size (GB)</b>	<p>Enter a custom domain block volume size for the instance. Default (minimum): 50GB</p> <p>You can increase the domain volume size post-provisioning by editing the stack. You cannot decrease the domain volume size. See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a>.</p>
<b>Key Management Service Configuration</b>	

Field Label	Description
<b>Use KMS Vault Secrets for passwords</b>	<p>Select this check box to enable KMS vault secrets for passwords. The KMS secrets must be created prior to provisioning an Oracle SOA Suite on Marketplace instance. On selection, fields in the provisioning UI support selections for KMS secrets for passwords:</p> <ul style="list-style-type: none"> <li>For WebLogic Server administration: <b>WebLogic Server Admin Secret Compartment and Validated Secrets OCID for Nodemanager password</b></li> <li>For WebLogic Server nodemanager: <b>WebLogic Server Nodemanager Secret Compartment and Validated Secrets OCID for Nodemanager password</b></li> <li>For OCI database: <b>OCI DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>For ATP database: <b>ATP DB Secret Compartment and Validated Secrets OCID for Autonomous Database ADMIN password</b></li> <li>For Exadata database: <b>Exadata DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>For database connection string: <b>External DB Secret Compartment and Validated Secrets OCID for Database Administrator Password</b></li> <li>For RCU schema: <b>RCU Schema Secret Compartment and Validated Secrets OCID for Custom RCU Schema Password</b></li> <li>For ATP DB wallet: <b>ATP DB Wallet Secret Compartment and Validated Secrets OCID for ATP DB Wallet Password</b></li> </ul> <p>Selecting this checkbox also exposes the <b>Backup/Restore Configuration</b> section (see below).</p>
<b>OCI Policies</b>	Select this check box to create required OCI policies to access the KMS secrets from the vault during provisioning.
<b>Instance Network</b>	
<b>Network Compartment</b>	Automatically populated with the compartment you selected on the landing page. This is the compartment where the instance will be created in the tenancy.
<b>Virtual Cloud Network Strategy</b>	Select either <b>Create New VCN</b> or <b>Use Existing VCN</b> in which to create the instance, network resources, and load balancer.
<b>SOA Server Network</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Create New VCN</b> , enter the name of the new VCN.
<b>SOA Server Network CIDR</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Create New VCN</b> , enter the unique CIDR to assign to the new VCN.
<b>Existing Network</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Use Existing VCN</b> , select the name of the VCN.

Field Label	Description
<b>Use Network Security Group for SOA Instance</b> <b>Note:</b> You can also edit an Oracle SOA Suite on Marketplace instance post-provisioning to disable and enable this option.	<p>If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Use Existing VCN</b>, select this check box to use a network security group (NSG) for controlling traffic to the Oracle SOA Suite on Marketplace compute instances.</p> <p>If you do not select this option, the compute instance uses the security list of the respective subnet.</p>
<b>NSG Compartment</b>	If you selected <b>Use Network Security Group for SOA Instance</b> , select the NSG's compartment.
<b>SOA Network Security Group</b>	If you selected <b>Use Network Security Group for SOA Instance</b> , select the NSG to be used for controlling traffic to the Oracle SOA Suite on Marketplace compute instance.
<b>Subnet Strategy</b>	<p>Select either <b>Create New Subnet</b> or <b>Use Existing Subnet</b>.</p> <p>If you use an existing subnet, note that the provisioning process will not create any security lists to open ports in the subnets. You must open the ports explicitly before provisioning. See <a href="#">Configure Security Lists</a>.</p>
<b>Subnet Compartment</b>	Select the compartment in which to create the new or existing subnet.
<b>Subnet Type</b>	Select either a public or private subnet.
<b>Subnet Span</b>	Select either a region or <b>AD Specific Subnet</b> to create the instance in an availability domain.
<b>Availability Domain</b>	<p>If you selected a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and a <b>Subnet Span</b> of <b>AD Specific Subnet</b>, select the name of the availability domain in which to create the instance.</p> <p><b>Note:</b> For a regional subnet, the nodes in an Oracle SOA Suite on Marketplace cluster are distributed evenly across all available availability domains.</p>
<b>Existing Subnet</b>	<p>If you selected a <b>Subnet Strategy</b> of <b>Use Existing Subnet</b>, select an existing subnet to use for the instance. This subnet must already be present in the chosen VCN.</p> <p>If you use an existing subnet, note that the provisioning process will not create any security lists to open ports in the subnets. You must open the ports explicitly before provisioning. See <a href="#">Prerequisites</a>.</p>
<b>Subnet CIDR</b>	If you selected a <b>Subnet Strategy</b> of <b>Create New Subnet</b> , enter the unique CIDR of the new subnet to create for the instance.



Field Label	Description
<b>Bastion Strategy</b>	<p>If you selected a <b>Subnet Strategy</b> of <b>Use Existing Subnet</b>, and a <b>Subnet Type</b> of <b>Use Private Subnet</b>, select a Bastion strategy:</p> <ul style="list-style-type: none"> <li>• (Default) <b>Use Private Endpoint</b> to use a private endpoint instead of a Bastion host for provisioning and scale out operations. A private endpoint enables private SSH access to compute instances created during provisioning of Oracle SOA Suite on Marketplace instances on a private subnet. <b>Note:</b> To use this feature, you must add security policies to your tenancy. See <a href="#">Manage Private Endpoints</a> in the Oracle Cloud Infrastructure documentation.</li> <li>• <b>Create New Bastion Instance</b> to create a new Bastion host for every SOA cluster</li> <li>• <b>Use Existing Bastion Instance</b> to use an existing Bastion host for every SOA cluster</li> </ul>
<b>Private Endpoint Strategy</b>	<p>If you selected a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b>, select either <b>Create New Private Endpoint</b> or <b>Use Existing Private Endpoint</b>.</p>
<b>Private Endpoint Compartment</b>	<p>Select the compartment in which to create the new private endpoint, or find the existing private endpoint.          This field is shown when you select:</p> <ul style="list-style-type: none"> <li>• a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and a <b>Subnet Type</b> of <b>Use Private Subnet</b></li> <li>• or, a <b>Subnet Strategy</b> of <b>Using Existing Subnet</b>, a <b>Subnet Type</b> of <b>Use Private Subnet</b>, and a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b></li> </ul>
<b>Private Subnet Compartment</b>	<p>Select the compartment for the new private endpoint subnet.          This field is shown when you select:</p> <ul style="list-style-type: none"> <li>• a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and a <b>Subnet Type</b> of <b>Use Private Subnet</b></li> <li>• or, a <b>Subnet Strategy</b> of <b>Using Existing Subnet</b>, a <b>Subnet Type</b> of <b>Use Private Subnet</b>, a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b>, and a <b>Private Endpoint Strategy</b> of <b>Create New Private Endpoint</b></li> </ul>
<b>Private Endpoint Subnet</b>	<p>If you selected a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b> and a <b>Private Endpoint Strategy</b> of <b>Create New Private Endpoint</b>, select a private subnet for creating the private endpoint.</p>
<b>Private Endpoint Subnet CIDR</b>	<p>If you selected a <b>Subnet Strategy</b> of <b>Create New Subnet</b>, and a <b>Subnet Type</b> of <b>Use Private Subnet</b>, enter the unique CIDR of the new subnet to create for the private endpoint. The new subnet's CIDR should not overlap with any other subnet CIDRs.</p>

Field Label	Description
<b>Use Network Security Group for Private Endpoint</b>	<p>select this check box to use a network security group (NSG) for controlling traffic to the private endpoint.</p> <p>This check box is shown when you select:</p> <ul style="list-style-type: none"> <li>• a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and a <b>Subnet Type</b> of <b>Use Private Subnet</b></li> <li>• or, a <b>Subnet Strategy</b> of <b>Using Existing Subnet</b>, a <b>Subnet Type</b> of <b>Use Private Subnet</b>, a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b>, and a <b>Private Endpoint Strategy</b> of <b>Create New Private Endpoint</b></li> </ul>
<b>Network Security Group Compartment</b>	If you selected <b>Use Network Security Group for Private Endpoint</b> , select the NSG's compartment.
<b>Private Endpoint Network Security Group</b>	If you selected <b>Use Network Security Group for Private Endpoint</b> , select the NSG to be used for controlling traffic to the private endpoint.
<b>Private Endpoint Display Name</b>	If you selected a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b> and a <b>Private Endpoint Strategy</b> of <b>Create New Private Endpoint</b> , enter a display name for the private endpoint.
<b>Existing Private Endpoint</b>	If you selected a <b>Bastion Strategy</b> of <b>Use Private Endpoint</b> and a <b>Private Endpoint Strategy</b> of <b>Use Existing Private Endpoint</b> , select the private endpoint to be used during provisioning of the instance.
<b>Bastion Host Subnet Compartment</b>	If you selected a <b>Bastion Strategy</b> of <b>Create New Bastion Instance</b> , select the compartment in which to create the new Bastion host subnet.
<b>Existing Subnet for Bastion Host</b>	If you selected a <b>Bastion Strategy</b> of <b>Create New Bastion Instance</b> , select an existing public subnet to use for a Bastion compute instance. This subnet must already be present in the chosen VCN. This field is required only if you did not assign public IP addresses to WebLogic Server.
<b>Bastion Host Shape</b>	<p>If you selected a <b>Bastion Strategy</b> of <b>Create New Bastion Instance</b>, select the shape of the Bastion instance.</p> <p><b>Note:</b> Flexible compute shapes are not supported for a Bastion instance.</p>
<b>Public IP of Bastion Instance</b>	If you selected a <b>Bastion Strategy</b> of <b>Use Existing Bastion Instance</b> , enter the public IP address of the existing Bastion instance.
<b>SSH Private Key Bastion Instance</b>	<p>If you selected a <b>Bastion Strategy</b> of <b>Use Existing Bastion Instance</b>, enter the SSH private key of the existing Bastion instance.</p> <p><b>Note:</b> the SSH private key must <i>not</i> be passphrase-protected.</p>

Field Label	Description
<b>Bastion Host Subnet CIDR</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Create New VCN</b> a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and a <b>Subnet Type</b> of <b>Use Private Subnet</b> , enter the unique CIDR of the new subnet to create for a Bastion compute instance. This is required only if you did not assign a public IP address to SOA Server.
<b>Use Network Security Group for Bastion Host</b>	If you selected a <b>Bastion Strategy</b> of <b>Create New Bastion Instance</b> , select this check box to use a network security group (NSG) for controlling traffic to the Bastion host.
<b>NSG Compartment</b>	If you selected <b>Use Network Security Group for Bastion Host</b> , select the NSG's compartment.
<b>Bastion Network Security Group</b>	If you selected <b>Use Network Security Group for Bastion Host</b> , select the NSG to be used for controlling traffic to the Bastion host.
<b>Provision Load Balancer</b> <b>Note:</b> You can also edit an Oracle SOA Suite on Marketplace instance post-provisioning to disable and enable this option.	Select this check box to enable the Oracle Cloud Infrastructure load balancer to distribute traffic. For more information, see <a href="#">Overview of Load Balancing</a> in the Oracle Cloud Infrastructure documentation. Enabling a load balancer is optional. If you decide you want to add one later, see <a href="#">Add or Delete a Load Balancer Post-Provisioning</a> .
<b>Load Balancer Strategy</b>	If you selected <b>Provision Load Balancer</b> , select whether to create a new load balancer or use an existing load balancer.
<b>Load Balancer Compartment</b>	If you selected <b>Provision Load Balancer</b> , select the compartment to create a new load balancer or use an existing load balancer.
<b>Existing Load Balancer</b>	If you selected <b>Provision Load Balancer</b> and <b>Use Existing Load Balancer</b> , select the existing load balancer to use.
<b>Load Balancer Subnet Compartment</b>	If you selected <b>Provision Load Balancer</b> , select the compartment in which to create the new or existing load balancer subnet. You can change the load balancer subnet compartment post-provisioning by editing the stack. See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a> .
<b>Load Balancer Subnet Type</b>	If you selected a <b>Subnet Type</b> of <b>Use Private Subnet</b> and <b>Provision Load Balancer</b> , select to use either a private or a public subnet for the load balancer.
<b>Load Balancer Subnet CIDR</b>	If you selected a <b>Subnet Strategy</b> of <b>Create New Subnet</b> and <b>Provision Load Balancer</b> , enter the CIDR of the new subnet to create for the load balancer. The new subnet's CIDR should not overlap with any other subnet CIDRs.

Field Label	Description
<b>Existing Subnet for Load Balancer</b>	<p>If you selected a <b>Subnet Strategy of Use Existing Subnet</b> and <b>Provision Load Balancer</b>, select an existing subnet to use for the load balancer. This subnet must already be present in the chosen VCN.</p> <p>You can change the load balancer subnet post-provisioning by editing the stack. See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a>.</p>
<b>Load Balancer Shape</b>	<p>If you selected <b>Provision Load Balancer</b>, select the load balancer shape: <b>100Mbps</b>, <b>400Mbps</b>, <b>8000Mbps</b>, or <b>Flexible</b>.</p> <p>If you select <b>Flexible</b>, the provisioning wizard exposes two fields to specify the minimum and maximum bandwidth for the load balancer:</p> <ul style="list-style-type: none"> <li>• <b>Minimum size of Flexible Shape (Mbps)</b></li> <li>• <b>Maximum size of Flexible Shape (Mbps)</b></li> </ul> <p>Enter a minimum bandwidth value greater than or equal to 10, and a maximum bandwidth value less than or equal to 8000. To set a fixed load balancer shape, set both the minimum and maximum bandwidth value to the same required load balancer shape.</p> <p>You can change the load balancer shape post-provisioning by editing the stack. See <a href="#">Edit an Oracle SOA Suite on Marketplace Instance</a>.</p>
<b>Use Network Security Group for Load Balancer</b>	<p>If you selected <b>Provision Load Balancer</b>, select this check box to use a network security group (NSG) for controlling traffic to the load balancer.</p>
<b>NSG Compartment</b>	<p>If you selected <b>Use Network Security Group for Load Balancer</b>, select the NSG's compartment.</p>
<b>Load Balancer Network Security Group</b>	<p>If you selected <b>Use Network Security Group for Load Balancer</b>, select the NSG to be used for controlling traffic to the load balancer.</p>
<b>Database</b>	

Field Label	Description
<b>Database Strategy</b>	<p>Select the database strategy for WebLogic Server:</p> <ul style="list-style-type: none"> <li>• <b>Database System</b> (the Oracle Cloud Infrastructure database), supported for any service type.</li> <li>• <b>Autonomous Transaction Processing Database</b>, supported for the <b>SOA with SB &amp; B2B Cluster</b> and <b>MFT Cluster</b> service types.</li> <li>• <b>Exadata Database</b>, supported for any service type.</li> <li>• <b>Database Connection String</b>. This option is only for advanced users, and not recommended. If selected, enter a value in <b>Database Connection String</b> using syntax <i>host:port/serviceName</i>. For example:  <pre>demodb- scan.demodb.demovcn.oraclevcn.com: 1521/ PDB1.demodb.demovcn.oracle.vcn.com</pre> </li> </ul>
<b>DB System Compartment</b> <b>Autonomous DB System Compartment</b>	Select the compartment for the database. This can be the same compartment as the Oracle SOA Suite on Marketplace instance, or a different compartment.
<b>DB System</b> <b>Autonomous Database</b>	Select the DB system to use for this WebLogic Server domain. This should be in the same VCN as WebLogic instances.
<b>Database home in the DB System</b>	If you selected a <b>Database Strategy</b> of <b>Database System</b> , select the database home within the DB system.
<b>Database in the DB System</b>	If you selected a <b>Database Strategy</b> of <b>Database System</b> , select the database in which to provision the schemas for a JRF-enabled WebLogic Server domain.
<b>PDB</b>	If you selected a <b>Database Strategy</b> of <b>Database System</b> , enter the name of the pluggable database (PDB) in which to provision the schemas for a JRF-enabled WebLogic Server domain.
<b>Exadata SCAN DNS Name</b>	If you selected a <b>Database Strategy</b> of <b>Exadata Database</b> , enter the SCAN DNS name of the Exadata VM cluster. Refer to the Exadata VM cluster details page in the Oracle Cloud Infrastructure Console for the SCAN DNS name..
<b>PDB Service name</b>	If you selected a <b>Database Strategy</b> of <b>Database System</b> or <b>Exadata Database</b> , enter the full service name of the pluggable database (PDB) in which to provision the schemas for a JRF-enabled WebLogic Server domain.
<b>Database Administrator</b>	If you selected a <b>Database Strategy</b> of <b>Database System</b> or <b>Exadata Database</b> , enter the name of a database user with DBA privileges.
<b>Database Administrator Password</b> <b>Autonomous Database Admin Password</b>	Enter a password for the database administrator.

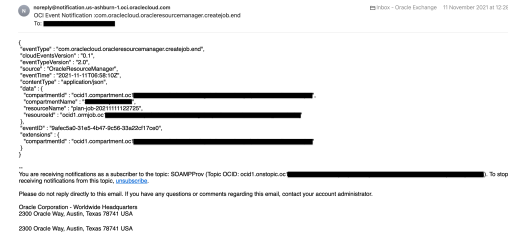

Field Label	Description
<b>OCI DB Secret Compartment Validated Secrets OCID for Database Administrator Password</b>	<p>If you selected a <b>Database Strategy</b> of <b>Database System</b> and you selected <b>Use KMS Vault Secrets for passwords</b>:</p> <ul style="list-style-type: none"> <li>Select the compartment for the OCI database secret.</li> <li>Select the OCID of the secret that contains the password for the OCI database administrator.</li> </ul>
<b>Exadata DB Secret Compartment Validated Secrets OCID for Database Administrator Password</b>	<p>If you selected a <b>Database Strategy</b> of <b>Exadata Database</b> and you selected <b>Use KMS Vault Secrets for passwords</b>:</p> <ul style="list-style-type: none"> <li>Select the compartment for the Exadata database secret.</li> <li>Select the OCID of the secret that contains the password for the Exadata database administrator.</li> </ul>
<b>ATP DB Secret Compartment Validated Secrets OCID for Autonomous Database ADMIN password</b>	<p>If you selected a <b>Database Strategy</b> of <b>Autonomous Transaction Processing Database</b> and you selected <b>Use KMS Vault Secrets for passwords</b>:</p> <ul style="list-style-type: none"> <li>Select the compartment for the ATP database secret.</li> <li>Select the OCID of the secret that contains the password for the ADMIN user in the ATP database.</li> </ul>
<b>External DB Secret Compartment Validated Secrets OCID for Database Administrator Password</b>	<p>If you selected a <b>Database Strategy</b> of <b>Database Connection String</b> and you selected <b>Use KMS Vault Secrets for passwords</b>:</p> <ul style="list-style-type: none"> <li>Select the compartment for the external database secret.</li> <li>Select the OCID of the secret that contains the password for the external database administrator.</li> </ul>
<b>Autonomous Database Service Level</b>	<p>If you selected a <b>Database Strategy</b> of <b>Autonomous Transaction Processing Database</b>, select the service level that the WebLogic Server domain should use to connect to the ATP database. Select <b>Custom Service Level</b> to add your custom ATP service level. Default: <b>low</b>.</p>
<b>Custom Autonomous Database Service Level</b>	<p>This field is exposed when you select <b>Custom Service Level</b> as your <b>Autonomous Database Service Level</b>. It allows you to add the custom ATP service level name.</p>
<b>Database Listener Port</b>	<p>If you selected a <b>Database Strategy</b> of <b>Database System</b> or <b>Exadata Database</b>, enter the listener port for the database. Default: 1521.</p>
<b>Specify custom RCU Schema Prefix</b>	<p>Select this check box to specify a custom RCU schema prefix name. If selected, enter an RCU schema prefix in <b>Specify custom RCU Schema Prefix</b> Note that it is your responsibility to make sure that the prefix name is unique in the selected database.</p>

Field Label	Description
<b>Specify RCU Schema custom Password</b>	Select this check box to specify a custom password for the RCU schema. The password must start with a letter, be 12 to 30 characters long, contain at least one number and two or more uppercase characters. Optionally, it can include the following characters: ( ) \$ # _ . If this option is not selected, the provisioning process generates a random password for the RCU schema.
<b>RCU Schema Secret Compartment Validated Secrets OCID for Custom RCU Schema Password</b>	If you selected <b>Specify RCU Schema custom Password</b> and <b>Use KMS Vault Secrets for passwords</b> : <ul style="list-style-type: none"> <li>Select the compartment for the RCU schema secret.</li> <li>Select the OCID of the secret that contains the password for the RCU schema.</li> </ul>
<b>File Storage</b>	This section is shown in the provisioning wizard when: <ul style="list-style-type: none"> <li>the <b>Service Type</b> is <b>MFT Cluster</b> and the <b>Database Strategy</b> is <b>Autonomous Transaction Processing Database</b>. This configuration is mandatory for the MFT Cluster service type on an Autonomous Transaction Processing (ATP) database.</li> <li>the <b>Service Type</b> is <b>SOA with SB &amp; B2B Cluster</b>, the <b>Database Strategy</b> is <b>Autonomous Transaction Processing Database</b>, and you select the optional check box labeled <b>Configure File Storage for shared location in cluster nodes</b>.</li> </ul> <p>The configuration settings here create a new file system, mounted on all the nodes of the cluster. Subsequent scale out operations handle mounting the file system on the newly added node. When configured, FSS will be used as an alternative to DBFS.</p>
<b>File System Compartment</b>	Select the compartment in which to create the file system.
<b>File Storage Availability Domain</b>	Select the name of the availability domain in which to create the file system and the mount target.
<b>Mount Target Strategy</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Use Existing VCN</b> and a <b>Subnet Strategy</b> of <b>Use Existing Subnet</b> , select: <ul style="list-style-type: none"> <li><b>Create New Mount Target</b> to create a new mount target to mount the file system.</li> <li><b>Use Existing Mount Target</b> to use an existing mount target to mount the file system.</li> </ul>
<b>Mount Target Compartment</b>	Select the compartment in which to create the new or existing mount target.
<b>Mount Target Subnet</b>	If you selected a <b>Virtual Cloud Network Strategy</b> of <b>Use Existing VCN</b> , a <b>Subnet Strategy</b> of <b>Use Existing Subnet</b> , and a <b>Mount Target Strategy</b> of <b>Create New Mount Target</b> , select the subnet in which to create the new or existing mount target.
<b>Mount Target Subnet CIDR</b>	If you selected a <b>Subnet Strategy</b> of <b>Create New Subnet</b> , enter the unique CIDR of the new mount target subnet.

Field Label	Description
<b>Existing Mount Target OCID</b>	<p>Enter the OCID of the mount target to be used for mounting the file system.</p> <p>This field is shown when you select:</p> <ul style="list-style-type: none"> <li>• a <b>VCN Strategy</b> of <b>Use Existing VCN</b>, a <b>Subnet Strategy</b> of <b>Using Existing Subnet</b>, a <b>Subnet Type</b> of either <b>Use Private Subnet</b> or <b>Use Public Subnet</b>, and a <b>Mount Target Strategy</b> of <b>Use Existing Mount Target</b></li> <li>• or, <b>VCN Strategy</b> of <b>Create New VCN</b>, a <b>Subnet Strategy</b> of <b>Create New Subnet</b>, and a <b>Subnet Type</b> of <b>Use Public Subnet</b></li> </ul>
<b>Use Network Security Group for Mount Target</b>	<p>Select this check box to use a network security group (NSG) for controlling traffic to the mount target.</p> <p>This check box is shown when you select:</p> <ul style="list-style-type: none"> <li>• a <b>VCN Strategy</b> of <b>Use Existing VCN</b> and a <b>Subnet Strategy</b> of <b>Create New Subnet</b></li> <li>• or, a <b>VCN Strategy</b> of <b>Use Existing VCN</b>, a <b>Subnet Strategy</b> of <b>Use Existing Subnet</b>, and a <b>Mount Target Strategy</b> of <b>Create New Mount Target</b></li> <li>• or, <b>VCN Strategy</b> of <b>Create New VCN</b>, a <b>Subnet Strategy</b> of <b>Create New Subnet</b>, and a <b>Subnet Type</b> of <b>Use Private Subnet</b></li> </ul>
<b>Network Security Group for Compartment</b>	<p>If you selected <b>Use Network Security Group for Mount Target</b>, select the NSG's compartment.</p>
<b>Mount Target Network Security Group</b>	<p>If you selected <b>Use Network Security Group for Mount Target</b>, select the NSG to be used for controlling traffic to the mount target.</p>
<b>Service Instance Advanced</b>	



Field Label	Description
<b>Service Instance Advanced Configuration</b>	<p>Select this check box to specify port configuration properties. Refer to the descriptions below each field:</p> <ul style="list-style-type: none"> <li>• <b>Specify custom WLS Nodemanager Password</b>            If you select this check box and also selected <b>Use KMS Vault Secrets for passwords</b>, the following fields display:           <ul style="list-style-type: none"> <li>– <b>WebLogic Server Nodemanager Secret Compartment</b></li> <li>– <b>Validated Secrets OCID for Nodemanager Password</b></li> </ul> </li> <li>• <b>Node Manager Port</b></li> <li>• <b>Admin Console Port</b></li> <li>• <b>Admin Console SSL Port</b></li> <li>• <b>External Admin Port</b></li> <li>• <b>External Admin SSL Port</b></li> <li>• <b>Managed Server Port</b></li> <li>• <b>Managed Server SSL Port</b></li> <li>• <b>Coherence Cluster Port</b></li> <li>• <b>Custom Cluster Name</b></li> <li>• <b>Custom Domain Name</b></li> <li>• <b>Custom Admin Server Name</b></li> <li>• <b>Custom Managed Server Name Prefix</b></li> <li>• <b>Custom Machine Name Prefix</b></li> <li>• <b>Deploy Sample Application</b></li> <li>• <b>Specify custom ATP wallet Password</b>            If you select this check box and also selected <b>Use KMS Vault Secrets for passwords</b>, the following fields display:           <ul style="list-style-type: none"> <li>– <b>ATP DB Wallet Secret Compartment</b></li> <li>– <b>Validated Secrets OCID for ATP DB Wallet Password</b></li> </ul> </li> </ul> <p><b>Note:</b> If you choose not to provide custom values, the default naming convention will be followed during provisioning.</p>
<p><b>Backup/Restore Configuration (enabled with KMS Configuration)</b>            This section is exposed only when you select <b>Use KMS Vault Secrets for Passwords</b>.</p>	
<p><b>Enable Backup/Restore configuration</b>  <b>Note:</b> You can also edit an Oracle SOA Suite on Marketplace instance post-provisioning to disable and enable this option.</p>	<p>Select this check box to enable Oracle SOA Suite on Marketplace domain home backup and restore. Backup and restore requires KMS to be configured in the following fields:</p> <ul style="list-style-type: none"> <li>• <b>KMS Vault Compartment.</b> Select the compartment where you have the KMS vault.</li> <li>• <b>KMS Vault.</b> Select the OCID of the KMS vault used to encrypt the backup files.</li> <li>• <b>KMS Encryption Key.</b> Select the OCID of the KMS encryption key used to encrypt the backup files.</li> <li>• <b>Object Storage Bucket Name.</b> Enter the name of the object storage bucket used for storing the backup files.</li> </ul>
<p><b>Email Notification</b>            When enabled, Oracle SOA Suite on Marketplace uses the OCI Notification Service (ONS) and OCI Events Service to send out email notifications upon completion of the Terraform job in the stack.</p>	

Field Label	Description
<b>Enable Email notifications</b>	Select this check box to send an email notification upon completion of the Terraform job in the stack, containing information about the job. Example email: 
<b>ONS Topic Strategy</b>	Select: <ul style="list-style-type: none"> <li>• <b>Use Existing ONS Topic</b> to reuse an existing ONS topic with an email subscription.</li> <li>• <b>Create New ONS Topic</b> to create a new ONS topic.</li> </ul>
<b>Existing ONS Topic OCID</b>	If you selected an <b>ONS Topic Strategy</b> of <b>Use Existing ONS Topic</b> , enter the OCID of the existing ONS topic to be used for configuring the email notification.
<b>Notification Email ID</b>	If you selected an <b>ONS Topic Strategy</b> of <b>Create New ONS Topic</b> , enter the email address to which the email notification should be sent. <b>Note:</b> A confirmation email will be sent to the provided email address. The email recipient must click the link provided in the email to confirm the subscription and enable email notifications. 
<b>Tags</b>	For more information, see <a href="#">Resource Tags</a> .
<b>Tag namespace</b>	Select free-form or defined tags for the instance.
<b>Tag key</b>	Optionally, enter a tag key for the instance.
<b>Tag value</b>	Enter the value for the specified tag key.

5. Click **Next**.
6. See [Complete Post-Provisioning Tasks](#).

## Provision an Oracle SOA Suite on Marketplace Quick Start Instance

You can use the Oracle SOA Suite on Marketplace Quick Start option to quickly provision an Oracle SOA Suite on Marketplace instance along with underlying Oracle Cloud Infrastructure network resources. This option is available in both BYOL and PAID offerings.

The Quick Start option allows you to provision an Oracle SOA Suite on Marketplace instance with default values and fewer clicks than going through the full provisioning wizard. A quick

start instance is useful for testing integrations with minimal knowledge required to set up Oracle Cloud Infrastructure network resources.

### Capabilities and Usage Notes

- An Oracle SOA Suite on Marketplace quick start instance is automatically provisioned with an Oracle Autonomous Transaction Processing (ATP) database, along with required network resources.
- Billing is for single node Oracle SOA Suite on Marketplace cost per the UCM hourly license model. This includes billing for an ATP shared database, which is provisioned by the Quick Start.
- A quick start instance is automatically provisioned with the following capabilities:
  - 12.2.1.4 Oracle SOA Suite, Oracle Service Bus, and Oracle B2B topology.
    - \* Compute shape: VM Standard 2.1, 15GB Memory
  - Oracle ATP database - 1 OCPU with 19c
  - Within the compartment, the following resources are created:
    - \* VCN - 10.0.0.0/16 (instance name prefix `QSVCN`)
    - \* Public subnet - 10.0.0.0/28 (instance name prefix `QSSubnet`)
    - \* Required security lists
    - \* Internet gateway (instance name prefix `internet-gateway`)
    - \* Route table
    - \* DHCP
    - \* All resources are tagged with freeform tag `QSTag:InstanceNamePrefix`
  - An Oracle SOA Suite on Marketplace quick start instance supports all Oracle Cloud Infrastructure operations on compute instances, such as start and stop.
  - To delete a quick start instance, you must destroy the stack and optionally delete the stack. Once the stack is destroyed, all resources and compute instances that are created with the stack will be deleted. See [Deprovision an Oracle SOA Suite on Marketplace Instance](#).
- Post-provisioning, you must add security lists to known CIDRs so you can access the WebLogic Server Administration Console URL.
- The following functionality is not supported in an Oracle SOA Suite on Marketplace quick start instance:
  - Multinode clusters.
  - Addition or removal of nodes (scale out and in).
  - Adding or editing a load balancer during provisioning.
  - MFT or BAM topologies.

 **Note:**

If you manually create additional resources such as subnets in the quick start VCN, you must delete them before destroying the stack. Otherwise, the destroy operation will delete only compute instances, without deleting the resources.

- DBFS mounts.

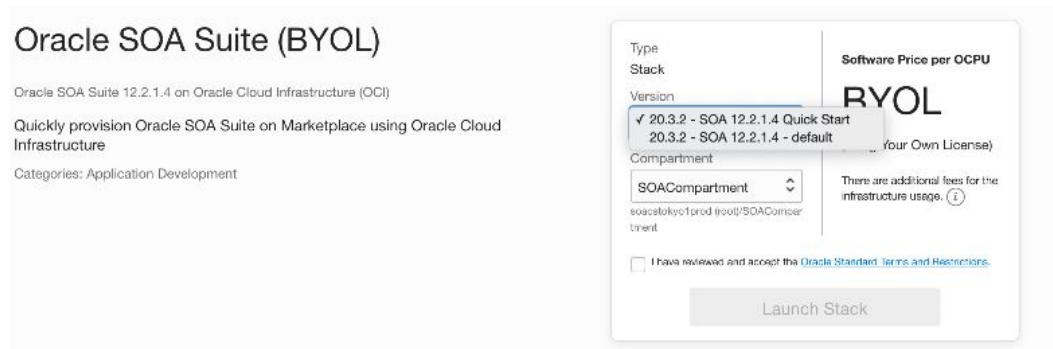
### Prerequisites

Before creating an Oracle SOA Suite on Marketplace quick start instance, you must set up a compartment and add required IAM policies. If your tenancy does not already include the compartment for your quick start instance, you can create a new one. See [Create a Compartment](#).

### Steps

To provision an Oracle SOA Suite on Marketplace quick start instance:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Click **Version** and select the **Quick Start** option.



3. Select the **Compartment** in which you want to create the database and quick start instance.

 **Note:**

If not already granted, you will need to ask your administrator to grant the following `manage` and `use` permissions in the compartment:

- allow group `groupName` to manage instance-family in compartment `compartmentName`
- allow group `groupName` to manage virtual-network-family in compartment `compartmentName`
- allow group `groupName` to manage volume-family in compartment `compartmentName`
- allow group `groupName` to use database-family in compartment `compartmentName`
- allow group `groupName` to use autonomous-database-family in compartment `compartmentName`

where `groupName` is the name of the group to which you belong and `compartmentName` is the name of the compartment where Oracle SOA Suite on Marketplace instances will be created.

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

The Create Stack wizard is displayed.

5. Configure the instance as follows:

Field Label	Description
<b>Server Instance</b>	
INSTANCE NAME PREFIX	Enter the prefix you wish to use for the instance name. This name must be unique in your identity domain. The instance name will be used as a prefix for compute and network resources that will be created for the quick start instance. For example, if the instance name is <code>QSSOA</code> , resources will be created as <code>QSSOA-QSVCN</code> , <code>QSSOA-QSSubnet</code> , and so on.
SSH PUBLIC KEY	Enter the public key for the secure shell (SSH). This key is used for authentication when connecting to the instance using an SSH client. See <a href="#">Generate a Secure Shell (SSH) Public/Private Key Pair</a> .
ADMINISTRATION PASSWORD	Enter a password that meets the specifications shown below the field. This password is used for signing in to SOA Consoles as the <code>weblogic</code> user. It is the administration password to connect to the ATP database.

For example:

### Create Stack

- 1 Stack Information
- 2 Configure Variables**
- 3 Review

Configure the variables for the infrastructure resources that this stack will create when you run the apply job for this execution plan.

#### Service Instance

**INSTANCE NAME PREFIX**

The names of all compute and network resources will begin with this prefix. It can only contain letters or numbers and must begin with a letter.

**SSH PUBLIC KEY**


Use the corresponding private key to access the service instances

**ADMINISTRATION PASSWORD**

The password for the Weblogic user and Database Admin user. Use an Administrator password that starts with a letter, is between 12 and 30 characters and contain at least one uppercase letter, one lowercase letter, and one number. The password cannot contain the double quote character or the username admin.

- After the quick start instance is created, confirm the resources, which should be similar to the following:

Networking > Virtual Cloud Networks > Virtual Cloud Network Details > Subnets



### OMCSVG-QSVCN

Move Resource Add Tags Terminate

VCN Information Tags

CIDR Block: 10.0.0.0/16 OCID: ...y5tq4a [Show](#) [Copy](#)

Compartment: SOACompartment [Default Route Table: Default Route Table for OMCSVG-QSVCN](#)

Created: Mon, Aug 17, 2020, 23:46:41 UTC DNS Domain Name: omcsvgvcn.oraclevcn.com

Resources

- Subnets (1)
- Route Tables (1)
- Internet Gateways (1)
- Dynamic Routing Gateways (0)
- Network Security Groups (0)
- Security Lists (4)
- DHCP Options (2)
- Local Peering Gateways (0)

#### Subnets in SOACompartment Compartment

[Create Subnet](#)

Name	State	CIDR Block	Subnet Access	Created
<a href="#">OMCSVG-QSSubnet</a>	● Available	10.0.0.0/28	Public (Regional)	Mon, Aug 17,

Networking > Virtual Cloud Networks > OMCSVG-QSVN > Subnet Details

### OMCSVG-QSSubnet

[Edit](#) [Move Resource](#) [Add Tag](#) [Terminate](#)

Subnet Information | Tags

**OCID:** [ip2hjq](#) [Show](#) [Copy](#)  
**CIDR Block:** 10.0.0.0/28  
**Virtual Router Mac Address:** 00:00:17:3E:24:77  
**Subnet Type:** Regional

**Compartment:** SOACompart  
**DNS Domain Name:** [subpubomcsvg...](#) [Show](#) [Copy](#)  
**Subnet Access:** Public Subnet  
**DHCP Options:** [OMCSVG-dhcpOptions](#)  
**Route Table:** [Default Route Table for OMCSVG-QSVN](#)

Resources

Security Lists (3)

[Add Security List](#)

Name	State	Compartment	Cre
<a href="#">OMCSVG-wls-ms-security-list</a>	Available	SOACompart	Mon
<a href="#">OMCSVG-wls-security-list</a>	Available	SOACompart	Mon
<a href="#">OMCSVG-internal-security-list</a>	Available	SOACompart	Mon

## Provision an Oracle SOA Suite on Marketplace Instance Using the Oracle Cloud Infrastructure Command Line Interface

The Oracle Cloud Infrastructure Command Line Interface (CLI) is a small-footprint tool that you can use on its own or with the Oracle Cloud Infrastructure Console to complete tasks. The CLI provides the same core functionality as the Oracle Cloud Infrastructure Console, plus additional commands. Some of these, such as the ability to run scripts, extend Console functionality. For more information about the CLI, see [Command Line Interface \(CLI\)](#) in the Oracle Cloud Infrastructure documentation.

You can provision an Oracle SOA Suite on Marketplace instance using Oracle Cloud Infrastructure CLI commands to perform operations such as creating a stack, creating a plan job, and creating an apply job.

### Topics:

- [Install the Command Line Interface](#)
- [Configure the Command Line Interface](#)
- [Start the Command Line Interface](#)
- [Use CLI Commands to Provision an Oracle SOA Suite on Marketplace Instance](#)

## Install the Command Line Interface

To install the CLI, see [Installing the CLI](#) in the Oracle Cloud Infrastructure documentation.

### Notes:

- Select default values during installation.
- Do not install any optional packages.

## Example CLI Installation Output

```
PS C:\WINDOWS\system32> powershell -NoProfile -ExecutionPolicy Bypass -
Command "iex ((New-Object System.Net.WebClient).DownloadString('https://
raw.githubusercontent.com/oracle/oci-cli/master/scripts/install/
install.ps1'))"

*****
        You have started the OCI CLI Installer in interactive mode. If you do
not wish
        to run this in interactive mode, please include the -
AcceptAllDefaults option.
        If you have the script locally and would like to know more about
input options for this script, then you can run:
        help .\install.ps1
        If you would like to know more about input options for this script,
refer to:
        https://github.com/oracle/oci-cli/blob/master/scripts/install/
README.rst

*****
VERBOSE: Python found in registry: HKCU:\Software\Python\PythonCore
VERBOSE: Python found in registry: HKLM:\Software\Python\PythonCore
VERBOSE: C:\Python34\python.exe Python version 3.4.2 is below minimum
required version 3.5.0
VERBOSE: Downloading install script to
C:\Users\vgorugan.ORADEV\AppData\Local\Temp\tmp4226.tmp
VERBOSE: False False
VERBOSE: Using Python executable:
C:\Users\vgorugan.ORADEV\AppData\Local\Programs\Python\Python38\python.exe to
run
install script...
VERBOSE: Arguments to python script:
"C:\Users\vgorugan.ORADEV\AppData\Local\Temp\tmp4226.tmp"
-- Verifying Python version.
-- Python version 3.8.1 okay.

==> In what directory would you like to place the install? (leave blank to
use 'C:\Users\vgorugan.ORADEV\lib\oracle-cli'): d:\ociclinew
-- Creating directory 'D:\ociclinew'.
-- We will install at 'D:\ociclinew'.

==> In what directory would you like to place the 'oci.exe' executable?
(leave blank to use 'C:\Users\vgorugan.ORADEV\bin'): d:\ociclinew
-- The executable will be in 'D:\ociclinew'.

==> In what directory would you like to place the OCI scripts? (leave blank
to use 'C:\Users\vgorugan.ORADEV\bin\oci-cli-scripts'): d:\ociclinew
-- The scripts will be in 'D:\ociclinew'.

==> Currently supported optional packages are: ['db (will install
cx_Oracle)']
What optional CLI packages would you like to be installed (comma separated
names; press enter if you don't need any optional packages)?:
```







```

command.

==> Modify PATH to include the CLI and enable tab completion in PowerShell
now? (Y/n):
--
-- ** Close and re-open PowerShell to reload changes to your PATH **
-- In order to run the autocomplete script, you may also need to set your
PowerShell execution policy to allow for running local scripts (as an
Administrator run Set-ExecutionPolicy RemoteSigned in a PowerShell prompt)
--
-- Installation successful.
-- Run the CLI with D:\ociclinew\oci.exe --help
VERBOSE: Successfully installed OCI CLI!

```

## Configure the Command Line Interface

To configure the CLI, see [Configuring the CLI](#) in the Oracle Cloud Infrastructure documentation.

For Oracle SOA Suite on Marketplace, create a profile file with the following values:

- `user`: Oracle Cloud ID (OCID) of the username you want to use to sign in.
- `fingerprint`: API key of that user (shown on the User Details page in the Oracle Cloud Infrastructure Console)
- `key_file`: Private key you want to use with new Oracle SOA Suite on Marketplace instances.

### Example Profile File in D:\ociclinew\config1

```

[DEFAULT]
user=ocid1.user.oc1..aaaaaaaav4dfgdfgdfgdfgdfgdfgdfgdfgdfgdfgdcyqak625cfltnfsy7zsnyn
y5qwmdmwqxjqzq
fingerprint=2e:e0:9r:35:2c:14:49:3a:d2:cd:e0:ba:ea:d8:f1:f1
key_file=d:\ociclinew\oci_api_key.pem
tenancy=ocid1.tenancy.oc1..aaaaaaaaxd6jemgcmdpb3wewcwchzswgi6g55gth7ioc2gbbpvq
o5ecoa
region=us-ashburn-1

```

## Start the Command Line Interface

To start a CLI session, see [Starting a CLI Session](#) in the Oracle Cloud Infrastructure documentation.

## Use CLI Commands to Provision an Oracle SOA Suite on Marketplace Instance

Use the CLI commands in the order provided here to provision an Oracle SOA Suite on Marketplace instance.



### Note:

Refer to [Oracle Cloud Infrastructure CLI Command Reference](#) for other CLI commands you can use to manage an Oracle SOA Suite on Marketplace instance.

**Topics:**

- [Set File Permissions](#)
- [Get the Compartment OCID](#)
- [Create a Stack](#)
- [Create a Plan Job](#)
- [Create an Apply Job](#)
- [Stop or Start a Compute Instance](#)

## Set File Permissions

Set permissions of a named profile file.

**Syntax**

See [setup repair-file-permissions](#) in the Oracle Cloud Infrastructure documentation.

**Example**

```
oci setup repair-file-permissions --file D:\opc_rsa
```

**Result**

Changes the profile file permissions as required by Oracle Cloud Infrastructure.

## Get the Compartment OCID

Get the OCID of the compartment in which you want to create the Oracle SOA Suite on Marketplace instance.

**Syntax**

See [iam compartment list](#) in the Oracle Cloud Infrastructure documentation.

**Example**

```
oci iam compartment list --config-file D:\ociclinew\config1
```

**Result**

Generates a list of compartment OCIDs in the tenancy. For example:

```
ocid1.compartment.oc1..aaaaaaaalmnpc2nvr7s7jfxkuxp6finc5dif7fqnrkpbczwnojp2jy6  
saq5a
```

## Create a Stack

Create a stack for the Oracle SOA Suite on Marketplace in a named compartment.

**Syntax**

See [resource-manager stack create](#) in the Oracle Cloud Infrastructure documentation.

**Example**

```
oci resource-manager stack create --compartment-id
"ocid1.compartment.oc1..aaaaaaaalmnpc2nvr7s7jfxkuxp6finc5dif7fqnrkpbczwnojp2jy
6saq5a"
--config-source
"D:\ociclinew\ocid1.ormjob.oc1.iad.aaaaaaaaramgqimwcjjvf7wpu3bg6fugwpvxvejymcmb
oixukkurcorach3dq.zip"
--display-name SOACmdline4 --terraform-version 0.12.x --config-file
D:\ociclinew\config1 --variables file://D:\ociclinew\stackinp.json
```

**where**

- `compartment-id` is the OCID of the compartment in which you want to create the stack, as shown in the output of `iam compartment list`
- `config-source` is the terraform configuration zip file
- `display-name` is the name the stack that will be created
- `variables` provides variables associated with the stack in a `.json` file, as shown below

**Example stackinp.json**

```
{
"compartment_ocid":"ocid1.compartment.oc1..aaaaaaaalmnpc2nvr7s7jfxkuxp6finc5di
f7fqnrkpbczwnojp2jy6saq5a",
"region":"us-ashburn-1",
"tenancy_ocid":"ocid1.tenancy.oc1..aaaaaaaaxd6jemgcmdpb3pnctl17yf2hzswgi6g55gth
7ioc2gbpbvqo5ecoa",
"topology":"MFT Cluster",
"wls_node_count":"2",
"use_kms_decryption":"false",
"add_load_balancer":"true",
"lb_shape":"100Mbps",
"lb_subnet_type":"Use Public Subnet",
"lb_subnet_1_id":"ocid1.subnet.oc1.iad.aaaaaaaashmjwyhall67kqwjqttggdipseaoidu
hx43mxejsms7gzqmt2bha",
"use_advanced_wls_instance_config":"false",
"network_compartment_id":"ocid1.compartment.oc1..aaaaaaaalmnpc2nvr7s7jfxkuxp6f
inc5dif7fqnrkpbczwnojp2jy6saq5a",
"ocidb_compartment_id":"ocid1.compartment.oc1..aaaaaaaaxw2j2w5xdlvia3vwz7gdxh2
5qk6d5pkdjpspawl4x4m3mfahudsa",
"subnet_compartment_id":"ocid1.compartment.oc1..aaaaaaaashmjwyhall67kqwjqttggd
ipseaoiduhx43mxejsms7gzqmt2bha",
"lb_subnet_compartment_id":"ocid1.compartment.oc1..aaaaaaaashmjwyhall67kqwjqtt
ggdipseaoiduhx43mxejsms7gzqmt2bha",
"existing_vcn_id":"ocid1.vcn.oc1.iad.aaaaaaaajnyi3pvohrm2qwgllghkfwmmqf7g33oh6a
f12eb3qaaywdufln6q",
"db_strategy_existing_vcn":"Database System",
"ocidb_dbssystem_id":"ocid1.dbssystem.oc1.iad.abuwcljt5zstolrw473is2urvdkuihmi6x
73fgjlu5vovflgahxcyb5j4biq",
"ocidb_dbhome_id":"ocid1.dbhome.oc1.iad.abuwcljtba7wilxmdnwq7qk3gg377epqf6vjf
gvhvqmhc4ya4if4tswdoqq",
"ocidb_database_id":"ocid1.database.oc1.iad.abuwcljt2ww2xxrtg6um62pqvca3fb7osk
ry6fj5xksoa4ukavmiwo3z5p7a",
"ocidb_pdb_service_name":"PDB1",
```

```

"oci_db_user":"SYS",
"oci_db_password":"W#1C0m#1#",
"service_name":"SOACLI1",
"instance_shape":{"instanceShape\']="VM.Standard.E4.Flex\","ocpus\"]=2,\memory\"]=45}",
"ssh_public_key":"","
"wls_availability_domain_name":"bcaH:US-ASHBURN-AD-2",
"wls_admin_user":"weblogic",
"wls_admin_password":"welcome1",
"existing_vcn_id":"ocidl.vcn.oc1.iad.aaaaaaaashmjwyhall67kqwjqttggdipseaoiduhx43mxejsms7gzqmt2bha",
"wls_subnet_id":"ocidl.subnet.oc1.iad.aaaaaaaashmjwyhall67kqwjqttggdipseaoiduhx43mxejsms7gzqmt2bha",
"vcn_strategy":"Use Existing VCN",
"subnet_strategy_existing_vcn":"Use Existing Subnet",
"subnet_type":"Use Public Subnet"
}

```

### Output

The output provides the OCID for the value of `stack-id` in [Create a Plan Job](#) and [Create an Apply Job](#).

## Create a Plan Job

Create a plan job in a named stack.

### Syntax

See [resource-manager job create-plan-job](#) in the Oracle Cloud Infrastructure documentation.

### Example

```

oci resource-manager job create-plan-job
--stack-id
"ocidl.ormstack.oc1.iad.aaaaaaaagvq5fw6nf76uozbdlxsonwwl4qgiwnacvgsrctvhlqiej2
oihvoq"
--config-file D:\ociclinew\config1

```

### where

- `stack-id` is the job OCID shown in the output of `resource-manager stack create`

### Output

The output provides the OCID for the value of `execution-plan-job-id` in [Create an Apply Job](#).

## Create an Apply Job

After the plan job completes successfully, create an apply job in a named stack and execution plan.

### Syntax

See [resource-manager job create-apply-job](#) in the Oracle Cloud Infrastructure documentation.

## Example

```
oci resource-manager job create-apply-job
--stack-id
"ocid1.ormstack.oc1.iad.aaaaaaaagvq5fw6nf76uozbdlxsonwwl4qgiwnacvgsrctvhlqiej2
oihvoq"
--execution-plan-strategy FROM_PLAN_JOB_ID
--execution-plan-job-id
"ocid1.ormjob.oc1.iad.aaaaaaaadvjowgs7zfv23224z4x3cpfdm3w74pdp5qmc26uiwf7rkwn
57la"
--config-file D:\ociclinew\config1
```

### where

- `stack-id` is the job OCID shown in the output of `resource-manager stack create`
- `execution-plan-job-id` is shown in the output of `resource-manager job create-plan-job`

When the apply job completes, check the job logs to verify that the Oracle SOA Suite on Marketplace instance was successfully created.

## Stop or Start a Compute Instance

Stop, start, or restart a compute instance.

### Syntax

See [compute instance action](#) in the Oracle Cloud Infrastructure documentation.



### Note:

This command stops or starts both WebLogic Servers and compute instances.

### Example to stop an instance

```
oci compute instance action
--config-file D:\ociclinew\config1
--action SOFTSTOP
--instance-id
ocid1.instance.oc1.phx.anyhqljtty92jdsmduytjowrsaa25oetrdqrbaw3wsv5klrj6r7rds
q6afq
```

### where

- `instance-id` is the OCID of the compute instance you want to stop.

Oracle recommends using `SOFTSTOP` or `SOFTRESET` instead of `STOP` or `RESET` actions.

# Provision an Oracle SOA Suite on Marketplace Instance Using Oracle Cloud Infrastructure REST APIs

You can provision an Oracle SOA Suite on Marketplace instance using Oracle Cloud Infrastructure REST APIs to perform operations such as creating a database, creating a stack, creating a plan job, and creating an apply job.

Use the REST APIs in the order provided here to provision an Oracle SOA Suite on Marketplace instance.

## Topics:

- [Create a Database](#)
- [Create a Stack](#)
- [Create a Plan Job](#)
- [Create an Apply Job](#)

## Create a Database

Use the `LaunchDbSystem` REST API to create a new database system in the specified compartment and availability domain. The Oracle Database edition that you specify applies to all the databases on that database system. The selected edition cannot be changed. An initial database is created on the database system based on the request parameters you provide and some default options.

### Syntax

See [LaunchDbSystem](#) in the Oracle Cloud Infrastructure documentation.

### Example Request Payload for Oracle SOA Suite on Marketplace

```
{
  "availabilityDomain": "#{availabilityDomain}",
  "compartmentId": "#{compartmentId}",
  "cpuCoreCount": 2,
  "displayName": "#{dbServiceName}",
  "hostname": "#{dbServiceName}host",
  "initialDataStorageSizeInGB": 512,
  "nodeCount": 1,
  "shape": "#{dbShape}",
  "source": "NONE",
  "sshPublicKeys": [
    "#{sshPublicKey}"
  ],
  "subnetId": "#{subnet}",
  "databaseEdition": "STANDARD_EDITION",
  "dbHome": {
    "database": {
      "adminPassword": "#{dbPassword}",
      "dbName": "#{dbName}",
      "pdbName": "#{pdbName}"
    },
    "dbVersion": "#{dbVersion}"
  }
}
```



```
}
}
```

### Example Response Payload for Oracle SOA Suite on Marketplace

```
{
  "availabilityDomain" : "OXET:PHX-AD-1",
  "compartmentId" : "ocidl.tenancy.oc1..<unique_ID>",
  "cpuCoreCount" : 8,
  "databaseEdition" : "ENTERPRISE_EDITION",
  "diskRedundancy" : "HIGH",
  "displayName" : "tst3dbsys",
  "domain" : "my.company.com",
  "hostname" : "athena",
  "id" : "ocidl.dbsystem.oc1.phx.<unique_ID>",
  "kmsKeyId" : "ocidl.key.oc1.phx.<unique_ID>",
  "lastPatchHistoryEntryId" : null,
  "licenseModel" : "LICENSE_INCLUDED",
  "lifecycleDetails" : null,
  "lifecycleState" : "PROVISIONING",
  "listenerPort" : 1521,
  "scanIpIds": null,
  "shape" : "BM.DenseIO1.36",
  "sshPublicKeys" : [ "ssh-rsa <public_SSH_key> name@example.com" ],
  "subnetId" : "ocidl.subnet.oc1.phx.<unique_ID>",
  "timeCreated" : "2016-11-23T01:59:07.030Z",
  "version" : "201609160308",
  "vipIds": null
}
```

## Create a Stack

Use the `CreateStack` REST API to create a stack in the specified compartment. You can create a stack from a Terraform configuration. The Terraform configuration can be directly uploaded or referenced from a source code control system. You can also create a stack from an existing compartment.

### Syntax

See [CreateStack](#) in the Oracle Cloud Infrastructure documentation.

### Example Request Payload for Oracle SOA Suite on Marketplace

```
{
  "compartmentId": "#{compartmentId}",
  "displayName": "#{serviceName}_AUTO_STACK",
  "description": "#{serviceName}_AUTO_STACK",
  "configSource": {
    "configSourceType": "ZIP_UPLOAD",
    "zipFileBase64Encoded": "#{zipFileBase64Encoded}",
    "workingDirectory": null
  },
  "variables": {
    "ocidb_database_id": "#{ocidbDatabaseId}",
    "use_kms_decryption": "false",
  }
}
```

```

"wls_node_count": "#{managedServerCount}",
"ocidb_dbhome_id": "#{ocidbDbHomeId}",
"ocidb_compartment_id": "#{compartmentId}",
"ocidb_pdb_service_name": "#{pdbName}",
"oci_db_user": "#{dbUserName}",
"oci_db_password": "#{dbPassword}",
"wls_subnet_id": "#{subnet}",
"use_schema_partitioning": "false",
"region": "#{region}",
"use_advanced_wls_instance_config": "false",
"ocidb_dbsystem_id": "#{ocidbDbSystemId}",
"tenancy_ocid": "#{tenancyOcid}",
"topology": "#{topology}",
"existing_vcn_id": "#{existingVcnId}",
"network_compartment_id": "#{compartmentId}",
"compartment_ocid": "#{compartmentId}",
"add_load_balancer": "#{addLoadBalancer}",
"ssh_public_key": "#{sshPublicKey}",
"service_name": "#{serviceName}",
"instance_image_id": "#{instanceImageId}",
"wls_availability_domain_name": "#{availabilityDomain}",
"instance_shape": "#{instanceShape}",
"wls_admin_user": "#{wlsUserName}",
"wls_admin_password": "#{wlsPassword}",
"subnet_strategy_existing_vcn": "#{subnetStrategyExistingVcn}",
"db_strategy_existing_vcn": "#{dbStrategyExistingVcn}",
"use_custom_schema_prefix": "#{useCustomSchemaPrefix}",
"rcu_schema_prefix": "#{rcuSchemaPrefix}",
"use_custom_schema_password": "#{useCustomSchemaPassword}",
"rcu_schema_password": "#{rcuSchemaPassword}"
},
"terraformVersion": "0.12.x"
}

```

### Example Response Payload for Oracle SOA Suite on Marketplace

```

{
  "id": "ocid.stack.oc1.<unique_ID>",
  "compartmentId": "ocid.compartment.oc1.<unique_ID>",
  "displayName": "Stack Display Name",
  "description": "Brief description of the stack.",
  "timeCreated": "2018-10-02T19:18:44.437Z",
  "lifecycleState": "CREATING"
  "configSource": {
    "configSourceType": "ZIP_UPLOAD"
    "workingDirectory": "<file_path_to_directory>"
  },
  "variables": {
    "additionalProp1": "myVariable01"
    "additionalProp2": "myVariable02"
  },
  "terraformVersion": "0.12.x",
  "stackDriftStatus": "DRIFTED",
  "timeDriftLastChecked": "2019-10-02T19:18:44.437Z",
  "freeformTags": {

```

```

    "additionalProp1": {"Department": "Finance"}",
  },
  "definedTags": {
    "additionalProp1": {
      "additionalProp1": {"CostCenter": "42"},
    }
  }
}

```

### Output

The response payload provides the OCID for the value of `stackId` in [Create a Plan Job](#) and [Create an Apply Job](#).

## Create a Plan Job

Once the stack is created successfully, use the `CreateJob` REST API to create a plan job, using the stack ID.

### Syntax

See [CreateJob](#) in the Oracle Cloud Infrastructure documentation.

### Example Request Payload for Oracle SOA Suite on Marketplace

```

{
  "displayName": "sob12214noncrop-plan",
  "stackId": "#{mp_createStack-id}",
  "jobOperationDetails": {
    "operation": "PLAN"
  }
}

```

where

- `stackId` is shown in the output of `CreateStack`

### Example Response Payload for Oracle SOA Suite on Marketplace

```

{
  "id": "ocid.job.oc1.<unique_ID>",
  "stackId": "ocid.stack.oc1.<unique_ID>",
  "compartmentId": "ocid.compartment.oc1.<unique_ID>",
  "displayName": "Stack Display Name",
  "operation": "Apply",
  "jobOperationDetails": {
    "operation": "APPLY",
    "executionPlanStrategy": "FROM_PLAN_JOB_ID",
    "executionPlanJobId": "ocid.job.oc1.<unique_ID>"
  },
  "applyJobPlanResolution": {
    "planJobId": "ocid.job.oc1.<unique_ID>"
  },
  "resolvedPlanJobId": "ocid.job.oc1.<unique_ID>",
  "timeCreated": "2018-10-02T19:18:44.437Z",
}

```

```

"timeFinished": "2018-10-02T19:18:44.439Z",
"lifecycleState": "IN_PROGRESS"
"workingDirectory": "<file_path_to_directory>",
"variables": {
  "additionalProp1": "myVariable01"
  "additionalProp2": "myVariable02"
},
"configSource": {
  "configSourceType": "GIT_CONFIG_SOURCE",
  "workingDirectory": "<file_path_to_directory>",
  "configurationSourceProviderId":
"ocid.OrmConfigSourceProvider.oc1..<unique_ID>",
  "branchName": "MyBranch",
  "repositoryUrl": "https://github.com/user/repo.git",
  "commitId": "3244456656565678787"
},
"freeformTags": {
  "additionalProp1": {"Department": "Finance"}
},
"definedTags": {
  "additionalProp1": {
    "additionalProp1": {"CostCenter": "42"}
  }
}
}

```

### Output

The response payload provides the OCID for the value of `executionPlanJobId` in [Create an Apply Job](#).

## Create an Apply Job

Once the plan job completes successfully, use the `CreateJob` REST API to create an apply job for the same stack.

### Syntax

See [CreateJob](#) in the Oracle Cloud Infrastructure documentation.

### Example Request Payload for Oracle SOA Suite on Marketplace

```

{
  "stackId": "#{mp_createStack-id}",
  "displayName": "sob12214noncrop-apply",
  "jobOperationDetails": {
    "operation": "APPLY",
    "executionPlanStrategy": "FROM_PLAN_JOB_ID",
    "executionPlanJobId": "#{mp_planJob-id}"
  }
}

```

where

- `stackId` is the job OCI shown shown in the output of `CreateStack`

**Example Response Payload for Oracle SOA Suite on Marketplace**

```

{
  "id": "ocid.job.oc1..<unique_ID>",
  "stackId": "ocid.stack.oc1..<unique_ID>",
  "compartmentId": "ocid.compartment.oc1..<unique_ID>",
  "displayName": "Stack Display Name",
  "operation": "Apply",
  "jobOperationDetails": {
    "operation": "APPLY",
    "executionPlanStrategy": "FROM_PLAN_JOB_ID",
    "executionPlanJobId": "ocid.job.oc1..<unique_ID>"
  },
  "applyJobPlanResolution": {
    "planJobId": "ocid.job.oc1..<unique_ID>"
  },
  "resolvedPlanJobId": "ocid.job.oc1..<unique_ID>",
  "timeCreated": "2018-10-02T19:18:44.437Z",
  "timeFinished": "2018-10-02T19:18:44.439Z",
  "lifecycleState": "IN_PROGRESS",
  "workingDirectory": "<file_path_to_directory>",
  "variables": {
    "additionalProp1": "myVariable01"
    "additionalProp2": "myVariable02"
  },
  "configSource": {
    "configSourceType": "GIT_CONFIG_SOURCE",
    "workingDirectory": "<file_path_to_directory>",
    "configurationSourceProviderId":
"ocid.ormconfigsourceprovider.oc1..<unique_ID>",
    "branchName": "MyBranch",
    "repositoryUrl": "https://github.com/user/repo.git",
    "commitId": "3244456656565678787"
  },
  "freeformTags": {
    "additionalProp1": "{\"Department\": \"Finance\"}",
  },
  "definedTags": {
    "additionalProp1": {
      "additionalProp1": {"CostCenter": "42"},
    }
  }
}

```

## Complete Post-Provisioning Tasks

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

**Topics:**

- (May be required for instances provisioned after 1 August 2020) [Add Ingress Rules to Access WebLogic Server Administration and Other Consoles](#)
- [Add an Ingress Rule to Allow ssh Access to SOA Servers](#)

- [Restart Servers for a Multinode Cluster](#)
- (Required if using a cloud adapter) [Add a Managed Server IP in a Non-Proxy Host to Enable Deployment from Fusion Middleware Control](#)
- (Required for MFT) [Complete Post-Provisioning Tasks for an MFT Cluster Service Type](#)
- (Optional but highly recommended) [Configure Scheduled Backups](#)
- (Optional) [Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure](#)
- (Optional) [Register a Custom Domain Name with a Third-Party Registration Vendor](#)

## Add Ingress Rules to Access WebLogic Server Administration and Other Consoles

If you provision an instance after 1 August 2020 and you are not able to access the WebLogic Server Administration Console or other console URLs from your browser after provisioning, then you must create rules to allow traffic into your Administration Server VM.

### Note:

Before performing these steps, be aware that this means that Weblogic Server allows inbound traffic to the known public IPs or CIDRs that you configure. Oracle recommends that you do not allow inbound traffic to be visible to unknown public IPs.

To add ingress rules to allow access to the WebLogic Server Administration Console or other console URLs:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Select the compartment where you created the new instance.
4. In the list of VCNs, select your VCN.
5. On the Virtual Cloud Network Details page, click **Security Lists** in the left pane.
6. Click the security list that the Administration Server VM is using.
7. Click **Add Ingress Rules** to open the Add Ingress Rules dialog.

Add Ingress Rules Cancel

---

**Ingress Rule 1**

Allows TCP traffic for ports: all

STATELESS ⓘ

SOURCE TYPE: CIDR SOURCE CIDR: Example: 10.0.0.0/16 IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All DESTINATION PORT RANGE OPTIONAL ⓘ: All  
Examples: 80, 20-22

DESCRIPTION OPTIONAL:   
Maximum 255 characters

+ Additional Ingress Rule

**Add Ingress Rules** Cancel

8. In the Add Ingress Rules dialog, create an ingress rule to access the WebLogic Server Administration Console:
  - a. Leave the STATELESS checkbox deselected.
  - b. For SOURCE TYPE, select **CIDR**.
  - c. In the SOURCE CIDR field, enter the public IP address of the machine where the Administration Server URL is opened from a browser (for example, if the public IP address is 123.123.456.456 then enter 123.123.456.456/32). Alternatively, you can enter a CIDR.
  - d. In the IP PROTOCOL field, select TCP.
  - e. In the DESTINATION PORT RANGE field, enter 7002.
  - f. Click **Add Ingress Rules**.

SOABYOL-wls-ms-security-list

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Move Resource Add Tags Terminate

Security List Information Tags

OCID: ...sk6pla Show Copy Compartment: SOACompartment  
 Created: Wed, May 20, 2020, 03:27:24 UTC

Resources

Ingress Rules (2)  
 Egress Rules (0)

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	7004		TCP traffic for ports: 7004	
<input type="checkbox"/>	No	162.142.142.152/32	TCP	All	7002		TCP traffic for ports: 7002	

0 Selected

- Repeat the steps above to add ingress rules to access other consoles, specifying the associated `DESTINATION PORT RANGE` value.

## Add an Ingress Rule to Allow ssh Access to SOA Servers

After provisioning, if you need to connect (`ssh`) to a SOA server, you must add an ingress rule to allow traffic from the host where `ssh` is initiated. For example, if your `ssh` client host public IP is 129.29.30.51, then add an ingress rule to allow traffic from 129.29.30.51/32.

To add an ingress rule to allow traffic from the `ssh` client host:

- Sign in to the Oracle Cloud Infrastructure Console.
- Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
- Select the compartment where you created the new instance.
- In the list of VCNs, select your VCN.
- On the Virtual Cloud Network Details page, click **Security Lists** in the left pane.
- Click the security list that the `ssh` client host is using.
- Click **Add Ingress Rules** to open the Add Ingress Rules dialog.

The screenshot shows the 'Add Ingress Rules' dialog box. At the top right is a 'Cancel' link. The main area is titled 'Ingress Rule 1' and contains the following fields:

- STATELESS**: A checkbox that is currently unchecked.
- SOURCE TYPE**: A dropdown menu set to 'CIDR'.
- SOURCE CIDR**: A text input field containing '129.29.30.51/32'. Below it, a note says 'Specified IP addresses: 129.29.30.51-129.29.30.51 (1 IP addresses)'.
- IP PROTOCOL**: A dropdown menu set to 'TCP'.
- SOURCE PORT RANGE**: A text input field containing 'All'. Below it, a note says 'Examples: 80, 20-22'.
- DESTINATION PORT RANGE**: A text input field containing '22'. Below it, a note says 'Examples: 80, 20-22'.
- DESCRIPTION**: A text input field containing 'Allow SSH Access'. Below it, a note says 'Maximum 255 characters'.

At the bottom right is a '+ Another Ingress Rule' button. At the bottom left are 'Add Ingress Rules' and 'Cancel' buttons.

- In the Add Ingress Rules dialog, create an ingress rule to access the `ssh` client host:
  - Leave the `STATELESS` checkbox deselected.
  - For `SOURCE TYPE`, select **CIDR**.



- c. In the `SOURCE CIDR` field, enter the public IP address of the machine where the `ssh` client host is opened from a browser (for example, if your public IP address is `129.29.30.51` then enter `129.29.30.51/32`). Alternatively, you can enter a CIDR.
- d. In the `IP PROTOCOL` field, select `TCP`.
- e. In the `SOURCE PORT RANGE` field, enter `All`.
- f. In the `DESTINATION PORT RANGE` field, enter `22`.
- g. Click **Add Ingress Rules**.

## Restart Servers for a Multinode Cluster

If you configure a multinode Oracle SOA Suite on Marketplace cluster, you must restart all servers immediately after provisioning.

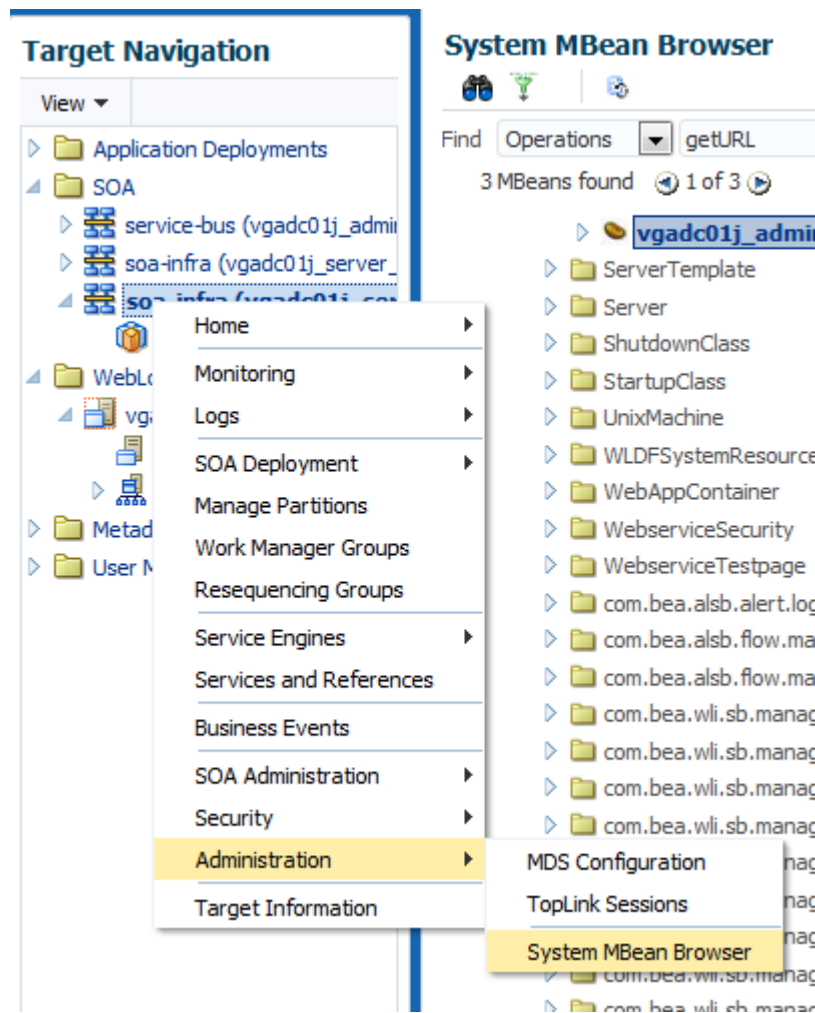
Restarting the Administration Server and Managed Servers propagates the Coherence cluster configuration across all the nodes in a multinode cluster. See [Stop or Start WebLogic Servers](#).

## Add a Managed Server IP in a Non-Proxy Host to Enable Deployment from Fusion Middleware Control

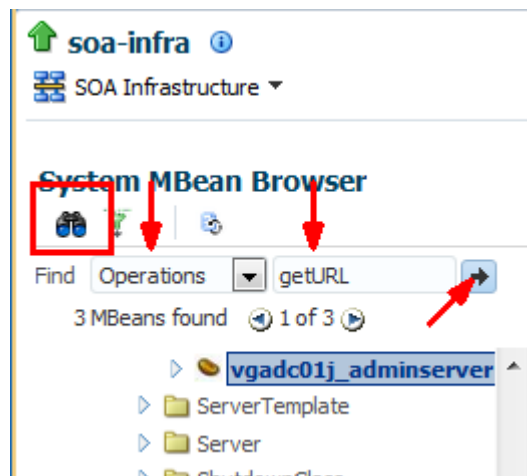
Before you can use Fusion Middleware Control to deploy applications, you must add a Managed Server IP in to a non-proxy host.

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**, then **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.



- Click **getURL**.

The screenshot shows the 'System MBean Browser' interface. On the left, a tree view shows the hierarchy of MBeans, with 'vgadc01j\_adminserver' selected. On the right, the 'Runtime MBeans: ServerRuntime:vgadc01j\_adminserver' window is open, displaying a list of operations. The 'getURL' operation is highlighted with a red box. The table below shows the details of the operations:

Name	Description
1 addRequestClassRuntime	
2 forceShutdown	Force shutdown the server. Causes the server to reject new requests and fail pending requests.
3 forceSuspend	Transitions the server from RUNNING to ADMIN state forcefully cancelling in-flight work.
4 getIPv4URL	The URL that clients use when connecting to this server using the specified protocol.
5 getIPv6URL	The URL that clients use when connecting to this server using the specified protocol.
6 getServerChannel	The address on which this server is listening for connections that use the specified protocol.
7 <b>getURL</b>	The URL that clients use when connecting to this server using the specified protocol.
8 isServiceAvailable	returns true iff the named service is available (configured, licensed & running)
9 lookupApplicationRuntime	Returns the ApplicationRuntimeMBean asked for, by name.
10 lookupLibraryRuntime	Returns the LibraryRuntimeMBean asked for, by name.
11 lookupMaxThreadsConstraintRuntime	
12 lookupMessagingBridgeRuntime	
13 lookupMinThreadsConstraintRuntime	
14 lookupPersistentStoreRuntime	Returns the Runtime mbean for the persistent store with the specified short name.
15 lookupRequestClassRuntime	
16 preDeregister	Restart all SSL channels on which the server is

- Type **http** in the **Value** field and then click **Invoke**.

The screenshot shows the 'Operation: getURL' dialog box. The 'Value' field contains 'http', which is highlighted with a red box. The 'Invoke' button is also highlighted with a red box. The dialog box contains the following information:

**Operation: getURL**

**Information**  
The changes made on this mbean are not managed by the configuration session. The changes will be applied immediately. You cannot undo the changes from the Change Center.

MBean Name: com.bea.wls.sb.management.OperationsMBean:vgadc01j\_adminserver:Location=vgadc01j\_adminserver,Type=ServerRuntime  
 Operation Name: getURL  
 Description: The URL that clients use when connecting to this server using the specified protocol.

**Note:**  
The listen address and listen part for a given protocol are persisted in the domain's config.xml file, however when a server instance is started, command-line options can override these persisted values. This operation method returns the URL values that are currently being used, not necessarily the values that are specified in config.xml.

Return Type: java.lang.String

Name	Description	Type	Value
protocol	the desired protocol	java.lang.String	<b>http</b>

**Return Value**  
http://vgadc01j:8020b2n-813-jca-wls-L-ops/bca/oradocloud/infant/7101

- Follow the instructions in "Configuring the Proxy Server for Runtime" in *Oracle Cloud Adapters Postinstallation Configuration Guide (12.2.1.4)* to update the `setDomainEnv.sh` file.

You must invoke `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:

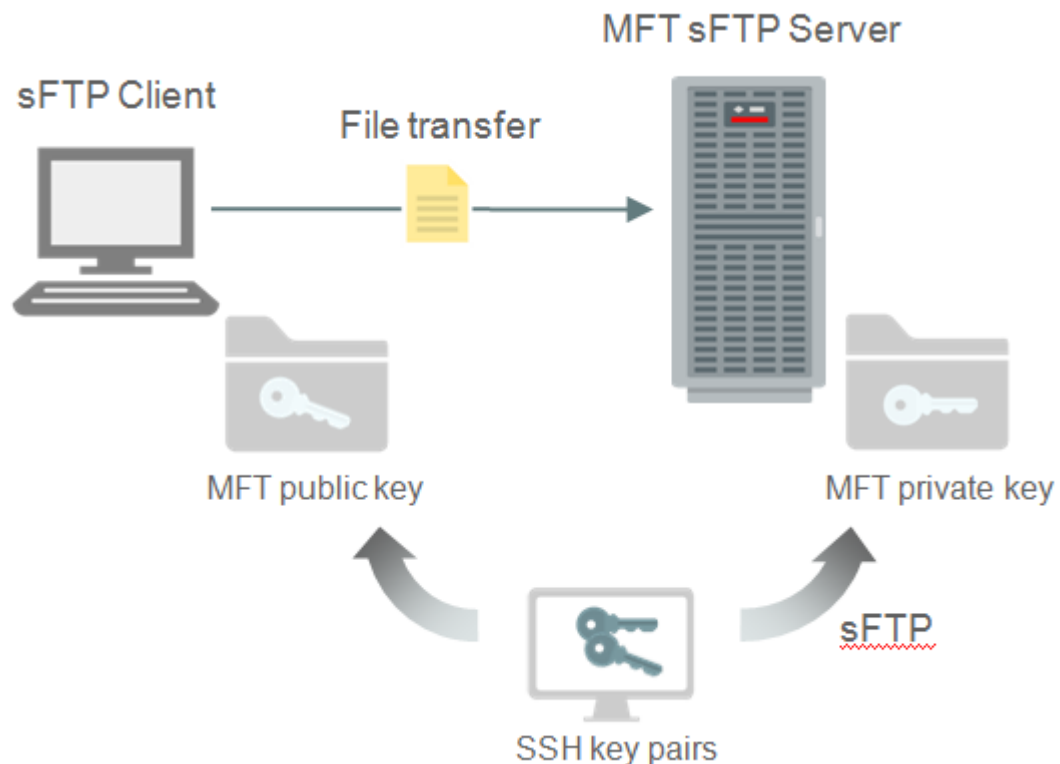
```
-Dhttp.proxyHost=www-proxy.my.url.com -Dhttp.proxyPort=80 -
Dhttp.nonProxyHosts=localhost|*.my.url.com|*.internal| 127.0.0.1|
10.196.75.214|10.*.*.*|*.foo.com|etc -Dhttps.proxyHost=www-
proxy.my.url.com -Dhttps.proxyPort=80
```

8. Restart the Administration Server and Managed Servers for the settings to take effect. See [Stop or Start WebLogic Servers](#).

## Complete 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.



### Topics:

- [Add an Ingress Rule to Allow sFTP Traffic to sFTP Servers](#)

- [Configure the SSH Keystore for the MFT sFTP Server](#)
- [Enable and Start the MFT sFTP Server](#)
- [Connect to MFT Embedded Servers Using the Load Balancer](#)

## Add an Ingress Rule to Allow sFTP Traffic to sFTP Servers

After provisioning, if you need to allow sFTP traffic to sFTP servers, you must add an ingress rule.

To add an ingress rule to allow traffic on the sFTP port:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Select the compartment where you created the new instance.
4. In the list of VCNs, select your VCN.
5. On the Virtual Cloud Network Details page, click **Security Lists** in the left pane.
6. Select a security list and click **Add Ingress Rules** to open the Add Ingress Rules dialog.
7. In the Add Ingress Rules dialog, create an ingress rule to allow sFTP traffic:
  - a. Leave the `STATELESS` checkbox deselected.
  - b. For `SOURCE TYPE`, select **CIDR**.
  - c. In the `SOURCE CIDR` field, enter `0.0.0.0/0`. Alternatively, you can enter a CIDR.
  - d. In the `IP PROTOCOL` field, select `TCP`.
  - e. In the `DESTINATION PORT RANGE` field, enter `7522`.
  - f. Click **Add Ingress Rules**.

## Configure 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.

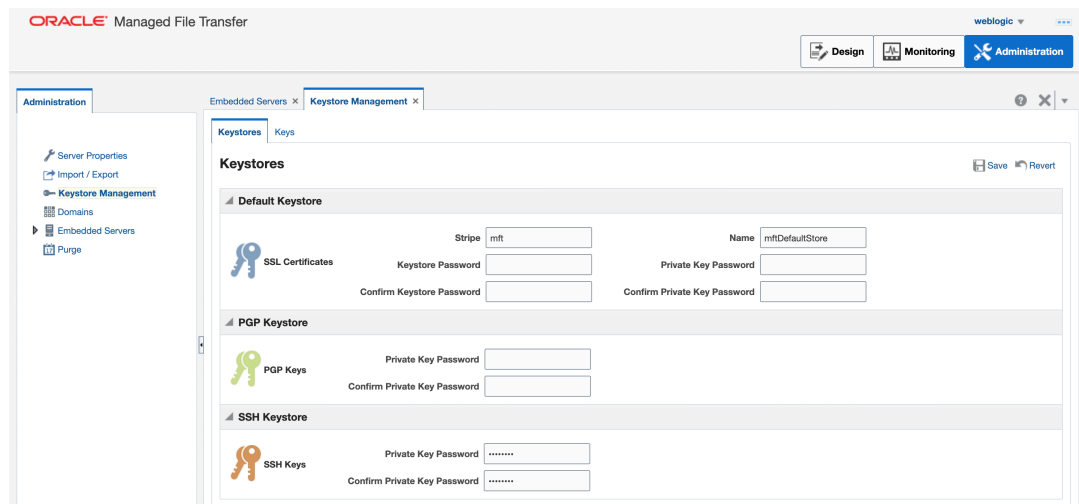
4. Enter the following details:
  - **Alias:** alias name
  - **Format:** select PGP or SSH type of key

- **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 the MFT SSH Keystore.

1. Go to the Details page of the MFT instance you want to access, as described in [View Oracle SOA Suite on Marketplace 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 on Marketplace 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**.

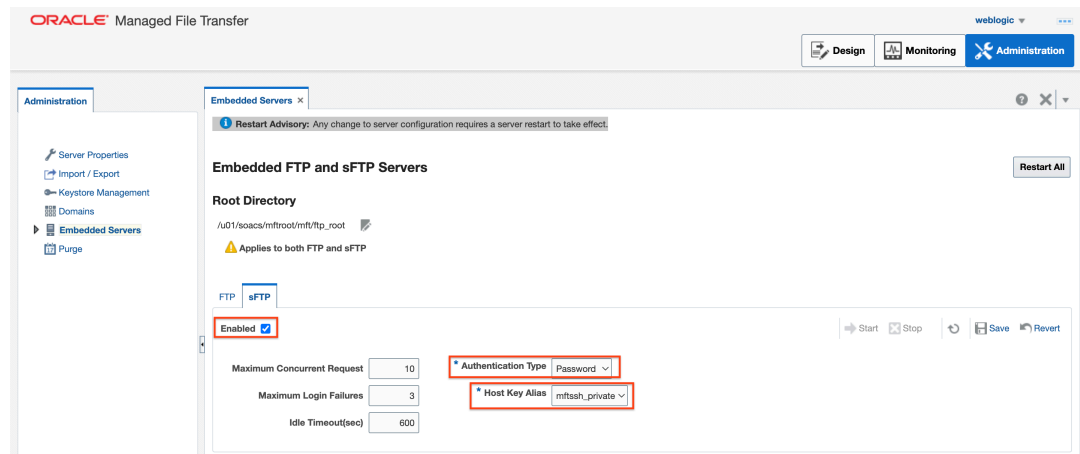
## Enable and Start the MFT sFTP Server

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

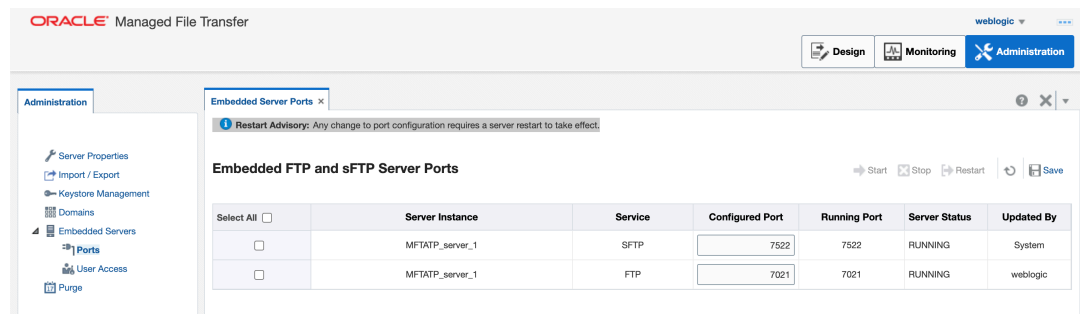
To enable and start the MFT sFTP Server:

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. Log in to the [WebLogic Server Administration Console](#) and 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.



**Note:**

For security reasons, it's recommended to stop the FTP server.

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
sftp> pwd
Remote working directory: /
sftp> exit
```

## Connect to MFT Embedded Servers Using the Load Balancer

To allow sFTP traffic from the public internet to MFT embedded sFTP servers using the load balancer IP address, open the required listener port for the Oracle Cloud Infrastructure load balancer using the Oracle Cloud Infrastructure Console.

To connect to MFT embedded servers through the Oracle Cloud Infrastructure load balancer:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Networking**, and then click **Load Balancers**.
3. Click the name of the Oracle Cloud Infrastructure load balancer to open the Load Balancer Details page.
4. Create backend sets:
  - a. In the left pane, click **Backend Sets**, then click **Create Backend Set**.
  - b. In the Create Backend Set dialog, enter the following information:
    - **Name:** Enter a name for the backend set.
    - **Protocol:** TCP
    - **Port:** 7522
  - c. Click **Create Backend Set**.
5. Create backends:
  - a. In the left pane of the Load Balancer Details page, click **Backend Sets**, then click name of the backend set you just created.
  - b. In the left pane of the Backend Set Details screen, click **Backends**, then click **Add Backends**.
  - c. In the Add Backends dialog, click **Change Compartment** to select the compartment for your Oracle SOA Suite on Marketplace instance if not already displayed, then select the check box next to the instance name, and enter a **Port** value of 7522.  
  
Repeat this step for all nodes in the cluster.
  - d. Click **Add**.
6. Create listeners:
  - a. In the left pane of the Load Balancer Details page, click **Listeners**, then click **Create Listener**.
  - b. In the Create Listener dialog, enter the following information.
    - **Protocol:** TCP
    - **Port:** 7522
    - **Backend set:** Select the backend set you created.



**Create Listener** [Help](#)

There are no hostnames for this load balancer. [Create a hostname.](#)

Protocol: TCP Port: 7522 Use SSL:

Backend Set: Test-lb-backendset

Idle Timeout In Seconds:  *Optional*

The default timeout for TCP is 300 seconds.

Enable Proxy Protocol  
Allows you to securely transport connection information such as a client's IP address across multiple layers of proxies to the backend server. Learn more about [proxy protocol](#).

There are no path route sets for this load balancer. [Create a path route set.](#)

**Create Listener** [Cancel](#)

- c. Click **Create Listener**.
7. Enter the following command to verify that you can connect to MFT embedded servers through the load balancer:

```
sftp -oPort=7522 weblogic@loadbalancerIP
```

## Configure Scheduled Backups

After provisioning, configure scheduled backups as a good practice.

To set up scheduled backups, see [Configure Automatic Block Volume Backups](#).

## Extend 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.

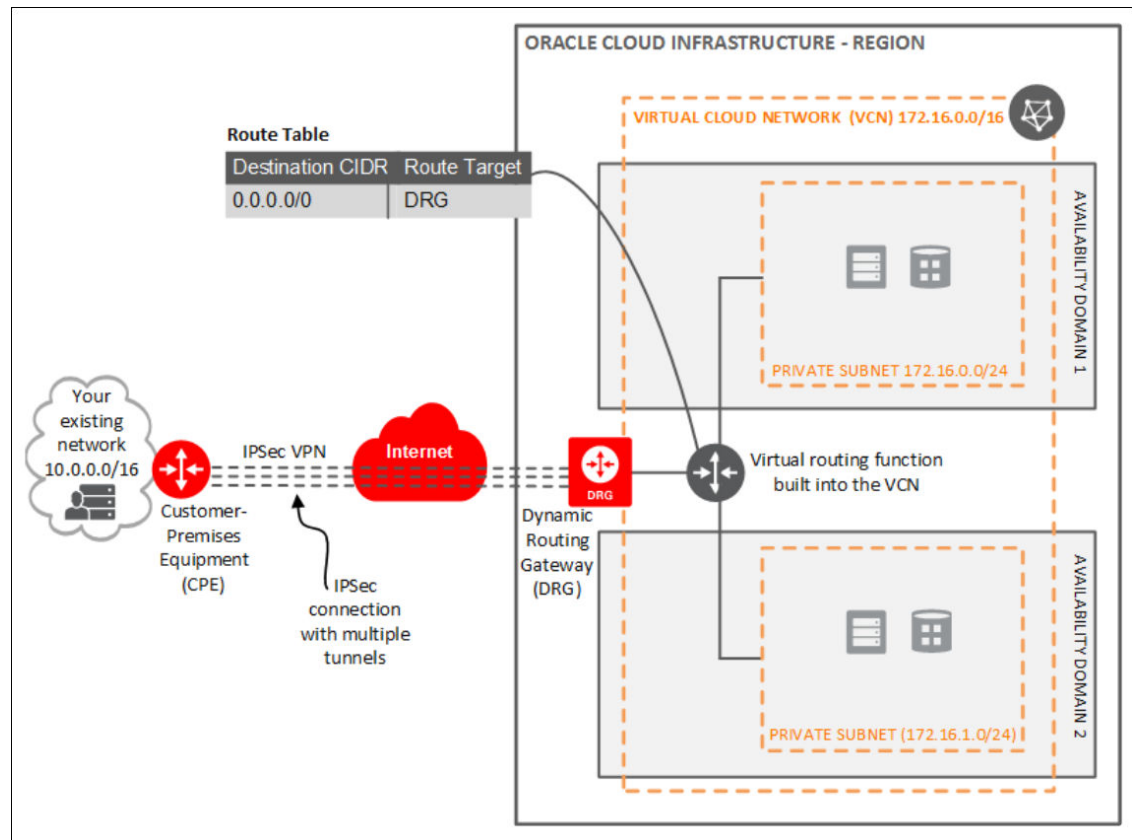
Just like a traditional data center network, a VCN provides you with control over your network environment. This includes assigning your own private IP address space, creating subnets, creating route tables and configuring stateful firewalls. A single tenant can have multiple VCNs, thereby providing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

In summary, the 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. [Sign in to the Oracle Cloud Infrastructure Console.](#)
2. Create a VCN.
  - a. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
  - b. Click **Create VCN**.
  - c. In the Create a Virtual Cloud Network dialog, enter a name for your VCN and select a compartment.
  - d. Click **Create VCN**.

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

3. 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 navigation pane, under **Resources**, select **Subnets**.
  - b. Click **Create Subnet**.

Enter the following details:

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

- c. Click **Create**.
4. Create a Dynamic Routing Gateway (DRG) to provide a path for private network traffic between your VCN and on-premises network.
  - a. Open the navigation menu and click **Networking**. Under **Customer Connectivity**, click **Dynamic Routing Gateway**.
  - b. Click **Create Dynamic Routing Gateway**.
  - c. Specify a compartment, enter a name for the DRG and click **Create**.
5. Once the Dynamic Routing Gateway is created, you can attach it to your VCN.
  - a. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
  - b. Click your VCN to open its details.
  - c. In the Virtual Cloud Network Details page, in the navigation pane, under **Resources**, click **Dynamic Routing Gateways**.
  - d. Click **Attach Dynamic Routing Gateway**.
  - e. Select the dynamic routing gateway that you created and click **Create**.
6. 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. Open the navigation menu, and click **Networking**. Under **Customer Connectivity**, click **Customer-Premises Equipment**.



## Register 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.

## View Oracle SOA Suite on Marketplace Instance Details

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

To view stack details for an Oracle SOA Suite on Marketplace instance and perform stack actions:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Developer Services**. Under **Resource Manager**, click **Stacks**.
3. If the stack is in a compartment, select the compartment in the **Compartment** field.
4. 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 Stack Details page:

Field	Description
<b>Stack Information</b> tab	<ul style="list-style-type: none"><li>• Usage instructions.</li><li>• Description of the stack.</li><li>• Compartment to which the stack is assigned.</li><li>• OCID value that uniquely identifies the stack.</li><li>• Created date and time.</li><li>• Terraform version.</li></ul>
<b>Edit Stack</b>	Click to edit the provisioning settings for the stack.
<b>Move Stack</b>	Click to move the stack to a different compartment. This action can take some time to complete.

Field	Description
<b>Terraform Actions</b>	<p>Click to select the following actions to perform on the selected stack and instance:</p> <ul style="list-style-type: none"> <li>• <b>Plan</b>: Creates the build plan for the environment required to create an instance.</li> <li>• <b>Apply</b>: Executes the Plan operation to create the instance.</li> <li>• <b>Import State</b></li> <li>• <b>Destroy</b>: Deletes the RCU schemas, 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 <b>Plan</b> and <b>Apply</b> operations. See <a href="#">Deprovision an Oracle SOA Suite on Marketplace Instance</a>.</li> </ul>
<b>Delete Stack</b>	<p>Click to delete the selected stack after selecting <b>Terraform Actions&gt;Destroy</b>. See <a href="#">Deprovision an Oracle SOA Suite on Marketplace Instance</a>.</p>
<b>Add Tags</b>	<p>Click to add tags to the selected stack. You can use tags to search for and categorize your instances in your tenancy. See <a href="#">Resource Tags</a>.</p>
<b>Tags tab</b>	<p>Displays any tags associated with the stack. Click <b>Add Tags</b> to add a tag.</p>
<b>Jobs section</b>	<p>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 on Marketplace instance. See <a href="#">Access an Oracle SOA Suite on Marketplace Instance</a>. On the Job Details page, you can download:</p> <ul style="list-style-type: none"> <li>• Logs .log file</li> <li>• Terraform configuration .zip file</li> <li>• Terraform state .json file</li> </ul>
<b>Application information tab</b>	<p>Displays the following details of the Oracle SOA Suite on Marketplace instance.</p> <ul style="list-style-type: none"> <li>• <b>Service Type</b></li> <li>• <b>SOAMP Stack Version</b></li> <li>• <b>SOAMP Cluster Size</b></li> <li>• Service Console URL links</li> <li>• Associated services such as <b>Database</b> and <b>Loadbalancer</b></li> </ul>

To view the compute instance details:

1. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
2. Click the instance name to display its details on the **Instance Information** and **Tags** tabs.

## Access an Oracle SOA Suite on Marketplace Instance

You can access an Oracle SOA Suite on Marketplace 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 on Marketplace instances. For users without view (or greater) permission to the console, a URL to the 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 on Marketplace instance:

1. Go to the Stack Details page of the instance you have provisioned, as described in [View Oracle SOA Suite on Marketplace 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:

```

FMW Console = https://150.136.163.170:7002/em
Instance Subnet Id = [
  ocid1.subnet.oc1.iad.aaaaaaaabjhebpwnpzgqchveglt5dqs6pv4o6dzb3eexmlwtqfeuofe3yq
]
Load Balancer Public Ip = [
  129.213.69.88
]
Loadbalancer Subnets Id = [
  ocid1.subnet.oc1.iad.aaaaaaaaywbc7q16ategyd4l6an6ysp6cskuyo3jsiqts2yy4x2wea6ha
]
Service Consoles =
SOA Composer      : https://129.213.69.88/soa/composer
B2B Console       : https://129.213.69.88/b2bconsole
Service Bus Console : https://150.136.163.170:7002/servicebus
Worklist Application : https://129.213.69.88/integration/worklistapp
Service Instances = [
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwlcljtnkmd4bychespdxj7bk6s5m6t6isstdqvw6dz2ep1mm5mhg6hoaa",
    "Instance name": "TESTKK-soa-0",
    "Private IP": "10.0.23.3",
    "Public IP": "150.136.163.170"
  },
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwlcljtnkmd4bycmingnhuyzajqzfv7akeutg12i4fry6mw1msyao4h6aq",
    "Instance name": "TESTKK-soa-1",
    "Private IP": "10.0.23.2",
    "Public IP": "150.136.161.126"
  }
]
Version = 12.2.1.4 (JRF with OCI DB)
Virtual Cloud Network Id = ocid1.vcn.oc1.iad.aaaaaaaajnyj3pvohrm2qwg1ghkfwmmqf7g33oh6af12eb3qaaywdkuf1n6q
Weblogic administration Console = https://150.136.163.170:7002/console
for MFT we will display mft URL in service Console URLs, remaining is same
Service Consoles =
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.

Service Type	Component	Provisioned with Load Balancer	Provisioned without Load Balancer
Any	Public (Admin) IP	150.136.163.170	150.136.163.170
	Load Balancer IP	129.213.69.88	N/A
	Administration Console	https:// 150.136.163.170:7002/ console	https:// 150.136.163.170:7002/ console
	FMW Console	https:// 150.136.163.170:7002/em	https:// 150.136.163.170:7002/em
<b>SOA with SB &amp; B2B Cluster</b>	SOA Composer	https:// <b>129.213.69.88</b> /soa/ composer	https:// 150.136.163.170/soa/ composer

Service Type	Component	Provisioned with Load Balancer	Provisioned without Load Balancer
	B2B Console	https:// <b>129.213.69.88</b> /b2bconsole	https://150.136.163.170/b2bconsole
	Service Bus Console	https://150.136.163.170:7002/servicebus	https://150.136.163.170:7002/servicebus
	Worklist Application	https:// <b>129.213.69.88</b> /integration/worklistapp	https://150.136.163.170/integration/worklistapp
<b>MFT Cluster</b>	MFT Console	https:// <b>129.213.69.88</b> /mftconsole	https://150.136.163.170/mftconsole
<b>BAM Cluster</b>	BAM Composer	https:// <b>129.213.69.88</b> /bam/composer	https://150.136.163.170/bam/composer
	BAM dashboards Note: Create and use ADF-based dashboards. JET-based dashboards are not certified for a multinode BAM cluster.	https:// <b>129.213.69.88</b> /bam/composer/faces/proxypage?project=projectName&dashboard=dashboardName	https://150.136.163.170/bam/composer/jet/dashboard?project=projectName&dashboard=dashboardName

5. Enter a URL in your browser to display the associated component in the Oracle SOA Suite on Marketplace instance.

## Migrate or Upgrade to an Oracle SOA Suite on Marketplace Instance

You can migrate or upgrade your existing on-premises Oracle SOA Suite instances or Oracle SOA Cloud Service Classic instances to Oracle SOA Suite on Marketplace instances in Oracle Cloud Infrastructure.

The high-level steps are:

- Set up an Oracle SOA Suite on Marketplace instance.
- Export SOA composite applications, Oracle Service Bus, and Managed File Transfer projects, and other configurations such as data sources and policies from your source system.
- Import SOA composite applications, Oracle Service Bus and Managed File Transfer projects, and other configurations from the source into the Oracle SOA Suite on Marketplace instance.
- Test the new Oracle SOA Suite on Marketplace instance.
- Retire the old SOA, Oracle Service Bus, and MFT servers.

For full details and limitations, see the following resources:

- To migrate existing Oracle SOA Cloud Service Classic instances to Oracle SOA Suite on Marketplace instances in Oracle Cloud Infrastructure, see *Migrating Oracle SOA Cloud Service Classic Instances to Oracle Cloud Infrastructure*.



- To migrate existing on-premises Oracle SOA Suite instances to Oracle SOA Suite on Marketplace instances in Oracle Cloud Infrastructure, see *Migrating to the Cloud and Side-by-Side Upgrade in the Cloud for SOA on Marketplace, SOA Cloud Service, and MFT Cloud Service*.
- To migrate existing Oracle SOA Cloud Service instances to Oracle SOA Suite on Marketplace instances using the Oracle SOA Suite migration manager, see [Migrate Oracle SOA Cloud Service Instances to Oracle SOA Suite on Marketplace Using the Migration Manager](#).

## Migrate Oracle SOA Cloud Service Instances to Oracle SOA Suite on Marketplace Using the Migration Manager

The Oracle SOA Suite migration manager is an automated tool that enables you to migrate your existing Oracle SOA Cloud Service instances running on Oracle Cloud Infrastructure (OCI) to Oracle SOA Suite on Marketplace.

### Note:

- The Oracle SOA Suite migration manager is available as a stack listing on the OCI Marketplace.
- The Oracle SOA Cloud Service domains and RCU schemas are reused in the new Oracle SOA Suite on Marketplace instance, ensuring that the domain-level configurations and deployments remain intact.
- There are no additional charges for using the Oracle SOA Suite migration manager since it does not create any new OCI resources.

## Prerequisites for Migration

### Prerequisites for Migration in the Source Oracle SOA Cloud Service

Before initiating migration, you must meet or complete the following prerequisites in the source Oracle SOA Cloud Service instance.

- The source version of the Oracle SOA Cloud Service instance is 12.2.1.3 or higher, with the latest Oracle SOA bundle patch installed. If your Oracle SOA Cloud Service instance is 12.2.1.2 or earlier versions, upgrade to either 12.2.1.3 or 12.2.1.4. See *Understand Migration and Side-by-Side Upgrade for SOA Cloud Service*.

Also, ensure that you apply the latest bundle patch. See *Patches Installed By Release*.

- If your Oracle SOA Cloud Service instance has Oracle Traffic Director (OTD) load balancer, switch to OCI load balancer and configure the necessary SSL certificates before initiating the migration since OTD is not supported in Oracle SOA Suite on Marketplace. See *Administer the Load Balancer for an Oracle SOA Cloud Service Instance*.
- The OCI load balancer is reused in the Oracle SOA Suite on Marketplace instance. After the migration, you must manually update the OCI load balancer's backend sets with the Oracle SOA Suite on Marketplace virtual machine. See [Editing a Load Balancer Backend Set](#).
- If the source Oracle SOA Cloud Service instance is built on the Classic Database systems, migrate the RCU schemas to the OCI DBCS. The Oracle domains and RCU schemas are

reused in the new Oracle SOA Suite on Marketplace instance, ensuring that the domain-level configurations and deployments remain intact. Make sure that you have the Oracle SOA Cloud Service VM's SSH private key. The SSH private key must be specified while initiating the migration. Also, ensure that your SSH private key does not contain any passphrase.

- Shut down the Oracle SOA Cloud Service servers before initiating the migration. See [Shut Down and Start Server Process](#).

The Oracle SOA Cloud Service Virtual Machines (VMs) must be up and running.

### Prerequisites for Migration in the Target Oracle SOA Suite on Marketplace

Oracle recommends auto-provisioning the target Oracle SOA Suite on Marketplace instance. However, you can choose to manually provision the target instance.

If you choose to manually provision the target instance, before you initiate the migration, you must meet or complete the following prerequisites.

- Provision a new Oracle SOA Suite on Marketplace instance with 23.2.2 or later versions. See [SOAMP Provision an Oracle SOA Suite Instance](#).
  - Provision the target instance in the same subnet as the source instance.
  - Provision the target instance with the same cluster size as the source instance.
  - Provision the target instance with the same WLS admin username, password, domain name, cluster name, admin server name, managed server name, and machine names as the source instance. You can configure custom names in the Advanced Configuration section in the provisioning UI of Oracle SOA Suite on Marketplace.
- Ensure that the database is accessible from the Oracle SOA Suite on Marketplace instance. The Oracle SOA Cloud Service domains, databases, and RCU schemas are reused by the new Oracle SOA Suite on Marketplace domain, ensuring that all the domain-level configurations and deployments remain intact.
- Ensure that the database is accessible from the Oracle SOA Suite on Marketplace instance. The Oracle SOA Cloud Service domains, databases, and RCU schemas are reused by the new Oracle SOA Suite on Marketplace domain, ensuring that all the domain-level configurations and deployments remain intact.
- Make sure you have the Oracle SOA Suite on Marketplace VM's SSH private key. The SSH private key must be specified while initiating the migration. Also, ensure that your SSH private key does not contain any passphrase.
- Manually replicate the following in the Oracle SOA Suite on Marketplace instance.
  - Move the custom logic deployments (libraries and web applications) outside the domain home in the source Oracle SOA Cloud Service instance to the same path in the target Oracle SOA Suite on Marketplace instance. The migration manager automatically migrates the custom XPath functions and the adapter configuration files.
  - Replicate the custom entries in the `/etc/hosts` file in Oracle SOA Cloud Service instance in the Oracle SOA Suite on Marketplace instance.

## Generate the Migration Report

The migration report highlights the differences between the Oracle SOA Cloud Service and the Oracle SOA Suite on Marketplace instances. You can generate the migration report before you run the migration. This is an optional feature that is available as part of the migration stack.

### Note:

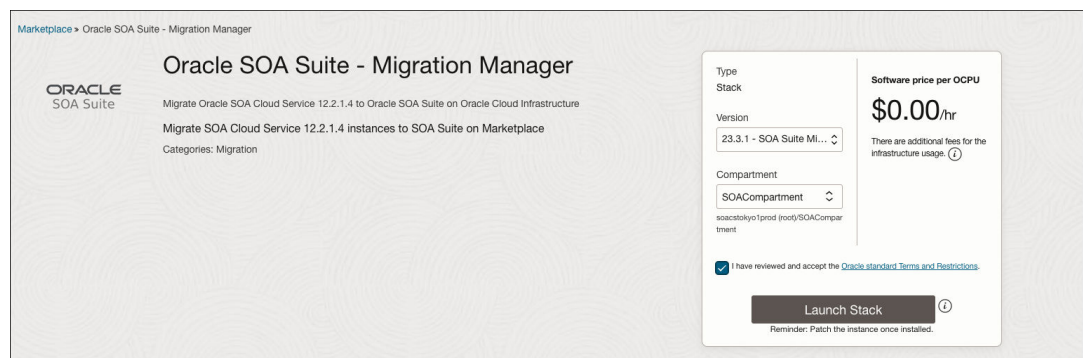
- You can generate multiple migration reports. Each report's file name is suffixed with a timestamp. For example, `migration_report_<timestamp>.txt`.
- You can either generate the report before the migration or while you migrate the Oracle SOA Cloud Service instance to the Oracle SOA Suite on Marketplace. See step 4 in [Run the Migration](#).
- The migration report is generated on the admin virtual machine in the Oracle SOA Suite on Marketplace.
- Once the report generation is complete, you can find the report in the following location: `/u01/logs/migration_report_<timestamp>.txt`.

The migration report has the following sections that highlight the differences between the Oracle SOA Cloud Service and the Oracle SOA Suite on Marketplace instances.

1. Patches applied in the Oracle SOA Cloud Service instance but not in the Oracle SOA Suite on Marketplace instance.
2. Patches applied in the Oracle SOA Suite on Marketplace instance but not in the Oracle SOA Cloud Service instance.
3. Custom mount paths in the Oracle SOA Cloud Service instance.
4. Custom deployments (EAR/WAR) in the Oracle SOA Cloud Service instance.
5. Custom libraries in the Oracle SOA Cloud Service instance.

Perform the following steps to generate the migration report.

1. In the OCI marketplace, choose **Oracle SOA Suite – Migration Manager**.



The home page of the migration stack listing is displayed.

2. Click **Launch Stack**.

The Create Stack page is displayed.

3. In the Stack information section, specify the name and description of the migration stack, and click **Next**.

Create stack

1 Stack information  
2 Configure variables  
3 Review

Your application will launch as part of a stack that includes the infrastructure resources required to ensure that the application deploys and runs properly.

Stack information

SOA Migration Terraform Input Variables

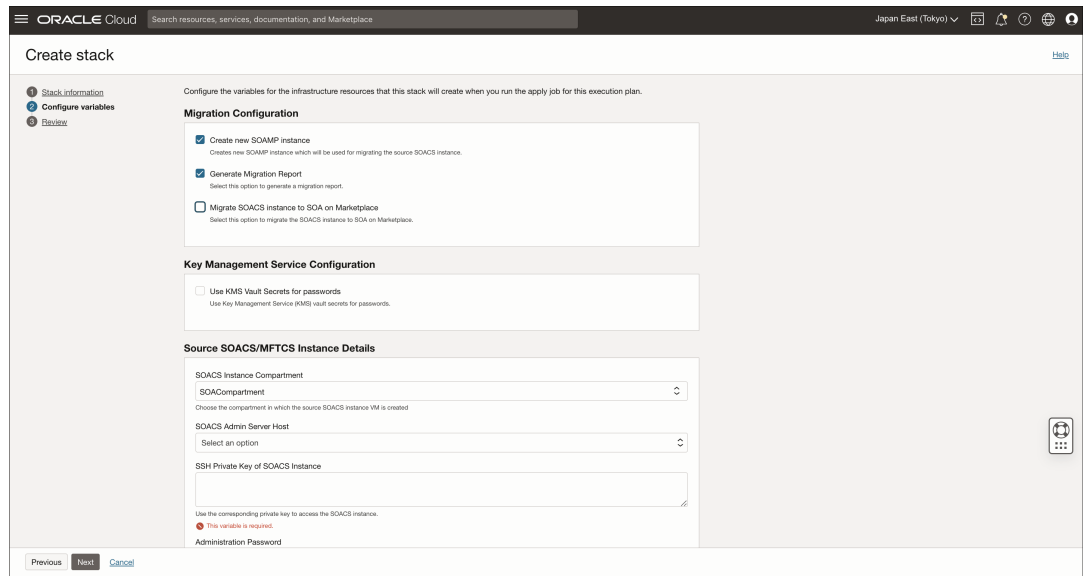
Custom providers

Use custom Terraform providers  
[Store custom Terraform providers in a bucket.](#)

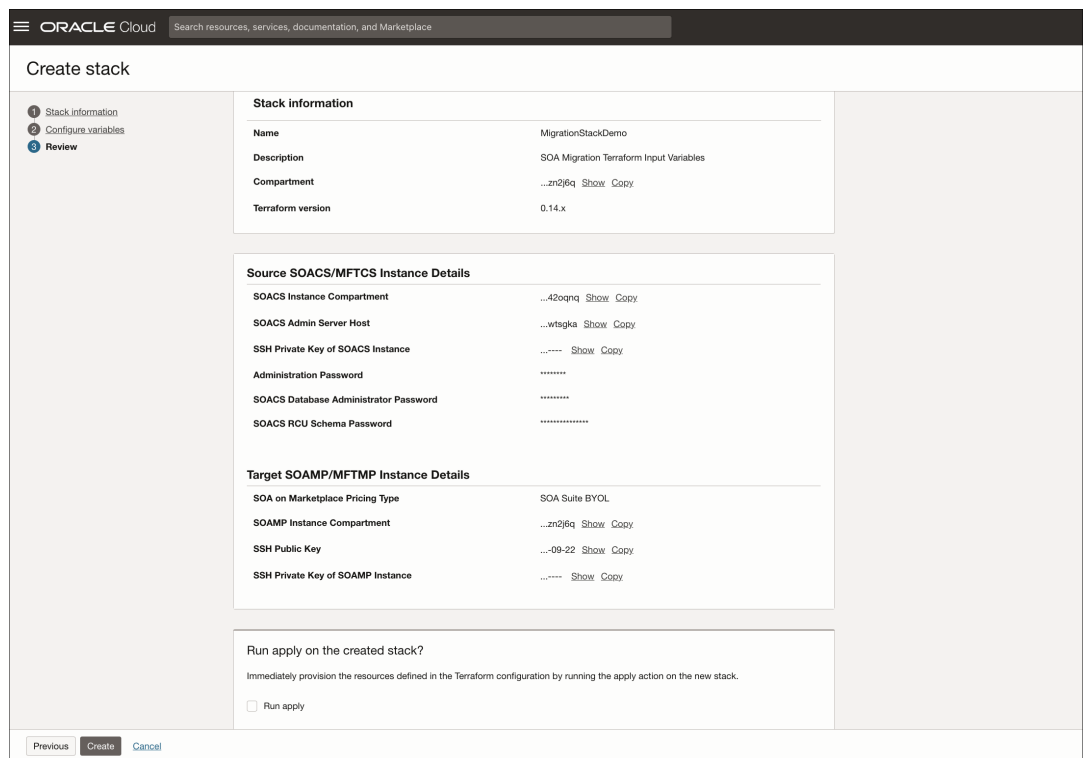
Name *Optional*  
Oracle SOA Suite - Migration Manager-20230704120958

Description *Optional*  
SOA Migration Terraform Input Variables

4. In the Configure variables section, specify the following details.
  - a. Select **Generate Migration Report**.
  - b. To auto-provision a Oracle SOA Suite on Marketplace instance, select **Create new SOAMP instance**.
  - c. Specify the **Instance Compartment, Admin Server Host, SSH Private Key, Administration Password, Database Administrator Password, and RCU Schema Password** of the source Oracle SOA Cloud Service instance.
  - d. Specify the **Pricing Type, Instance Compartment, Name Prefix, Domain Volume Size (GB), SSH Public Key, and SSH Private Key** of the target Oracle SOA Suite on Marketplace.



5. If either the source Oracle SOA Cloud Service or the target Oracle SOA Suite on Marketplace instances are in a private subnet, specify either the private endpoint or the Bastion host details to establish SSH connection.
6. Click **Next**.
7. In the Review section, review the details of the source and target instances. Select **Run apply** to automatically trigger the apply job operation when the migration stack is created.



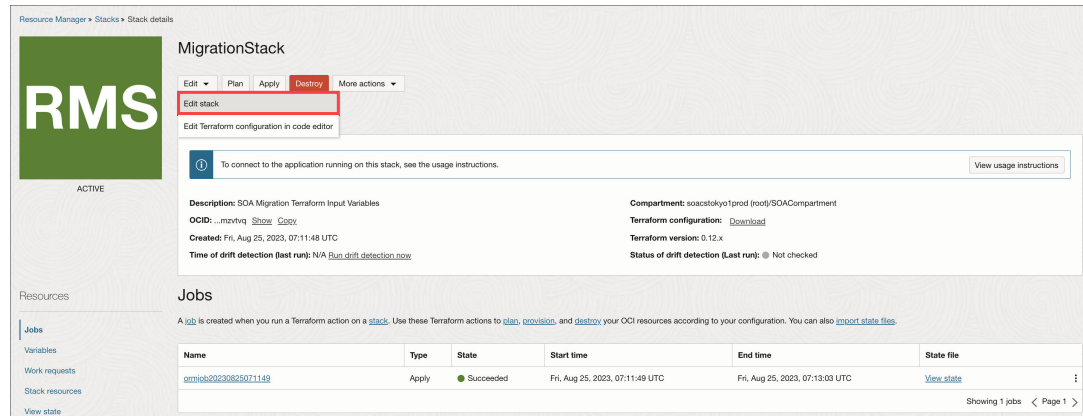
8. Click **Create** to create the migration stack. The apply job operation is automatically triggered.

Once the report generation is complete, you can find the report in the following location: /u01/logs/migration\_report\_<timestamp>.txt.

## Run the Migration Manager by Editing the Migration Stack

After generating the report, you can edit the migration stack to run the migration manager.

1. On the Migration Stack page, click **Edit** and select **Edit stack**.



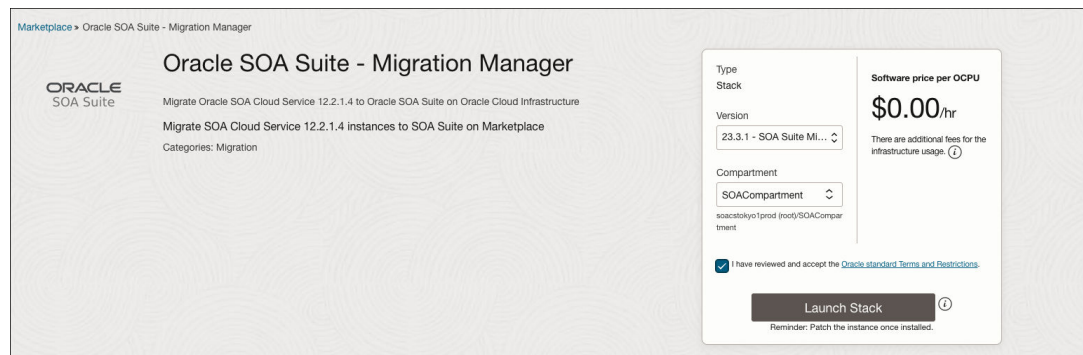
2. In the Stack information section, click **Next**.
3. In the Configure variables section, select **Migrate SOACS instance to SOA on Marketplace** and click **Next**.
4. In the Review section, select **Run apply** and click **Save changes**.

The apply job operation is automatically triggered.

## Run the Migration Manager

The migration manager is available as a stack listing in the OCI marketplace. Perform the following steps to run the automated migration tool.

1. In the OCI marketplace, choose **Oracle SOA Suite – Migration Manager**.



The home page of the migration stack listing is displayed.

2. Click **Launch Stack**.

The Create Stack page is displayed.

3. In the Stack information section, specify the name and description of the migration stack, and click **Next**.

### Create stack

- 1 Stack information
- 2 Configure variables
- 3 Review

Your application will launch as part of a stack that includes the infrastructure resources required to ensure that the application deploys and runs properly.

Stack information

SOA Migration Terraform Input Variables

Custom providers

Use custom Terraform providers

[Store custom Terraform providers in a bucket.](#)

Name Optional

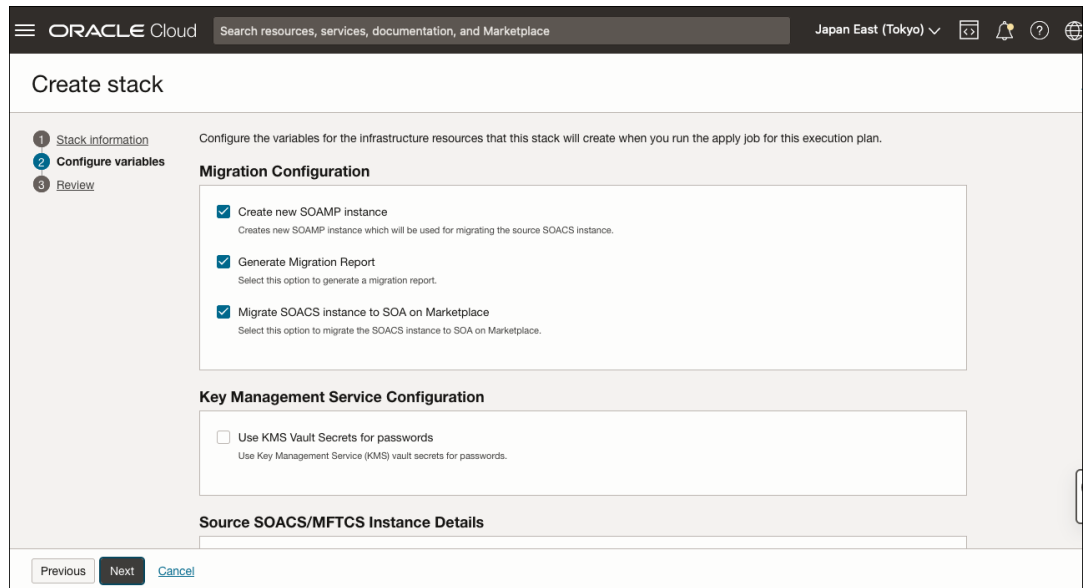
Description Optional

4. In the Configure variables section, specify the following details.
  - a. (Optional) To generate the migration report, select **Generate Migration Report**.
  - b. (Optional) To auto-provision a Oracle SOA Suite on Marketplace instance, select **Create new SOAMP instance**.
  - c. Select **Migrate SOACS instance to SOA on Marketplace** to run the migration.

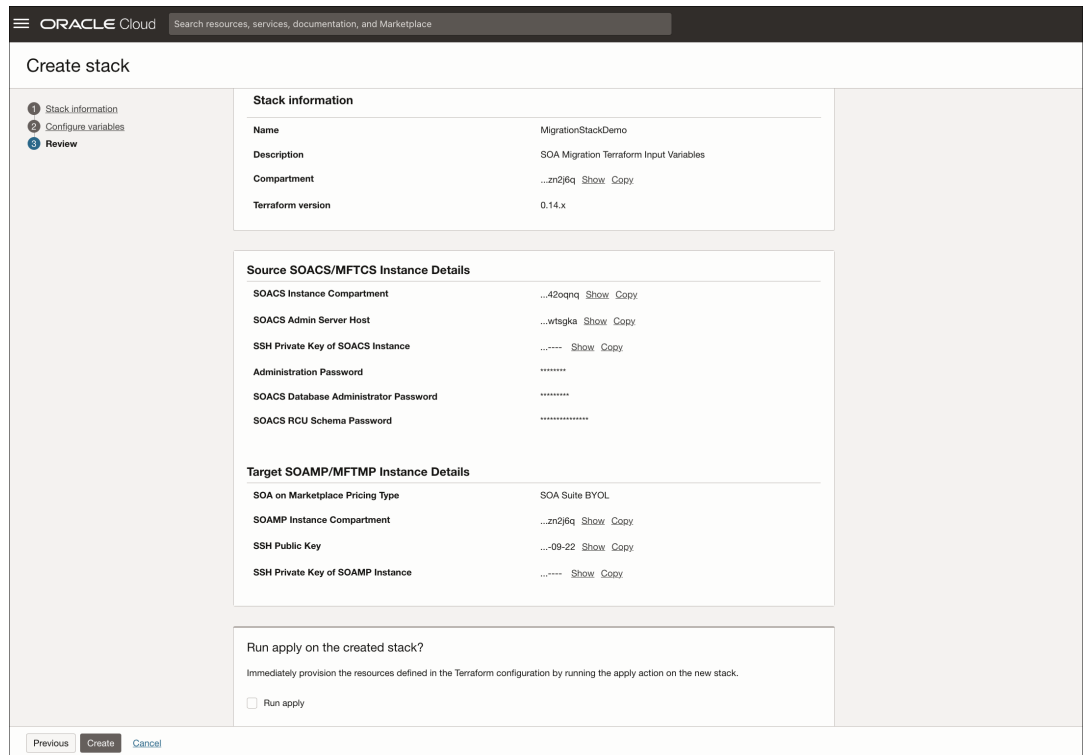
**Note:**

You can either generate the migration report before the migration or generate the migration report and run the migration simultaneously. To generate the migration report alone, see [Generate the Migration Report](#).

- d. Specify the **Instance Compartment**, **Admin Server Host**, **SSH Private Key**, **Administration Password**, **Database Administrator Password**, and **RCU Schema Password** of the source Oracle SOA Cloud Service instance.
- e. Specify the **Pricing Type**, **Instance Compartment**, **Name Prefix**, **Domain Volume Size (GB)**, **SSH Public Key**, and **SSH Private Key** of the target Oracle SOA Suite on Marketplace.



5. If either the source Oracle SOA Cloud Service or the target Oracle SOA Suite on Marketplace instances are in a private subnet, specify either the private endpoint or the Bastion host details to establish SSH connection.
6. Click **Next**.
7. In the Review section, review the details of the source and target instances. Select **Run apply** to automatically trigger the apply job operation when the migration stack is created.



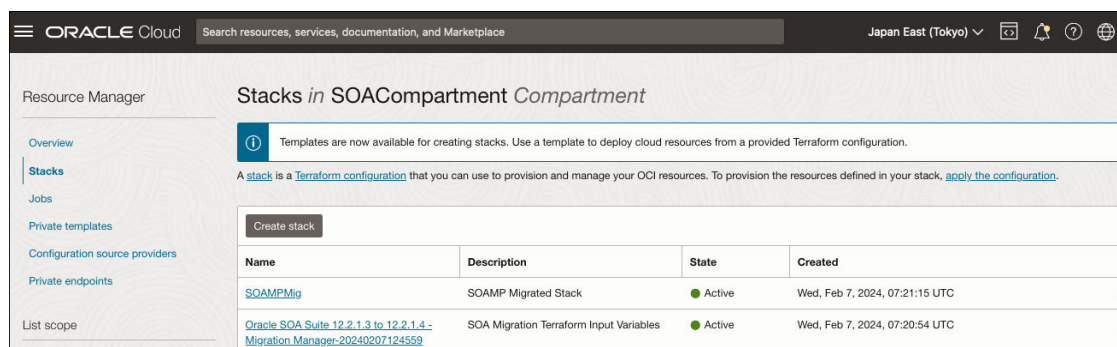
8. Click **Create** to create the migration stack. The apply job operation is automatically triggered.



After the migration, ensure that you move any custom files or deployments located outside the Domain Home in the source Oracle SOA Cloud Service instance to the target Oracle SOA Suite on Marketplace instance.

## Review the Migrated Oracle SOA Suite on Marketplace Stack

After the migration, the Oracle SOA Suite on Marketplace stack is created in the Oracle Cloud Infrastructure console.



## Delete the Oracle SOA Suite on Marketplace RCU Schemas

### Note:

This step is optional if you auto-provision a Oracle SOA Suite on Marketplace instance as part of the migration.

After the migration, the Oracle SOA Suite on Marketplace domain uses the Oracle SOA Cloud Service RCU schemas. You can delete the new Oracle SOA Suite on Marketplace RCU schemas that are created as part of provisioning. To do so, run the following command.

```
$/opt/scripts/migration/deleteSoampRCU.sh <SYS_DB_PASSWORD>
<RCU_SCHEMA_PREFIX>
```

## Update Oracle SOA Suite on Marketplace Stack Variables

### Note:

This step is optional if you auto-provision a Oracle SOA Suite on Marketplace instance as part of the migration.

After the migration, you must update the RCU schema prefix and the stack variables (DB details and WLS admin credentials) in Oracle SOA Suite on Marketplace to match the Oracle SOA Cloud Service domain configuration.

### Update the RCU Schema Prefix

Edit the `/u01/app/oracle/private/schemaPrefix` file in the Oracle SOA Suite on Marketplace virtual machine and replace the existing RCU schema prefix with the Oracle SOA Cloud Service RCU schema prefix.

### Update the Stack Variables

To update the Oracle SOA Suite on Marketplace stack variables, see [Steps To Update SOAMP Stack Variables](#).

Review and update the following stack variables.

### WLS Admin Credentials

- `wls_admin_user`
- `wls_admin_password` (if KMS is not enabled)
- `wls_kms_admin_secret_compartment_id` (if KMS is enabled)
- `wls_kms_admin_password_ocid` (if KMS is enabled)

### OCI DB Details:

- `ocidb_compartment_id`
- `ocidb_dbssystem_id`
- `ocidb_dbhome_id`
- `ocidb_database_id`
- `ocidb_pdb_service_name`
- `oci_db_port`
- `oci_db_password` (if KMS is not enabled)
- `oci_kms_db_secret_compartment_id` (if KMS is enabled)
- `oci_kms_db_password_ocid` (if KMS is enabled)

### ATP Details

- `atp_db_compartment_id`
- `atp_db_id`
- `atp_db_level`
- `custom_atp_db_level`
- `atp_db_password` (if KMS is not enabled)
- `atp_kms_db_secret_compartment_id` (if KMS is enabled)
- `atp_kms_db_password_ocid` (if KMS is enabled)

## Rollback Migration

If the migration fails, you can revoke the migration changes by running the **Destroy** job.

Resource Manager > Stacks > Stack details

**RMS**  
ACTIVE

Edit Plan Apply **Destroy** More actions

Stack information Tags

Description: SOA Migration Terraform Input Variables  
OCID: ...jchy2a [Show](#) [Copy](#)  
Created: Mon, Jun 12, 2023, 15:32:26 UTC  
Time of drift detection (last run): N/A [Run drift detection now](#)

Compartment:  
Terraform configuration: [Upload](#) [Download](#)  
Terraform version: 0.12.x  
Status of drift detection (Last run):  Not checked

Resources

Jobs

A [job](#) is created when you run a Terraform action on a [stack](#). Use these Terraform actions to [plan](#), [provision](#), and [destroy](#) your OCI resources according to your configuration.

Name	Type	State	Start time	End time
<a href="#">ormjob20230612153227</a>	Apply	<span style="color: green;">●</span> Succeeded	Mon, Jun 12, 2023, 15:32:27 UTC	Mon, Jun 12, 2023, 15:32:27 UTC



**Note:**

You must manually undo any changes made before or after the migration.

Restart the Oracle SOA Cloud Service servers, since they have shut down as a result of the rollback.

## Frequently Asked Questions About the Oracle SOA Suite Migration Manager

Review the following frequently asked questions about the Oracle SOA Suite migration manager.

Question	Description
What is the average duration of the migration process?	The migration time varies based on the size of the Oracle SOA Cloud Service cluster. Migrating the Oracle SOA Cloud Service clusters with two nodes take 10-15 minutes. The Oracle SOA Cloud Service cluster nodes are migrated in sequence. After the migration of each cluster node, the managed servers are initiated.
Will the Oracle SOA Cloud Service instance backups be available after the migration?	No. The Oracle SOA Cloud Service instance backups will not be available after the migration.
How do I terminate the Oracle SOA Cloud Service instance after the migration?	Once you validate the migrated Oracle SOA Suite on Marketplace instance, you can terminate the Oracle SOA Cloud Service instance from the Oracle SOA Cloud Service console. See About Stopping or Starting an Oracle SOA Cloud Service Instance and Individual VMs.
How do I ensure that the Oracle SOA Cloud Service RCU schemas are not deleted while terminating the Oracle SOA Cloud Service instances?	The migration process ensures that the RCU Schemas in the Oracle SOA Cloud Service are not deleted. You must terminate the Oracle SOA Cloud Service instance with force deletion enabled.

Question	Description
How do I delete the RCU schemas in the Oracle SOA Suite on Marketplace instance, which is left unused after the migration?	See <a href="#">Delete the Oracle SOA Suite on Marketplace RCU Schemas</a> .
Can I run life cycle operations on the migrated Oracle Suite on Marketplace instances?	Yes. Before running the life cycle operations, you must update the stack variables in the Oracle SOA Suite on Marketplace instance. See <a href="#">Update Oracle SOA Suite on Marketplace Stack Variables</a> .
How do I undo the migration in case of a failure?	You can undo the migration by running the destroy job of the migration stack. See <a href="#">Rollback Migration</a> . You must restart the Oracle SOA Cloud Service servers since they shut down during the rollback.

# 5

## Deploy Applications for Oracle SOA Suite on Marketplace

This chapter includes topics related to deployment of Oracle SOA Suite on Marketplace instances.

### Topics:

- [Deploy and Undeploy Applications for an Oracle SOA Suite on Marketplace Instance](#)
- [Use a Shared File System](#)
- [Access the WSDL of a Composite Deployed to a SOA Server](#)
- [Use the Frontend Host and HTTPS Port Values in the WSDL URL for Inbound Cloud Adapters](#)

## Deploy and Undeploy Applications for an Oracle SOA Suite on Marketplace Instance

This section describes deploying and undeploying applications to an Oracle SOA Suite on Marketplace instance by using JDeveloper, Fusion Middleware Control, the WebLogic Server Administration Console, and WLST commands.

### Topics:

- [Overview of Deployment Tasks for an Oracle SOA Suite on Marketplace Instance](#)
- [Use Oracle JDeveloper to Deploy Applications](#)
- [Use Oracle Enterprise Manager Fusion Middleware Control to Deploy an Application](#)
- [Use the WebLogic Server Administration Console to Deploy and Undeploy an Application](#)
- [Use WLST Commands to Deploy and Undeploy an Application](#)
- [Access an Application Deployed to an Oracle SOA Cloud Service Instance](#)

## Overview of Deployment Tasks for an Oracle SOA Suite on Marketplace Instance

Consider the typical tasks for deploying and undeploying an application to an Oracle SOA Suite on Marketplace instance, as shown in the following table.

Task	Description	More Information
Use Oracle JDeveloper	Deploy SOA composite applications and Oracle Service Bus applications.	<a href="#">Use Oracle JDeveloper to Deploy Applications</a>
Use Fusion Middleware Control	Deploy and undeploy applications just as you would for an on-premise service instance.	<a href="#">Use Oracle Enterprise Manager Fusion Middleware Control to Deploy an Application</a>

Task	Description	More Information
Use the WebLogic Server Administration Console	Deploy and undeploy applications just as you would for an on-premise service instance.	<a href="#">Use the WebLogic Server Administration Console to Deploy and Undeploy an Application</a>
Use WLST commands	Use WLST commands online or offline to deploy an application.	<a href="#">Use WLST Commands to Deploy and Undeploy an Application</a>
Access a deployed application	Copy the public IP address of the load balancer into the URL for the application.	<a href="#">Access an Application Deployed to an Oracle SOA Cloud Service Instance</a>

## Use Oracle JDeveloper to Deploy Applications

You can use Oracle JDeveloper to deploy SOA composite applications and Oracle Service Bus applications to an Oracle SOA Suite on Marketplace instance.

### Topics:

- [Add an Ingress Rule to Allow the JDeveloper Connection](#)
- [Create an Application Server Connection in JDeveloper](#)
- [Deploy a SOA Composite Application to Oracle SOA Suite on Marketplace from JDeveloper](#)
- [Deploy an Oracle Service Bus Application to Oracle SOA Suite on Marketplace from JDeveloper](#)

## Add an Ingress Rule to Allow the JDeveloper Connection

After provisioning the Oracle SOA Suite on Marketplace instance, you must set up your JDeveloper environment before you can use it to deploy applications.

To set up JDeveloper for deploying to Oracle SOA Suite on Marketplace:

1. Refer to [Access an Oracle SOA Suite on Marketplace Instance](#) and make a note of the public IP address (or addresses in the case of a multinode cluster) associated with each SOA server.
2. Log in to the [WebLogic Server Administration Console](#).
3. On the Summary of Servers page, click each Managed Server name and make a note of the **Listen Address** value:

Be sure to capture the listen addresses for all Managed Servers.

4. On the host on which JDeveloper is running, map the listen address of each Managed Server to the associated SOA server public IP address in the `hosts` file. For Windows, the `hosts` file is typically located at `C:\Windows\System32\Drivers\etc\hosts`. For example:

```
129.146.136.141 sobdemo-wls-1.soacsp2pubsubne.soacsp2vcn.oraclevcn.com
158.101.23.141 sobdemo-wls-2.soacsp2pubsubne.soacsp2vcn.oraclevcn.com
129.146.136.141 sobdemo-wls-1
158.101.23.141 sobdemo-wls-2
```

5. Add the ingress rule to permit traffic from JDeveloper to the SSL listener port of the Managed Server:
  - a. [Sign in to the Oracle Cloud Infrastructure Console](#).
  - b. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
  - c. Select the compartment where you created the new instance.
  - d. In the list of VCNs, select your VCN.
  - e. On the Virtual Cloud Network Details page, click **Security Lists** in the left pane.
  - f. Select a security list, and click **Add Ingress Rules** to open the Add Ingress Rules dialog.
  - g. In the Add Ingress Rules dialog, create an ingress rule for port 9074 to access JDeveloper as shown in the following screenshot:

The screenshot shows the 'Add Ingress Rules' dialog box. At the top right is a 'Cancel' link. The main area is titled 'Ingress Rule 1' and contains the following fields:

- A green status indicator: 'Allows TCP traffic 9074'
- A 'STATELESS' checkbox with an information icon.
- 'SOURCE TYPE' dropdown menu set to 'CIDR'.
- 'SOURCE CIDR' text input field containing '129.159.24.56/32'. Below it, a note says 'Specified IP addresses: 129.159.24.56-129.159.24.56 (1 IP addresses)'.
- 'IP PROTOCOL' dropdown menu set to 'TCP'.
- 'SOURCE PORT RANGE' text input field set to 'All'. Below it, examples: '80, 20-22'.
- 'DESTINATION PORT RANGE' text input field set to '9074'. Below it, examples: '80, 20-22'.
- 'DESCRIPTION' text input field containing 'Allow traffic from JDeveloper CIDR'. Below it, a note: 'Maximum 255 characters'.

At the bottom right is a '+ Additional Ingress Rule' button. At the bottom left are 'Add Ingress Rules' and 'Cancel' buttons.

**Note:**

The source CIDR is the CIDR of the machine where JDeveloper is running.

- h. Add another ingress rule for port 9072, with the same source CIDR as port 9074.

**Important:**

By adding this ingress rule, be aware that you are allowing traffic from the internet (known CIDRs) into WebLogic Server. You must be extra cautious and open traffic to known CIDRs only.

**Next step:** [Create an application server connection.](#)

## Create an Application Server Connection in JDeveloper

To create a new application server connection in JDeveloper:

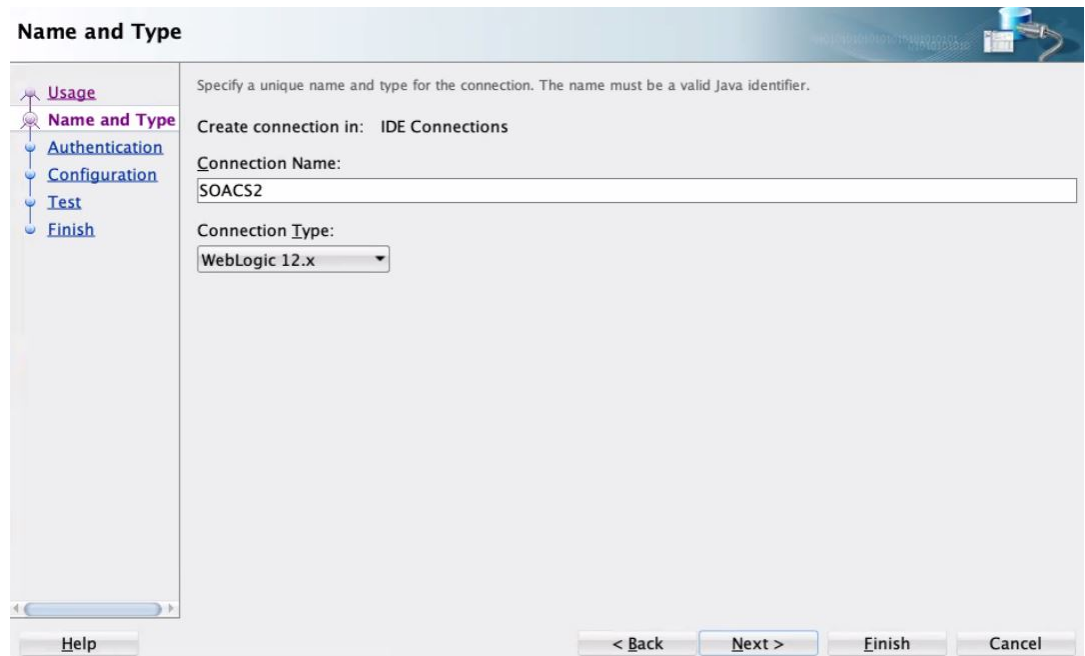
1. Before you test the connection, clear your JDeveloper cache:
  - a. In JDeveloper, click the **Help** menu and select **About**.
  - b. In the About dialog, on the Properties tab, find `ide.user.dir` and note its value, which is the name of the cache directory.
  - c. Back up the cache directory, then delete it.



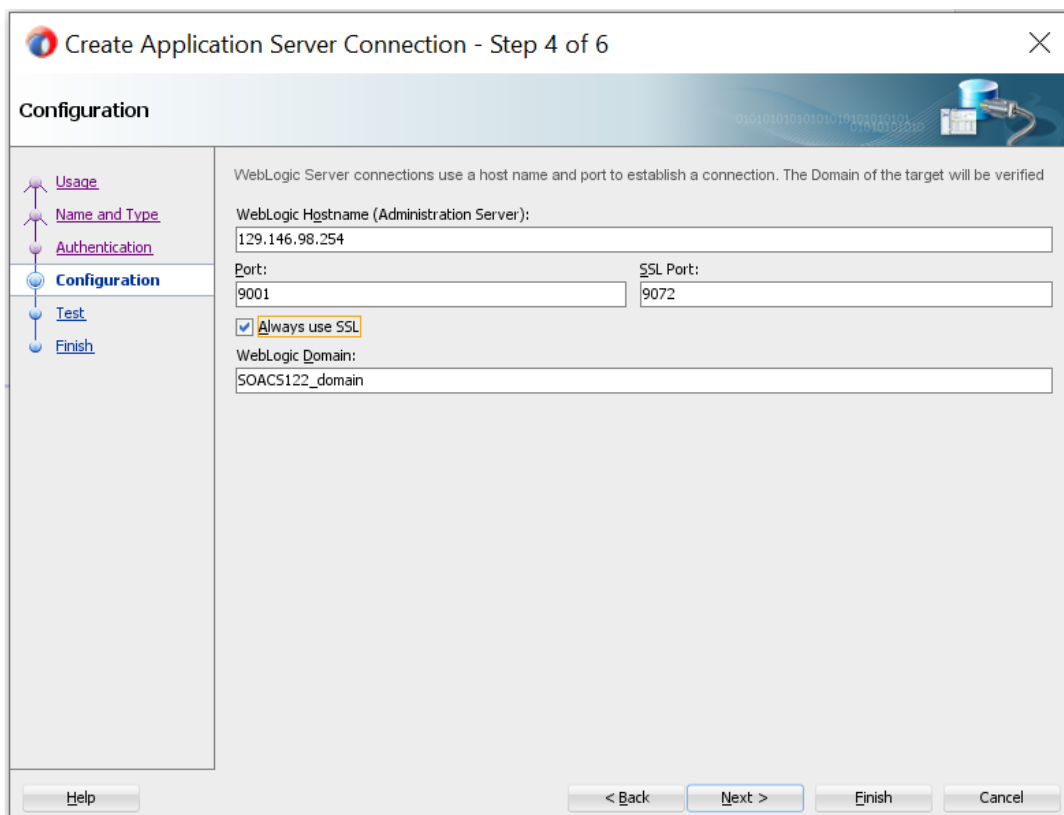
 **Note:**

All JDeveloper database connections and integrated WebLogic Server settings are lost when you delete the cache.

2. Restart JDeveloper.
3. On the Name and Type page, in the **Connection Name** field, enter a name for the connection, and select a **Connection Type** of **WebLogic 12.x**.



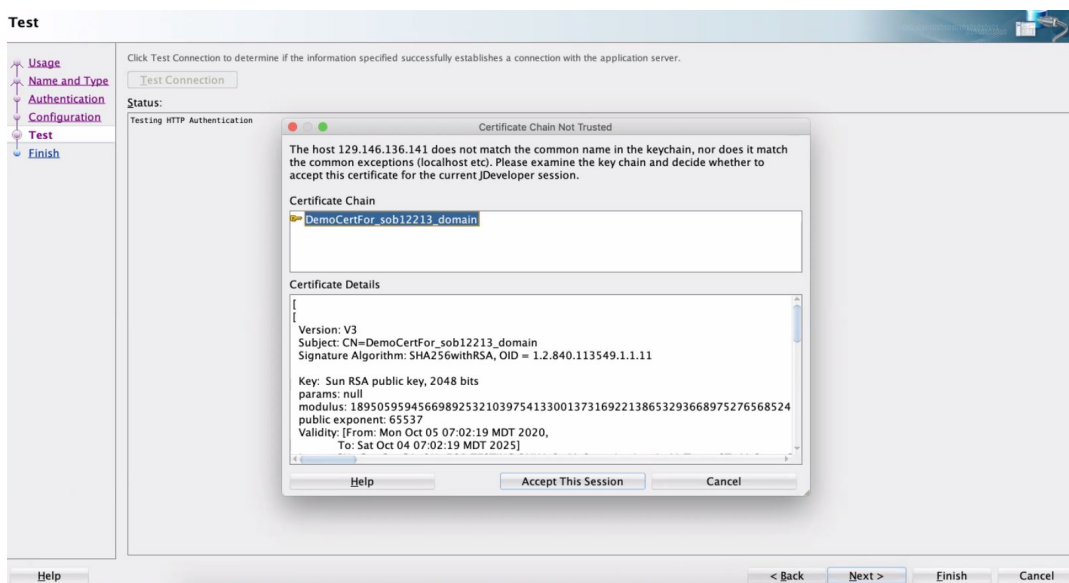
4. On the Authentication page, enter your WebLogic Server credentials.
5. On the Configuration page:
  - In the **WebLogic Hostname (Administration Server)** field, enter the public IP address of the Administration Server that you noted down for the provisioned Oracle SOA Suite on Marketplace instance.
  - Enter a **Port** value of 9001 and an **SSL port** value of 9072.
  - Select **Always use SSL** when the instance is using a public IP address. For instances with a private IP address only, leave this unchecked.
  - Enter the name of your **WebLogic Domain**.

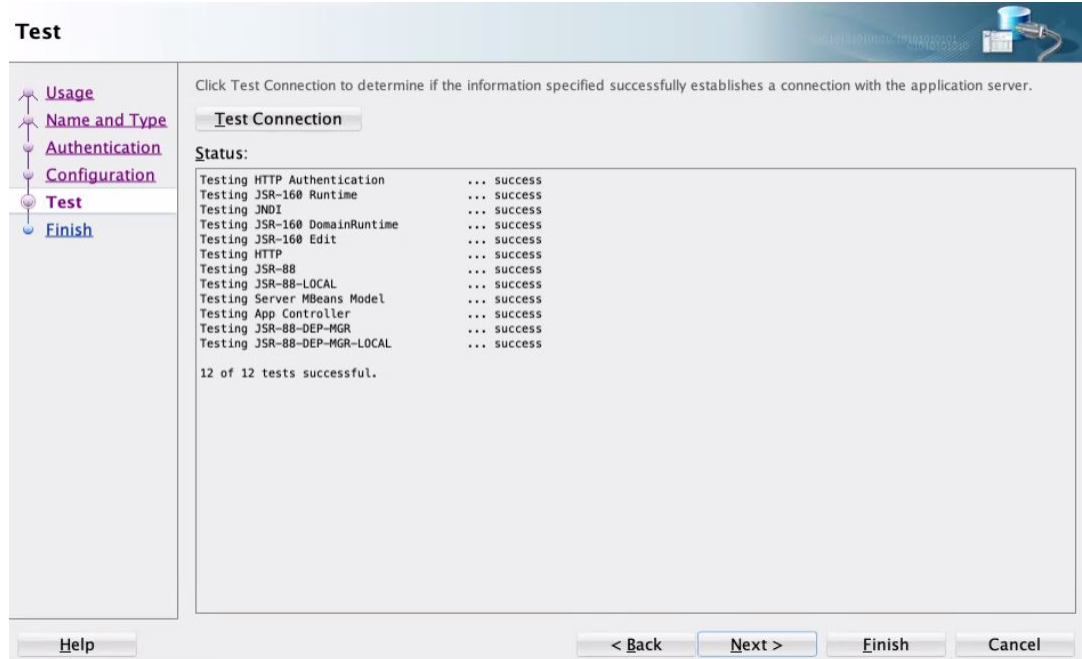


- 6. On the Test page, click **Test Connection**. If the instance is using a public IP address, then click **Accept This Session** to accept the certificates in the dialog that is displayed.

**Note:**

If the Certificate Chain Not Trusted dialog does not display, you must clear your JDeveloper cache as described in step 1 and try again.

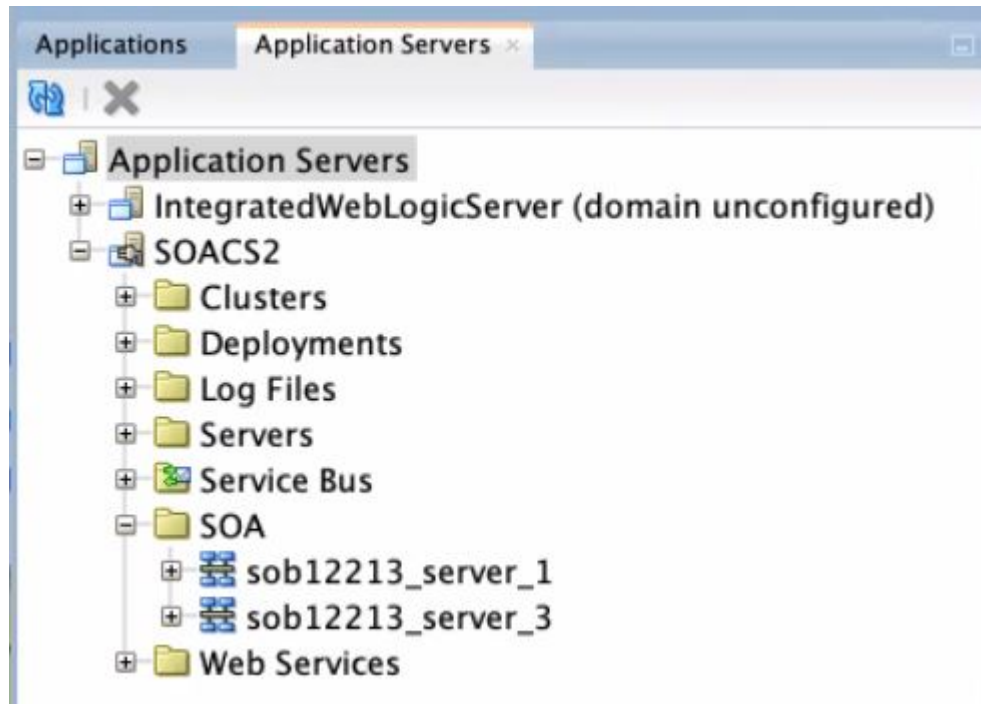




 **Notes:**

- If **Test Connection** has failures, then ensure that `/etc/hosts` has the required entries and ports 9072/9074 allow inbound traffic from the JDeveloper host.
- Do not proceed without accepting the certificates when using instances with a public IP address.

7. In JDeveloper, on the Application Servers tab, expand the connection name, then **SOA** (or **Service Bus**), and confirm that the names of the Managed Servers are listed, indicating that the connection is established from JDeveloper to the servers. If servers are not displayed, then check the `/etc/hosts` file has both host name and fully qualified domain name entries.



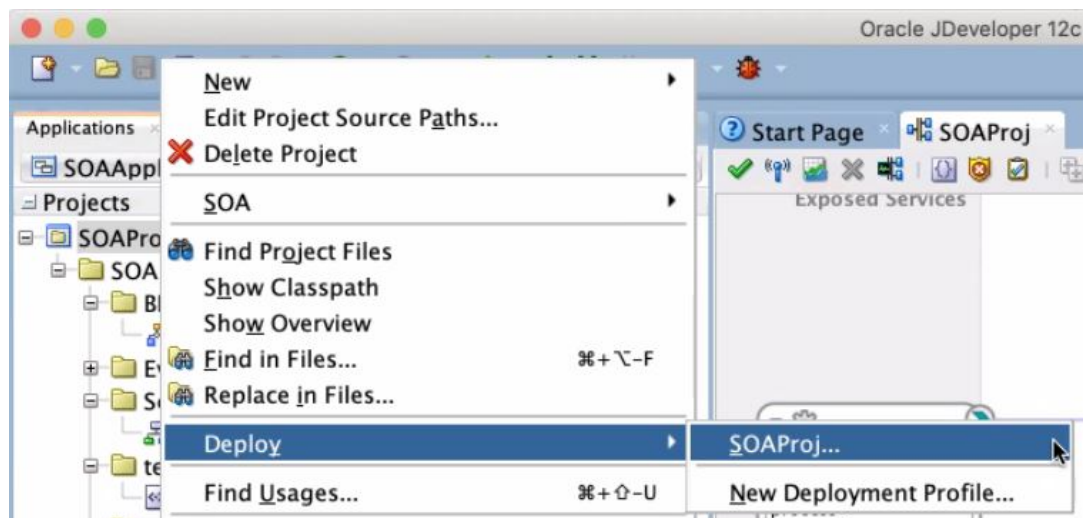
**Next step:** [Deploy a SOA composite application](#) or [Deploy an Oracle Service Bus application](#).

## Deploy a SOA Composite Application to Oracle SOA Suite on Marketplace from JDeveloper

SOA composite applications are deployed to Managed Servers.

To deploy a SOA composite application to Oracle SOA Suite on Marketplace from JDeveloper:

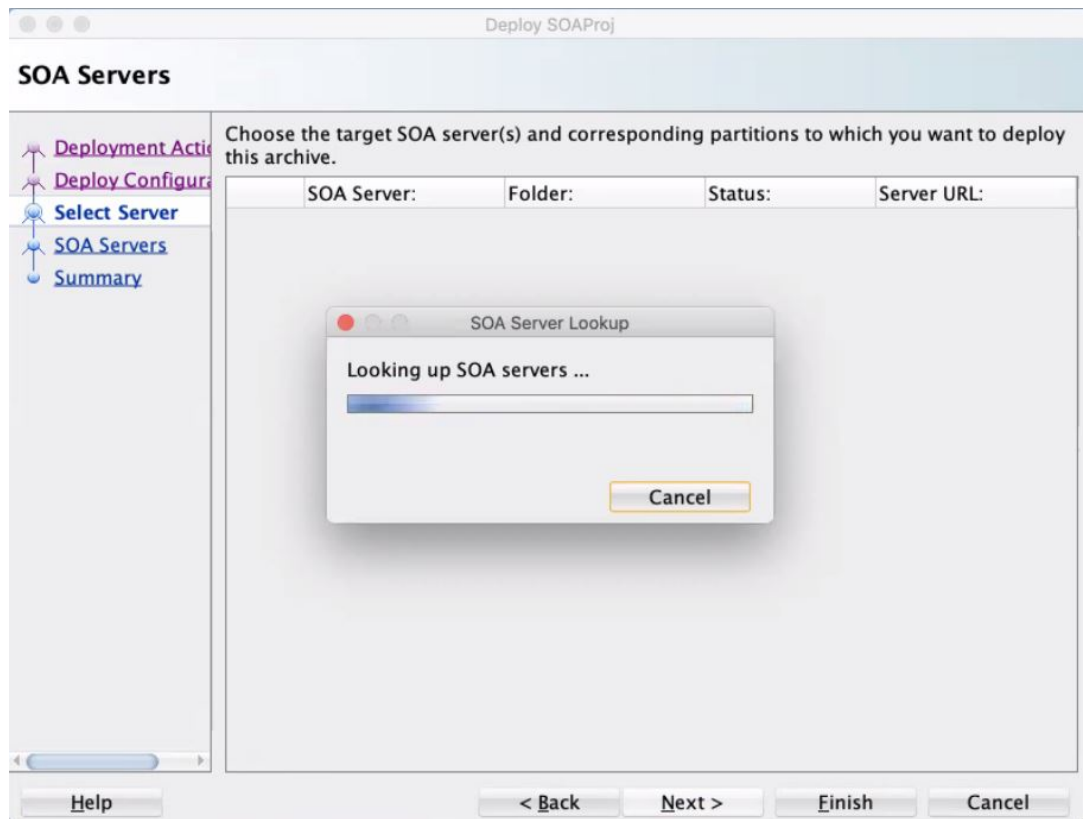
1. In JDeveloper, right-click the SOA project you want to deploy and select **Deploy**, then the name of the project.

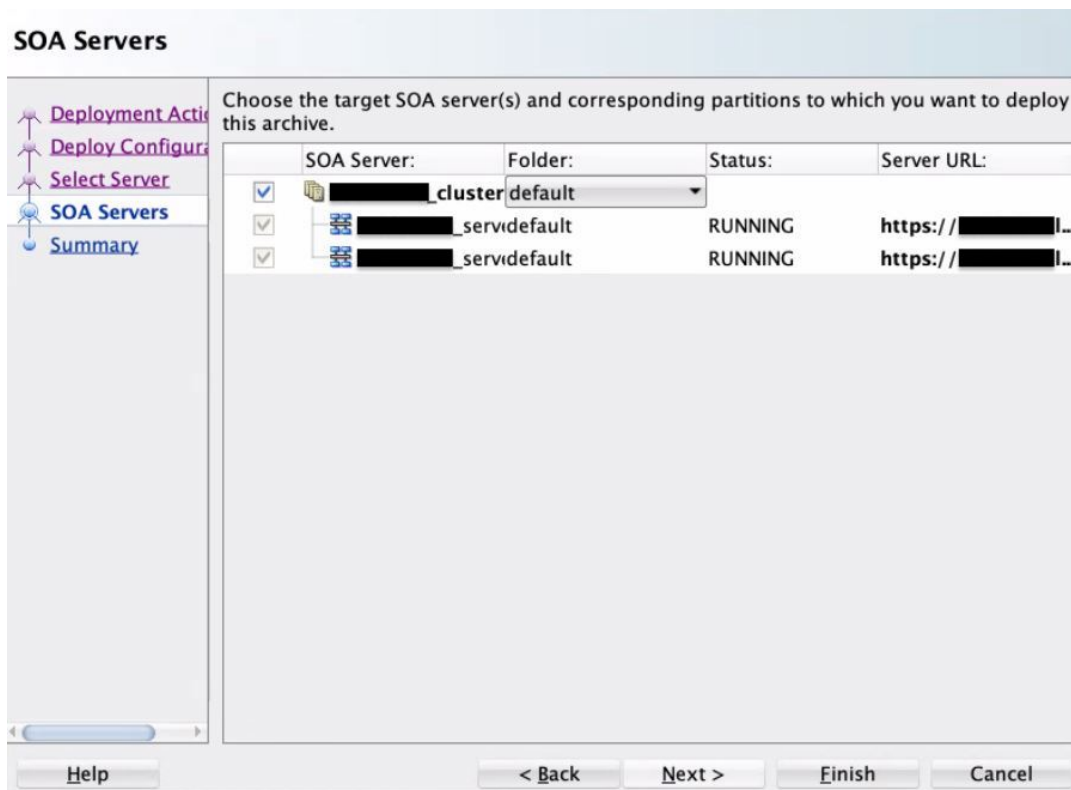


The deployment wizard is displayed.

2. On the Select Server page, select the application server connection that you created.

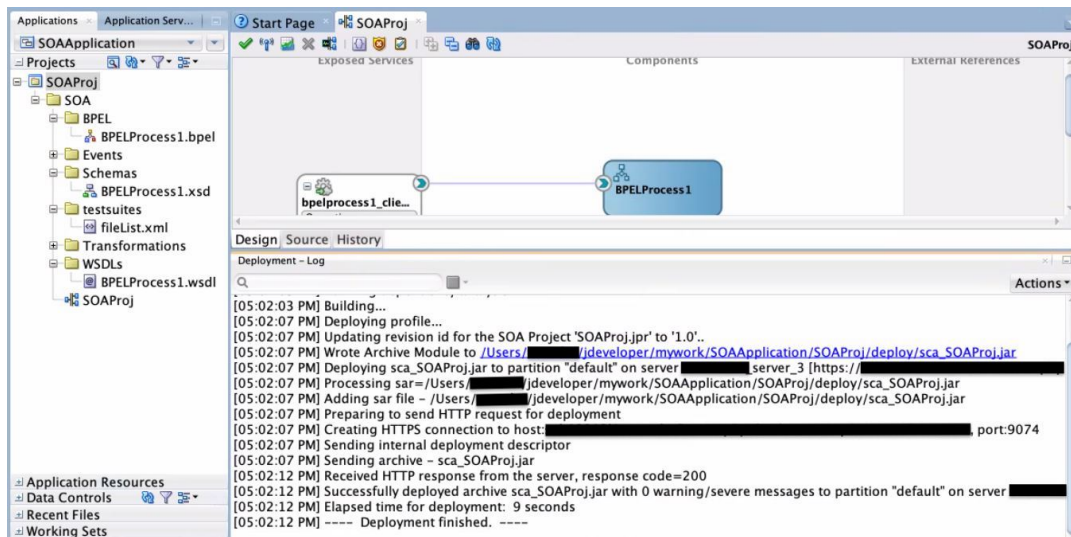
If the server is configured correctly, the deployment wizard looks up the SOA servers and shows the SOA servers to which to deploy the SOA composite application.





**Note:** If the SOA Server lookup has failures, then ensure that `/etc/hosts` has the required entries and ports 9072/9074 allow inbound traffic from the JDeveloper host.

3. Click **Finish** and verify that the deployment completes successfully as shown in the following screenshot.



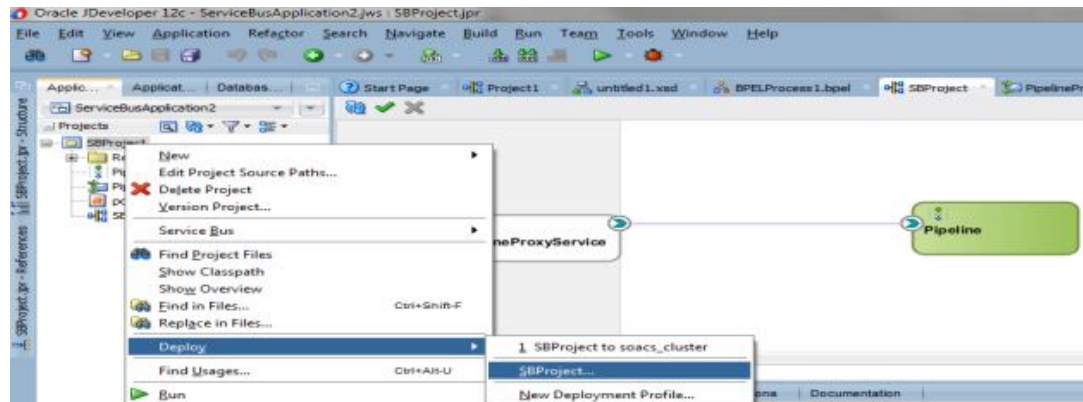
The JDeveloper Console logs indicate that the composite application was deployed successfully.

## Deploy an Oracle Service Bus Application to Oracle SOA Suite on Marketplace from JDeveloper

Oracle Service Bus applications are deployed to the Administration Server.

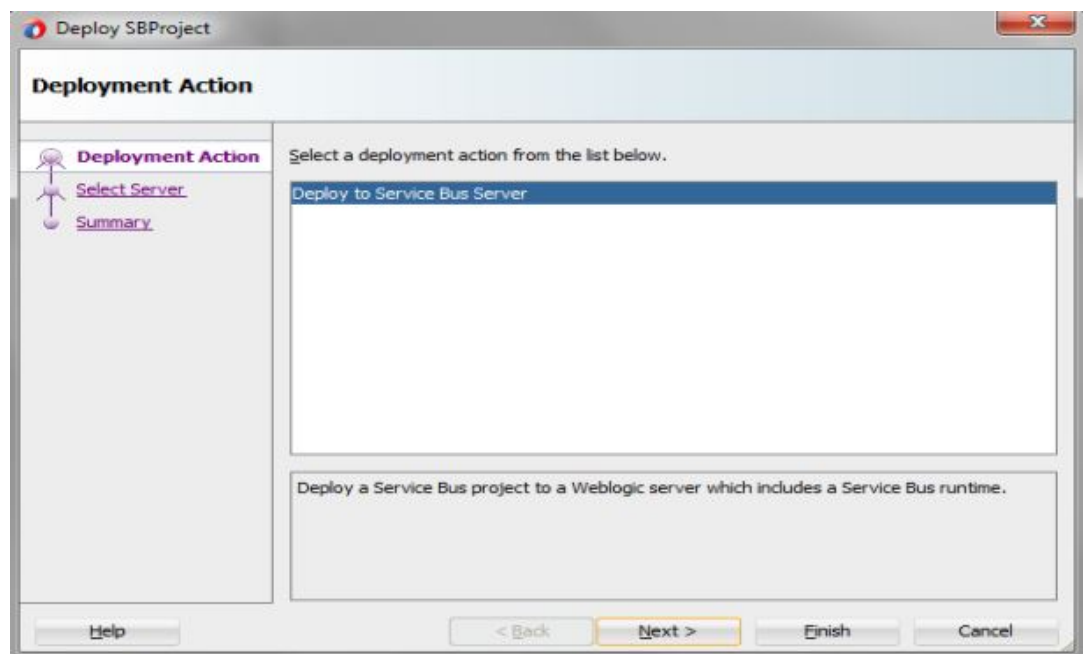
To deploy an Oracle Service Bus application to Oracle SOA Suite on Marketplace from JDeveloper:

1. In JDeveloper, right-click the Oracle Service Bus application you want to deploy and select **Deploy**, then the name of the application.

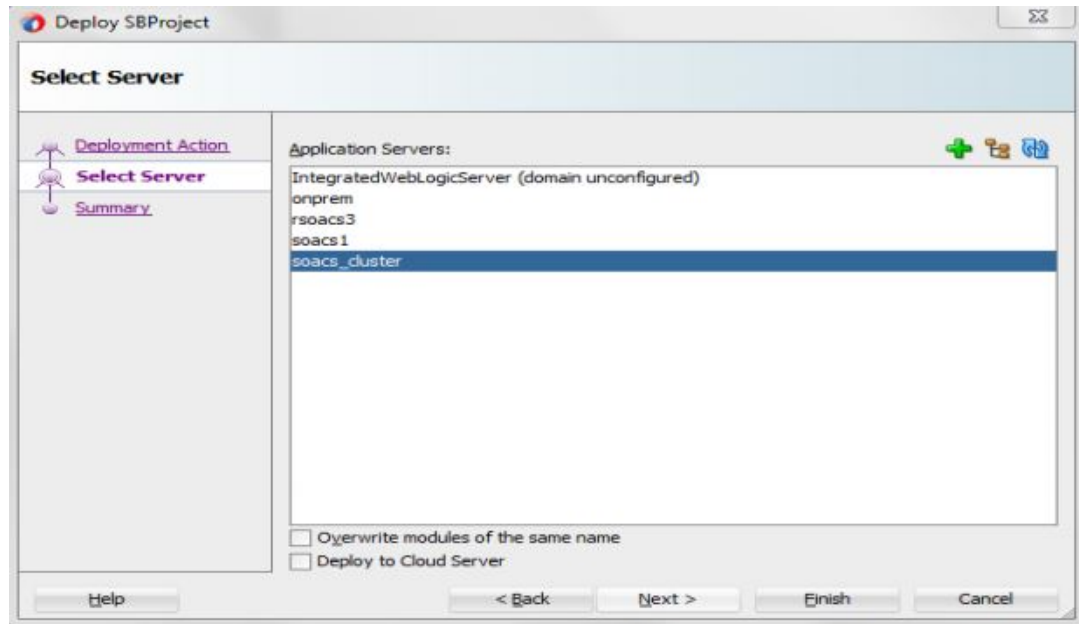


The deployment wizard is displayed.

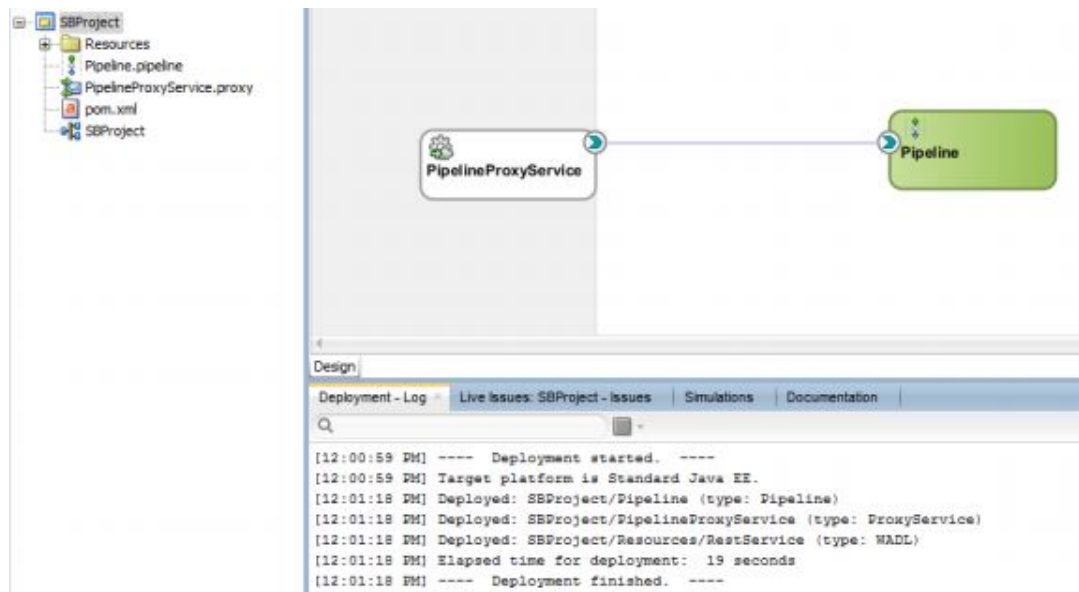
2. On the Deployment Action page, select **Deploy to Service Bus Server**.



3. On the Select Server page, select the application server connection that you created.



4. Click **Finish** and verify that the deployment completes successfully as shown in the following screenshot.



The JDeveloper Console logs indicate that the application was deployed successfully.



## Use Oracle Enterprise Manager Fusion Middleware Control to Deploy an Application

You can use Oracle Enterprise Manager Fusion Middleware Control to deploy and undeploy an application to an Oracle SOA Suite on Marketplace instance, just as you would deploy and undeploy the application to an on-premises service instance.

 **Note:**

Before you can use Oracle Enterprise Manager Fusion Middleware Control to deploy an application, you must add a managed server IP as described in [Add a Managed Server IP in a Non-Proxy Host to Enable Deployment from Fusion Middleware Control](#).

For additional resources, see [Deploying, Undeploying, and Redeploying SOA Composite Applications](#) in *Administering Oracle Fusion Middleware*.

## Use the WebLogic Server Administration Console to Deploy and Undeploy an Application

You can use the Oracle WebLogic Server Administration Console to deploy and undeploy an application to an Oracle SOA Suite on Marketplace instance, just as you would deploy and undeploy the application to an on-premises service instance.

**Topics:**

- [Use the WebLogic Server Administration Console to Start an Application](#)
- [Use the WebLogic Server Administration Console to Undeploy an Application](#)

## Use the WebLogic Server Administration Console to Start an Application

You must start the application to make it ready to accept requests.

To start an application:

1. Log in to the [WebLogic Server Administration Console](#).
2. In the Change Center, click **Lock & Edit**.
3. On Deployments table on the WebLogic Server Administration Console, select the application.
4. Click **Start**, then **Servicing all requests**.
5. On the Start Deployments dialog, click **Yes** to confirm the deployment.

The application is now in the **Active** state and is ready to accept requests.

## Use the WebLogic Server Administration Console to Undeploy an Application

You can use the WebLogic Server Administration Console to undeploy an application from an Oracle SOA Suite on Marketplace instance.

To undeploy the application:

1. Log in to the [WebLogic Server Administration Console](#).
2. In the Change Center, click **Lock & Edit**.
3. In the left pane of the WebLogic Server Administration Console, select **Deployments**.
4. In the right pane, select the check boxes next to the application you want to remove, and click **Delete**.
5. Click **Yes** to confirm your decision and remove the application.
6. To activate your changes, click **Activate Changes** in the Change Center of the WebLogic Server Administration Console.

## Use WLST Commands to Deploy and Undeploy an Application

You can use WLST commands to deploy and undeploy an application to and from an Oracle SOA Suite on Marketplace instance. All WLST commands are supported.

You can use a secure shell (SSH) to connect to the virtual machine (VM) that hosts the Administration Server and run WLST commands locally. For information, see [Create an SSH Tunnel](#). When running WLST commands locally on the VM, you can use WLST online and offline. You can only undeploy an application online. Alternatively, if you are not connected to the VM that hosts the Administration Server, you can connect to the Administration Server using WLST commands online and run WLST commands remotely (for example, from a command shell in your local environment). When running WLST commands remotely, you can use WLST commands for deployment and undeployment online only. For more information, see [Use WLST to Administer a Service Instance in \*Administering Oracle Java Cloud Service\*](#).

For additional information about using WLST commands, see:

- "Using WLST Online to Deploy Applications" in *Understanding the WebLogic Scripting Tool* (12.2.1.4)
- *WLST Command Reference for SOA Suite* (12.2.1.4)

## Access an Application Deployed to an Oracle SOA Cloud Service Instance

You can access an application deployed to an Oracle SOA Suite on Marketplace instance through a URL in a browser.

To access a deployed application:

1. Log in to the [Service Bus Console](#).
2. Copy the Host IP Address of the load balancer or Managed Server, depending on whether your Oracle SOA Suite on Marketplace instance has a load balancer.
3. Find the context-root of the application.

The context-root is defined in the service project as a project property, or in the `weblogic.xml` file. The context-root may or may not be the same as the internal application name.

- a. Log in to the [WebLogic Server Administration Console](#) and under **Domain Structure**, expand **Environment**, select **Clusters**, and select your SOA cluster.
  - b. Select **domain**, then **Deployments**, where **domain** is the domain where the application is deployed.
  - c. In the Deployments table, click on the name of your service.  
The Settings dialog is displayed.
  - d. In the Overview tab, locate the context-root.
4. Open a browser.
  5. In the address bar, specify the URL of the application:  

```
https://public_IP_of_load_balancer_or_managed_server:port/  
application_context_root
```

or

```
http://public_IP_of_load_balancer_or_managed_server:port/  
application_context_root
```
  - a. Paste the Host IP Address of the load balancer or Managed Server into the URL.
  - b. Specify the port number.
  - c. Specify the context-root for the application.  

If you do not want to specify the IP address and port when you access the application, you can create a custom URL. To do this, you must acquire and configure a third-party DNS provider to map the custom URL. See [Configure a Custom URL for an Application Deployed to a Service Instance in \*Administering Oracle Java Cloud Service\*](#).
  6. If you receive a warning, accept the signed certificate.  
The application opens in your browser.

## Use a Shared File System

By default, SOA Servers save adapter deployment plans on your local file system. Any changes made to adapter configuration generates a new deployment plan. In a multinode cluster, the deployment plan must be copied to all nodes of the cluster. To avoid this copy operation, you can save deployment plans in shared folders that are accessible to all nodes in a cluster. Similarly, it is recommended to use shared folders for other features such as File Adapter read/write. This can be achieved in either of the following ways:

- **Database File System (DBFS).** A standard Oracle SOA Suite or Managed File Transfer (MFT) instance in Oracle Public Cloud has the following DBFS-based shared file system mount points, configured by default during provisioning and scale out operations:

- /u01/soacs/dbfs
- /u01/soacs/dbfs\_directio

Store deployment configuration plans (and other shared files) in one or more DBFS folders to make them available across all nodes in a cluster.

 **Note:**

DBFS is not configured when using an ATP-S or ATP-D database. This option is available for other [supported databases](#).

- **File Storage Service (FSS)**. Can be used with Oracle SOA Suite only, not with Managed File Transfer (MFT). To use FSS, you must complete the following manual configuration tasks post-provisioning:
  1. [Sign in to the Oracle Cloud Infrastructure Console](#).
  2. (If not already done) Create File Storage Service (FSS):
    - a. Open the navigation menu and click **Storage**. Under **File Storage**, click **File Systems**.  
A list of the file systems in your tenancy is displayed.
    - b. Click **Create File System**.
    - c. In the Create File System dialog, click the File System Information **Edit Details** link, and enter a name for the file system.  
For example: `FileSystem-SOAShare`
  3. Configure security rules to allow network traffic to and from the mount target. You can set up security rules in subnet security lists, network security groups, or by using a combination of both.  
For more information, see [Overview of File Storage](#) in the Oracle Cloud Infrastructure documentation.
  4. Mount FSS on each node of the cluster and subsequently on newly added nodes after a scale out operation.  
For example:

```
sudo mkdir -p /mnt/FileSystem-SOAShare
sudo yum install nfs-utils
sudo mount -v 10.0.0.69:/FileSystem-SOAShare /mnt/FileSystem-SOAShare
sudo chmod 777 /mnt/FileSystem-SOAShare
```

To see the new mount point, enter: `df -h`

 **Note:**

Optionally, you can add an entry in `/etc/fstab` to mount FSS during node restarts. Enter the mount point entry for FSS using the following syntax:

```
FSmount_location mount_point nfs defaults,proto=tcp,port=2049
0 0
```

For example:

```
10.0.0.69:/FileSystem-SOAShare /mnt/FileSystem-SOAShare nfs
defaults,proto=tcp,port=2049 0 0
```

After configuring FSS mount points, store deployment configuration plans (and other shared files) in one or more FSS folders to make them available across all nodes in a cluster. FSS mounts are accessible across availability domains in an Oracle Cloud Infrastructure region.

## Access 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 Administration Console as described in [Access an Oracle SOA Suite on Marketplace 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 of the WebLogic Server Administration Console.

```
http://ws_console_IP_address/services/default/HelloWorld/  
helloworldprocess_client_ep?WSDL
```

For example:

```
http://12.251.267.111/services/default/HelloWorld/  
helloworldprocess_client_ep?WSDL
```

## Use the Frontend Host and HTTPS Port Values in the WSDL URL for Inbound Cloud Adapters

If you use the cloud adapters in the inbound direction, you must specify the frontend host and HTTPS port values found in the Oracle WebLogic Server Administration Console in your WSDL URL.

Use a WSDL URL of the following format:

```
https://frontend_hostname:frontend_HTTPS_port/integration/flowsvc/adapter/  
partition_name/composite_name/service_name/version?wsdl
```

For example:

```
https://host.mycompany.com:8080/integration/flowsvc/osc/default/oscinbound/  
OscService/v1.0/?wsdl
```

To obtain the frontend host and HTTP port values:

1. Log in to the [WebLogic Server Administration Console](#).
2. Expand **Environment**, then select **Clusters**.
3. Click the cluster name.
4. Click the **HTTP** tab.
5. Update the following values as shown in the table.

<b>Field</b>	<b>Value</b>
Frontend Host	The <i>admin_host</i>
Frontend HTTP Port	<i>HTTP_port</i> (typically, the default value is 80)
Frontend HTTPS Port	<i>HTTPS_port</i> (typically, default value is 443)

6. Restart the Administration Server and Managed Servers for the updated values to take effect. See [Stop or Start WebLogic Servers](#).

# 6

## Manage Oracle SOA Suite on Marketplace 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.

### Topics:

- [Edit an Oracle SOA Suite on Marketplace Instance](#)
- [Add or Delete a Load Balancer Post-Provisioning](#)
- [Access a VM Through a Secure Shell \(SSH\)](#)
- [Perform Lifecycle Operations on an Oracle SOA Suite on Marketplace Instance](#)
- [Perform Database Operations for an Oracle SOA Suite on Marketplace Instance](#)
- [Increase the Domain Volume Size Post-Provisioning](#)
- [Update the JVM Heap Size Parameter Values for Managed Servers](#)
- [Enable OS Management for Oracle SOA Suite on Marketplace Instances](#)
- [Perform a JNDI Lookup of JMS Resources Deployed on the Administration Server](#)

## Edit an Oracle SOA Suite on Marketplace Instance

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

To edit an Oracle SOA Suite on Marketplace instance:

1. Go to the Stack Details page of the instance you want to edit, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. On the Stack Details page, click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and edit any of the following editable fields as required:
  - **Compute Shape** (see [Scale an Oracle SOA Suite on Marketplace Instance Up or Down](#))
  - **Cluster Node Count** (see [Scale Out an Oracle SOA Suite on Marketplace Instance Cluster](#))
  - **Domain Volume Size (GB)** (see [Increase the Domain Volume Size Post-Provisioning](#))
  - **Use Network Security Group for SOA Instance**
  - **Provision Load Balancer** (see [Edit the stack to add a new load balancer](#))

- **Enable Backup/Restore configuration.** Configure the following fields, then refer to [Back Up the Domain Home](#) and [Restore the Domain Home](#):
  - **KMS Vault Compartment.** Select the compartment where you have the KMS vault.
  - **KMS Vault.** Select the OCID of the KMS vault used to encrypt the backup files.
  - **KMS Encryption Key.** Select the OCID of the KMS encryption key used to encrypt the backup files.
  - **Object Storage Bucket Name.** Enter the name of the object storage bucket used for storing the backup files.
- **Tags.** You can add, update, or delete the tags associated with the resources created as part of the Oracle SOA Suite on Marketplace instance stack.
  - **Tag namespace.** Select free-form or defined tags for the instance.
  - **Tag key.** Enter a tag key for the instance..
  - **Tag value.** Enter the value for the specified tag key.

See [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#) for field descriptions.

4. Click **Next** to navigate to the Review page, then click **Save Changes**.
5. On the Stack Details page, click **Terraform Actions** and select **Plan**. In the Plan dialog, click **Plan**.
6. When the Terraform Plan job completes successfully, click **Terraform Actions** and select **Apply**. In the Apply dialog, click **Apply**.

## Add or Delete a Load Balancer Post-Provisioning

If you did not enable a load balancer when provisioning your Oracle SOA Suite on Marketplace instance, you can optionally configure an existing load balancer or add a new load balancer at any time after provisioning. Subsequently, you can delete the load balancer.

The tasks of adding or deleting a load balancer post-provisioning are performed using the Oracle Cloud Infrastructure Console Resource Manager.

Guidelines for adding or deleting a load balancer in a SOA cluster:

- For a multinode cluster, it is recommended to always front-end nodes with a load balancer.
- SOA Servers must be in running state.
- When you configure an *existing* load balancer:
  - Do not add the load balancer using the Edit Stack option. Instead, follow the steps in [Configure an Existing Load Balancer for a Provisioned Instance](#).
  - Once the load balancer is configured, any subsequent scale out or scale in operations to the Oracle SOA Suite on Marketplace instance will NOT make necessary changes in the load balancer configuration. These changes include adjusting backend sets.
  - Any changes to the stack will NOT affect the load balancer accordingly. For example, deprovisioning the Oracle SOA Suite on Marketplace instance does not delete the load balancer.
- When you add a *new* load balancer:



- Once the load balancer is added, any subsequent scale out or scale in operations to the Oracle SOA Suite on Marketplace instance will make necessary changes in the load balancer configuration. These changes include adjusting backend sets.
- Any changes to the stack will affect the load balancer accordingly. For example:
  - \* Deprovisioning the Oracle SOA Suite on Marketplace instance deletes the load balancer.
  - \* Deselecting `PROVISION_LOAD_BALANCER` deletes the load balancer only.

The steps to add or delete a load balancer depend on whether you are using a new or existing subnet:

- [Configure an Existing Load Balancer for a Provisioned Instance](#)
- [Add a New Load Balancer in a New Subnet](#)
- [Add a New Load Balancer in an Existing Subnet](#)
- [Delete a Load Balancer When Added in a New Subnet](#)
- [Delete a Load Balancer When Added in an Existing Subnet](#)

## Configure an Existing Load Balancer for a Provisioned Instance

You can configure an existing Oracle Cloud Infrastructure load balancer for a provisioned Oracle SOA Suite on Marketplace instance.

### Usage Notes:

- You can configure only one Oracle Cloud Infrastructure load balancer for one Oracle SOA Suite on Marketplace instance.
- The Oracle Cloud Infrastructure load balancer has high availability (HA) features, spanned across different Availability Domains.
- If you have manually imported any certificates into SOA Servers, you must reimport these certificates into the load balancer.
- After completing the steps to configure the Oracle Cloud Infrastructure load balancer:
  - If you are not using a DNS name and using an IP address (see [Register a Custom Domain Name with a Third-Party Registration Vendor](#)), make sure your runtime URLs use the Oracle Cloud Infrastructure load balancer IP address instead of the SOA Server IP address.
  - URLs for all Managed Servers such as b2bconsole, mftconsole, and composer are accessible using the Oracle Cloud Infrastructure load balancer URL using https.
  - You must manually add or delete backends in the Oracle Cloud Infrastructure load balancer after scale out and scale in operations.
  - Deprovisioning of the Oracle SOA Suite on Marketplace instance will not delete the Oracle Cloud Infrastructure load balancer backend set and backend servers. You must manually delete the load balancer backend set and backend servers from the Oracle Cloud Infrastructure Console.

 **Note:**

This procedure uses the following example IP addresses:

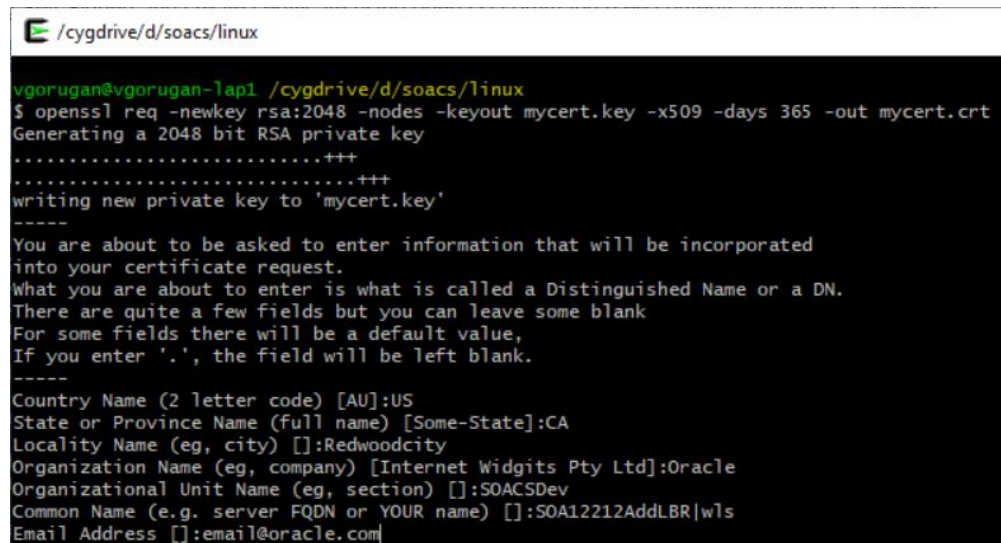
- WebLogic Server Public IP: 129.146.200.44
- Oracle Cloud Infrastructure load balancer Public IP: 129.146.91.95

To configure an existing Oracle Cloud Infrastructure load balancer for a provisioned Oracle SOA Suite on Marketplace instance:

1. As a prerequisite, it is assumed that the Oracle SOA Suite on Marketplace instance is already provisioned without a load balancer.
2. **Create the MyCert certificate.** This is a self-signed certificate and uses a private key that you generate. It is used for external clients to connect to the Oracle Cloud Infrastructure load balancer using port 443.
  - a. As the `oracle` user, run the following command to generate the self-signed certificate:

```
openssl req -newkey rsa:2048 -nodes -keyout mycert.key -x509 -days 365 -out mycert.crt
```

- b. Provide requested input as shown in the following screenshot:



```
/cygdrive/d/soacs/linux
vgorugan@vgorugan-lap1 /cygdrive/d/soacs/linux
$ openssl req -newkey rsa:2048 -nodes -keyout mycert.key -x509 -days 365 -out mycert.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'mycert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:Redwoodcity
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Oracle
Organizational Unit Name (eg, section) []:SOACSDev
Common Name (e.g. server FQDN or YOUR name) []:SOA12212AddLBR|wls
Email Address []:email@oracle.com
```

- c. Save the output to your local drive as `mycert.key`.

```

E /cygdrive/d/soacs/linux
vgorugan@vgorugan-lap1 /cygdrive/d/soacs/linux
$ cat mycert.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBkwwgS1AgEAAoIBAQL7Tch3kGRQ7cI
oon2zGdNhU+PVBBA28ynUfGp3oF/FNNKL1aXNdhT1T71AqMBjN4gk01Ybb/DYrWs
sxZ2o2Gcz1QcVetZ2WgHUWjbStTiqE3sR8R1nQMVFLLBYpa/25no1iJrpsPQoX3h
NnBWA+gu/5c4R5J+Uoyh1How2xVu0wS9E3Nn19Sz+L14sCSD11G593VyF+tbwvTF
uDykPVeIFZ8oiOIQWij0aMoiJnbZ01pKptGgXBN5rS2cFeasoKERd3+nQYhxumij
KSBobf1GcXbvvgBwO2Uzthv7H5ZQgUrf1/+XU+ItD31UU4jDU8CwtG5PUKwbydM
NMwc9WnXAgMBAAECggEAAxMEbcJIASekcbBhbl3K7gCwphZFjr80nPVtw/34gm
N0wXZhgtrXUS0eNRyy2HI+StP6SkYN/cacRg6Ba7F4/711tOuGIK/QYghXSt8gJ
xLIgSBWh4kN51RuHYkURQO1Zf334HcERGL+tWd6dNXgs83BAyR69eAIBQ8wd4Tt
UwEom+IbEW1j5cULr7d9wpcE2ILs41JDOYFv1j20j61/Iz6VVC5zogTiwK9IFS39
b0vk0jN5JBiKJ9ZOf2uMMMa/BbDtze5a7oDd9ghyEScfk0Us9Qu2DYswLV9UZIE61
tv3pBApSfe19etqDw24qfjwZ3x0okKwcvC8rVw04QKBgQD/IZeyRV0zK5xtvC9p
fDn5i01DzdpBaLIwZ6FEGQSVuNrkt0afv0EFpQLPgMBtbegTSjnaf3yXMCKiqw
+40YEb47MRmdXe+TD/GTWm7ekCqFZhmK7GQjVXdfGXnpwMvE6aDUZHBPFHKjzQC
v31Jsq1EXHy1exj59euV47UyOwKBgQDMnvxfCIt8WJDUnj0oLSKy2XmgqXt9D0U5
i38Fk5BAs55d5AcD57hsvImcyikJRvgN1lp3Di6UBto77ivmeab7cPiK03KsJmgm
MdgUE5dvSSSOC06BGP8ufqt1R+wCpIr+WWFZ1BeYmh89akMR4Zz+/zu70RWFs3wq
ZGm/hsExFQKBgQDjHx6SPxm3Ae3h6pMyjrp1okMIR2syq2d1nAFHnIFPI7aU/1dE
2SjInv4nPcEbw8Lo1ZEszp7HAXj2x1726xC9AZ6dxoMc6FhA+KE0Q695w1TcA8H
d9is3IVCBQoa7RzyfCQRX9BzNbrQgyFhb8FKp1xE/yY+prDet9csjeOHQKBgQCe
AmeAi7gq3X15tnDNFY097xITLrNdb11VgpMkCz9ptWjIuD1y1o2j6j0aD8KA130V
gbsqFJmDVYdQoCrmXyrDIAnNq1ry9PWYCWc+14FYcYIqH0E0/i6PrbIajGmGmN8
f6jdM67E+L8G/fes5zwE7bOC5YJ88B2B3uikLdUhwQKBgQDknRfNN16a5QPDoSet
ytwd4Y3ZAimw7ZZtgwKm2/+N8dwYDxd10vhtFSZz03VYRhl8F7nze9CtCqPfx7F
UVomFkKW43w1nGdQ+FeKF9nqaByInR+6s+Mb7pAxxox9aJQ2e/0effY4qToBNWvE
K708IGoeVQS6IQXnzP2X2kHvdA==
-----END PRIVATE KEY-----

```

3. In the **Oracle Cloud Infrastructure Console**, edit the existing load balancer.
  - a. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
  - b. In the left pane, click **Load Balancers**.
  - c. Scroll down in the left pane and select the compartment where the load balancer exists.
  - d. Click the name of the existing load balancer you want to configure.
  - e. In the left pane of the Load Balancer Details screen, click **Backend Sets**, then click **Create Backend Set**.
  - f. In the Create Backend Set dialog, enter the following information:
    - **Name:** httpBackend
    - **Port:** 9073
    - **Status Code:** 404
  - g. Click **Create Backend Set**.
4. On the Load Balancer Details screen, note that the **Overall Health** and **Backend Sets Health** shows a status of **Unknown**. To resolve this, continue with the steps below.

**5. Add backends.**

- a. In the left pane of the Load Balancer Details screen, click **Backend Sets**, then click the link to the `httpBackend` backend set.
- b. In the left pane of the Backend Set Details screen, click **Backends**, then click **Add Backends**.
- c. In the Add Backends dialog, click **Change Compartment** to select the compartment for your Oracle SOA Suite on Marketplace instance if not already displayed, then select the check box next to the instance name, and enter a **Port** value of 9073.

**Add Backends** [Help](#)

Choose how to add backend servers by selecting Compute instances or by entering IP addresses.

COMPUTE INSTANCES  IP ADDRESSES

Specify the Compute instances to include in your set of backend servers.

INSTANCES IN MOCKMANAGEDCOMPARTMENTSOA [\[CHANGE COMPARTMENT\]](#)

<input type="checkbox"/>	Name	IP Address	OCID	Availability Domain	Port	Weight
<input type="checkbox"/>	500104469 dbaas dbaasOCi0308 db_1 vm-1	10.0.0.48	...s4eklq <a href="#">Show</a> <a href="#">Copy</a>	bcaH.PHX-AD-1	80	1
<input checked="" type="checkbox"/>	SOA SOA12214AddLBRVG wis vm-1	10.0.0.150	...7swr2a <a href="#">Show</a> <a href="#">Copy</a>	bcaH.PHX-AD-1	9073	1
<input type="checkbox"/>	SOA SOA12214AddLBRVG wis vm-2	10.0.0.152	...ynmpha <a href="#">Show</a> <a href="#">Copy</a>	bcaH.PHX-AD-1	80	1
<input type="checkbox"/>	SOA SOA12214AtpStress10 lb vm-1	10.0.0.147	...s3pdvq <a href="#">Show</a> <a href="#">Copy</a>	bcaH.PHX-AD-1	80	1

**Note:**

If you have a multinode cluster, then choose all the instances in the cluster and enter the same **Port** value of 9073.

Scroll down to view the security list rules that will be created.

**AUTOMATICALLY ADD SECURITY LIST RULES**

Select a security list for each load balancer subnet, and then check the egress security rules you want to apply.

Security List	Subnet	Egress Rules (Allow Sending Traffic To)
Default Security List for testvcn	Public Subnet bcaH:PHX-AD-1	<input checked="" type="checkbox"/> SUBNET: 10.0.0.0/24 PORT: 9073
Default Security List for testvcn	Public Subnet bcaH:PHX-AD-2	<input checked="" type="checkbox"/> SUBNET: 10.0.0.0/24 PORT: 9073

Showing 2 Items

Select a security list for each load balancer subnet, and then check the ingress security rules you want to apply.

Security List	Subnet	Ingress Rules (Allow Receiving Traffic From)
Default Security List for testvcn	Public Subnet bcaH:PHX-AD-1	<input checked="" type="checkbox"/> SUBNET: 10.0.0.0/24 TO PORT: 9073 <input checked="" type="checkbox"/> SUBNET: 10.0.1.0/24 TO PORT: 9073

Showing 1 Item

**Add** [Cancel](#)

- d. Click **Add**.
6. **Add a rule set.**
    - a. In the left pane of the Load Balancer Details screen, click **Rule Sets**, then click **Create Rule Set**.
    - b. In the Create Rule Set dialog, enter a name for the rule set, then select **Specify Request Header Rules** and enter the following information:
      - **Name:** SSLHeader.
      - **Action:** Select **Add Request Header**.
      - **Header:** Enter WL-Proxy-SSL.
      - **Value:** Enter true.

**Create Rule Set** [Help](#)

Specify the rules that control traffic flow through the listener.

NAME  
SSLHeader

SPECIFY ACCESS CONTROL RULES  
 SPECIFY ACCESS METHOD RULES  
 SPECIFY URL REDIRECT RULES  
 SPECIFY REQUEST HEADER RULES


**Request Header Rules**

ORDER	ACTION	HEADER	VALUE
↑ ↓	Add Request Header	WL-Proxy-SSL	true

[+ Another Request Header Rule](#)

SPECIFY RESPONSE HEADER RULES

- c. Click **Create**.
7. **Add a listener.**

- a. In the left pane of the Load Balancer Details screen, click **Listeners**, then click **Create Listener**.
  - b. In the **Create Listener** dialog, enter the following information:
    - **Name:** `httpsListener`.
    - **Protocol:** HTTP.
    - **Port:** 443.
    - **Status Code:** 404.
    - Select **Use SSL**.
    - **Certificate Name:** `mycert.crt`.
    - **Backend Set:** Enter the name of the backend set (`httpBackend`) you created in Step 3.
  - c. Click **Create Listener**.
- 8. Edit the listener.**
- a. In the left pane of the Load Balancer Details screen, click **Listeners**, then click the  icon at the far right of the row for the listener you created, and select **Edit**.
  - b. In the Edit Listener dialog, select the rule set you created.

**Edit Listener** [Help](#)

To allow your load balancer to accept ingress traffic, specify the protocol and port for your public IP address.

NAME  
httpsListener

There are no hostnames for this load balancer. [Create a hostname.](#)

PROTOCOL: HTTP | PORT: 443 | USE SSL:

CERTIFICATE NAME: cert\_lb\_2020-0501-1654 | VERIFY PEER CERTIFICATE:

BACKEND SET: httpBackend

IDLE TIMEOUT IN SECONDS (OPTIONAL): 60  
The default timeout for HTTP is 60 seconds.


There are no path route sets for this load balancer. [Create a path route set.](#)

ORDER	RULE SET
↑ ↓	SSLHeader

There are no more rule sets associated with this load balancer.

[+ Additional Rule Set](#)

**Save Changes** **Cancel**

- c. Click **Save Changes**.
- 9. Update session persistence for the backend set.**
- a. In the left pane of the Load Balancer Details screen, click **Backend Sets**, then click the  icon at the far right of the row for the `httpBackend` backend set you created, and select **Edit**.

- b. In the Edit Backend Set dialog, select **Enable application cookie persistence**.
- c. In the **Cookie Name** field, enter `*`.

- d. Click **Update Backend Set**.
10. **Import required certificates into the Oracle Cloud Infrastructure load balancer.** If there are any inbound requests to Oracle SOA Suite on Marketplace that require you to import SSL certificates into the Oracle Cloud Infrastructure load balancer, import them now.
  11. **Update front end hosts.**

You can update front end hosts using an automation script or perform the steps manually:  
To update front end hosts using an automation script:

- a. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@VM_IP_address
```

- b. Change to the `oracle` user:

```
sudo su - oracle
```

- c. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

- d. Run the script to update front end hosts and respond to the prompts for WebLogic Server administration password, load balancer IP address, and load balancer port:

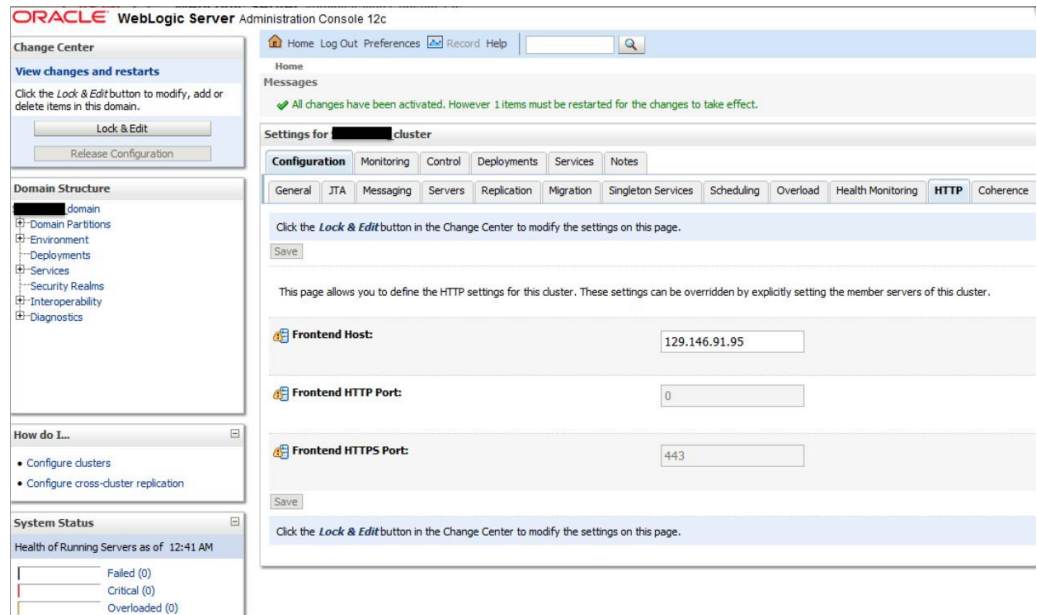
```
./updateFrontEndHostPort.sh
```

To update front end hosts manually:

- a. Log in to the [WebLogic Server Administration Console](#).
- b. Set the **Frontend Host** to the DNS server name. If the DNS server is not configured, then enter the IP address of the Oracle Cloud Infrastructure load balancer.

DNS (domain name system) translates host and domain names into the corresponding numeric Internet Protocol (IP) addresses, and also identifies and locates resources on the Internet.

- c. Set **Frontend HTTP Port** to `0`.



## 12. Enable the WebLogic Plug-In at the cluster level.

You can enable the WebLogic Plug-In in a cluster using an automation script or perform the steps manually:

To enable the WebLogic Plug-In using an automation script:

- a. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@VM_IP_address
```

- b. Change to the `oracle` user:

```
sudo su - oracle
```

- c. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

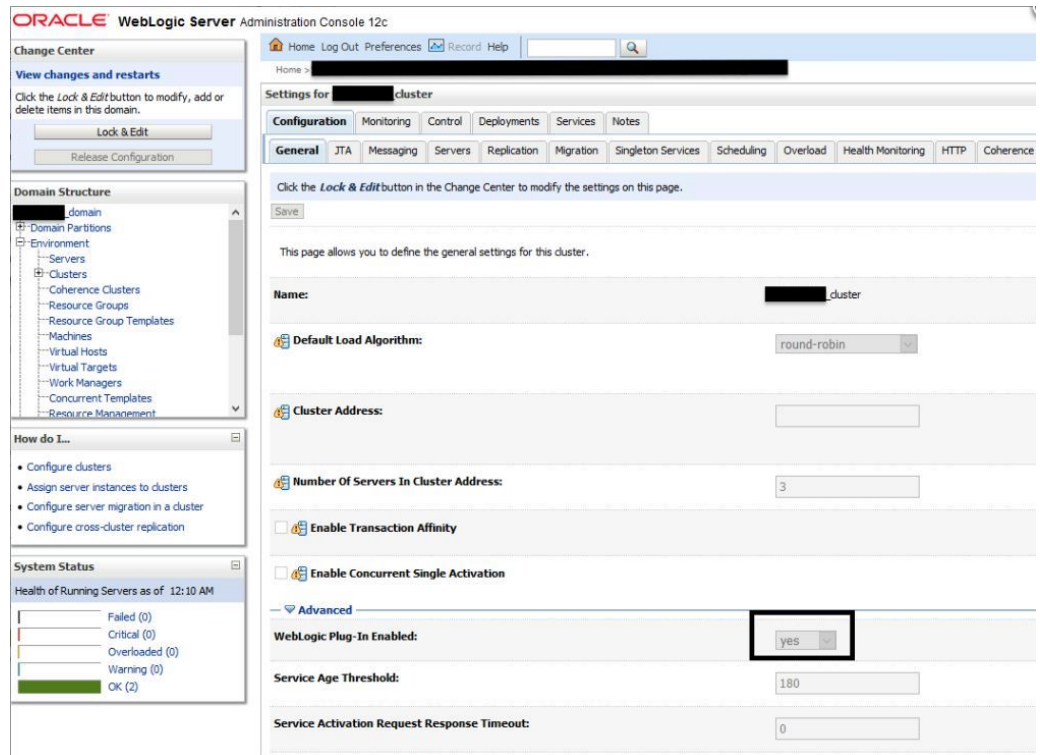
- d. Run the script to enable the WebLogic Plug-In:

```
./enableWeblogicPlugin.sh
```

To enable the WebLogic Plug-In manually:

- a. Log in to the [WebLogic Server Administration Console](#).
- b. In the **Domain Structure** pane, expand the **Environment** node, then **Clusters**, and click the cluster name.
- c. On the **Configuration: General** tab, scroll down to the **Advanced** section and expand it.
- d. Click **Lock & Edit**, then set **WebLogic Plug-In Enabled** to **Yes**.





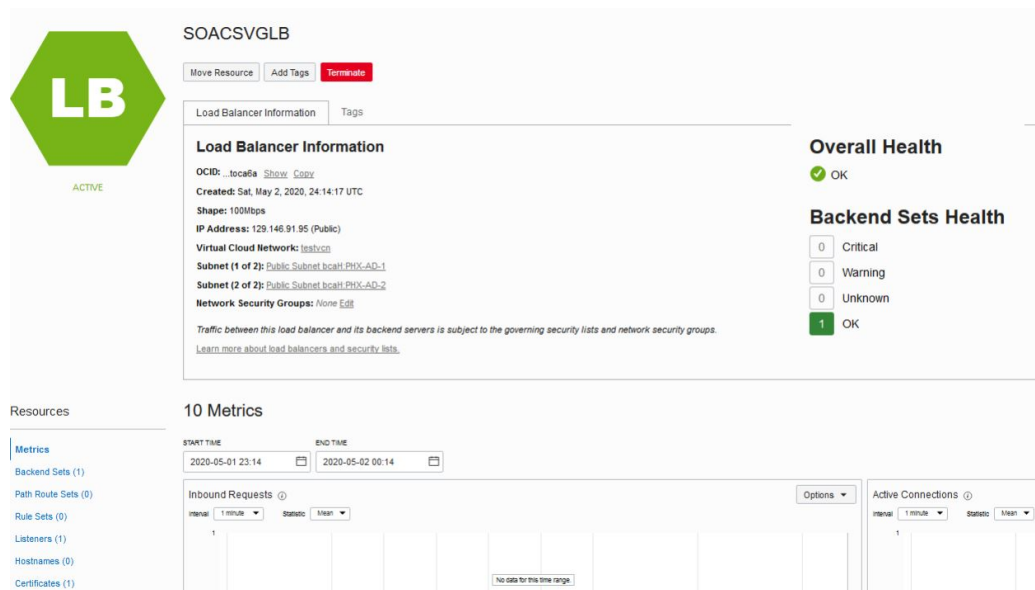
e. Click **Save**, then click **Activate Changes**.

**13. Restart the servers.**

Restart the Administration Server and Managed Servers. See [Stop or Start WebLogic Servers](#).

**14. Verify your configuration.**

- Verify the health of the Oracle Cloud Infrastructure load balancer: the **Overall Health** and **Backend Sets Health** should show a status of **OK**.



- Verify the URLs: you should be able to access the following Managed Server URLs using the Oracle Cloud Infrastructure load balancer IP address (for example, 129.146.91.95).
  - <https://129.146.91.95/soa/composer>
  - <https://129.146.91.95/mftconsole>
  - <https://129.146.91.95/b2bconsole>

### Troubleshooting Tips

If any steps in the configuration are missed or incorrectly implemented, the Oracle Cloud Infrastructure load balancer will not generate any error messages to alert you to issues. You can navigate to Oracle Cloud Infrastructure load balancer work requests and make sure the work requests have succeeded to confirm that the load balancer is working.

Use the following checklist to troubleshoot an Oracle Cloud Infrastructure load balancer that is not in Ready state:

- In the Oracle Cloud Infrastructure Console, verify:
  - Healthcheck: port number is 9073 and status code is 404.
  - Https Listener: listen port is 443.
  - Security lists has rule defined with 0.0.0.0/0 for 443. See [Configure Security Lists](#).
  - Backends are configured to use port 9073.
  - The `WL-Proxy-SSL` header is added to `httpslistener`.
- In the WebLogic Server Administration Console, verify:
  - `Frontendhost` and `port` are configured for the cluster.
  - The WebLogic Plug-In is enabled.

## Add a New Load Balancer in a New Subnet

Follow these steps to add a load balancer if the `SUBNET STRATEGY` was set to **Create New Subnet** during provisioning of the Oracle SOA Suite on Marketplace instance.

To add a load balancer in a new subnet:

- [Identify and remove the Managed Server security list from the subnet](#)
- [Edit the stack to add a new load balancer](#)
- [Execute the Terraform Plan operation](#)
- [Execute the Terraform Apply operation](#)
- [Get the load balancer details and validate results](#)
- [Update the load balancer console URL in the WebLogic Server Administration Console](#)
- [Restart the servers](#)

### Remove the Managed Server security list from the subnet

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Select the VCN for the instance.

- On the Virtual Cloud Network Details page, select the subnet for the instance.
- On the Subnet Details page, locate the security list for the instance.

ORACLE Cloud

Networking » Virtual Cloud Networks » soa\_examples\_vcn » Subnet Details

### SOALBR-wls-subnet

[Edit](#)
[Move Resource](#)
[Add Tags](#)
[Terminate](#)

Subnet Information | Tags

OCID: [\\_y6pxeq](#) [Show](#) [Copy](#)
Compartment: SOACSDev  
 CIDR Block: 10.0.6.0/24
 DNS Domain Name: subpub  
 Virtual Router Mac Address: 00:00:17:2D:18:B0
 Subnet Access: Public Subn  
 Subnet Type: Regional
 DHCP Options: [SOALBR-dh](#)  
Route Table: [SOALBR-route](#)

Resources

Security Lists (3)


Tag Filters [add](#) | [clear](#)

*no tag filters applied*

#### Security Lists

[Add Security List](#)

Name	State	Compartment
<a href="#">SOALBR-wls-ms-security-list</a>	Available	SOACSDev
<a href="#">SOALBR-wls-security-list</a>	Available	SOACSDev
<a href="#">SOALBR-internal-security-list</a>	Available	SOACSDev

- At the far right of the row for the security list, click  and select **Remove**, then click **Remove** in the Remove Security List From Subnet dialog.

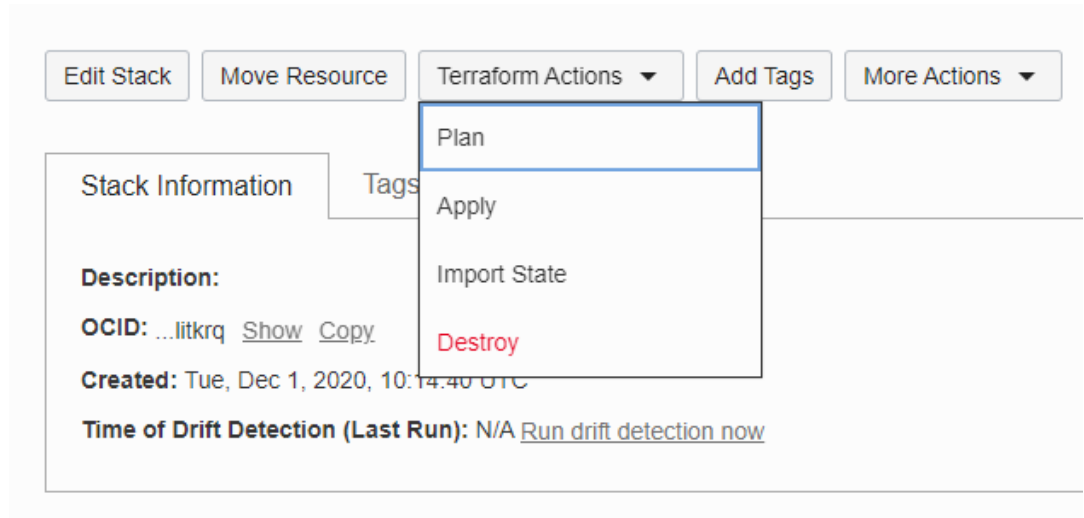
#### Edit the stack to add a new load balancer

- Go to the Stack Details page of the instance to which you want to add a load balancer, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
- On the Stack Details page, click **Edit Stack**.
- In the Edit Stack wizard, click **Next** to go to **Configure Variables** and select the **Provision Load Balancer** check box, then select the required **Load Balancer Shape**.
- Click **Next** to navigate to the Review page, then click **Save Changes**.

#### Execute the Terraform Plan operation

- Go to the Stack Details page of the instance, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).

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



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

### Execute the Terraform Apply operation

The Terraform Apply operation creates a new load balancer, along with the associated resources such as a listener, backend sets, and so on.

1. When the Terraform Plan job completes successfully, click **Terraform Actions** and select **Apply**.
2. In the Apply dialog, click **Apply**.

### Get the load balancer details and validate results

After the Terraform Apply operation completes successfully, view the log:

1. Go to the Stack Details page of the instance to which you want to add a load balancer, as described in [View Oracle SOA Suite on Marketplace 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 log.
4. Make a note of the load balancer URL and newly updated service console URLs at the end of the log. For example:

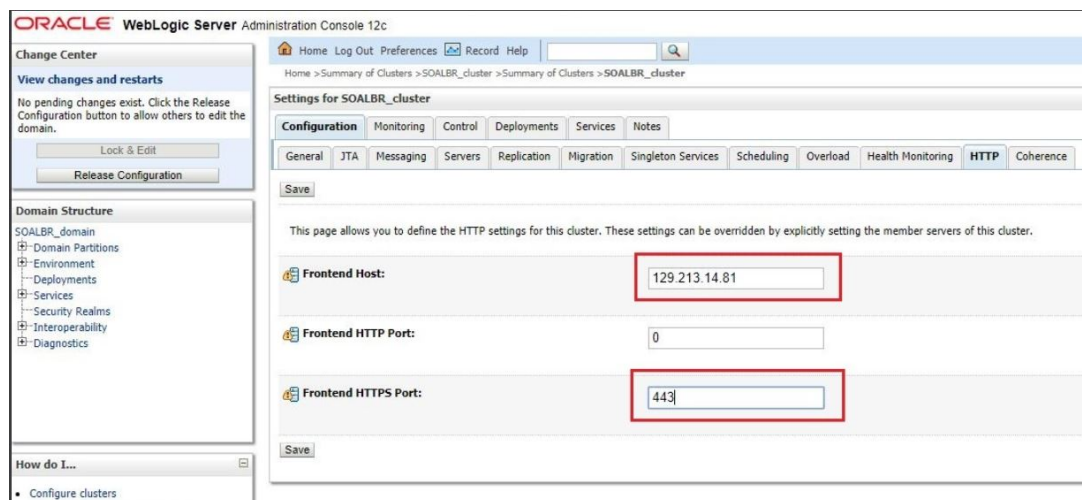
```

Outputs:

FMW Console = https://150.136.86.147:7002/em
Instance Subnet Id = [
  ocid1.subnet.oc1.iad.aaaaaaaa2rgtinr12e2okspdoycrkzhvwaotyccexfsbgd4dchr5y6pxeq
]
Load Balancer Public Ip = [
  129.213.14.81
]
Loadbalancer Subnets Id = [
  ocid1.subnet.oc1.iad.aaaaaaaasod73q5hg34yupj4er42zyep3lsm5z4en4ha6wn3o4djn6e5y6oq
]
Service Consoles =
SOA Composer      : https://129.213.14.81/soa/composer
B2B Console       : https://129.213.14.81/b2bconsole
Service Bus Console : https://150.136.86.147:7002/servicebus
Worklist Application : https://129.213.14.81/integration/worklistapp
Service Instances = [
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwcljtnkmd4byc47m4hytpfax73hsvaeyasg2nrrmko5h2r7qswmwxoxa",
    "Instance name": "SOALBR-soa-0",
    "Private IP": "10.0.6.3",
    "Public IP": "150.136.86.147"
  },
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwcljtnkmd4byck7iwcqiwpbw4tozwbks3ovde2m5bmfvf7kghkcxu5q",
    "Instance name": "SOALBR-soa-1",
    "Private IP": "10.0.6.2",
    "Public IP": "129.213.203.99"
  }
]
Version = 12.2.1.4 (JRF with OCI DB)
Virtual Cloud Network Id = ocid1.vcn.oc1.iad.aaaaaaaajnyi3pvohrm2qwg1ghkfwmmqf7g33oh6af12eb3qaaywdkufln6q
Weblogic administration Console = https://150.136.86.147:7002/console
  
```

### Update the load balancer console URL in the WebLogic Server Administration Console

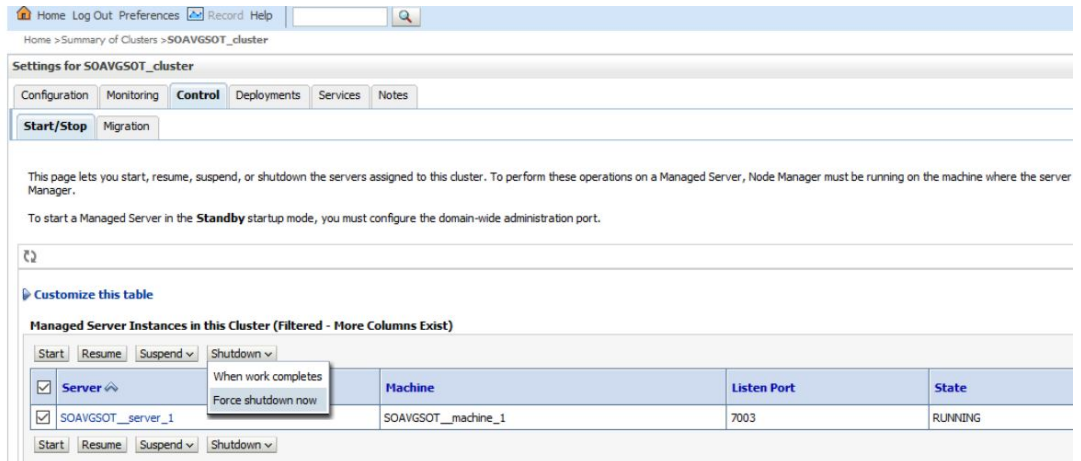
1. Log in to the [WebLogic Server Administration Console](#) and under **Domain Structure**, expand **Environment**, select **Clusters**, and select your SOA cluster.
2. On the Configuration page, select the **HTTP** tab.
3. Update the **Frontend Host** value to the load balancer public IP address (from the log) and set the **Frontend HTTPS Port** to 443.



4. Click **Save**.

### Restart the servers

1. In the WebLogic Server Administration Console, select the **Control** tab, then the **Start/Stop** tab.
2. Select all Managed Servers, then click **Shutdown** and select **Force shutdown now**.



3. After shutdown completes, select all Managed Servers and click **Start**.

## Add a New Load Balancer in an Existing Subnet

Follow these steps to add a load balancer if the `SUBNET STRATEGY` was set to **Use Existing Subnet** during provisioning of the Oracle SOA Suite on Marketplace instance.

If you use an existing subnet, note that the provisioning process will not create any security lists to open ports in the subnets. You must open the ports explicitly before provisioning. See [Prerequisites](#).

To add a load balancer in an existing subnet:

1. Go to the Stack Details page of the instance to which you want to add a load balancer, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. On the Stack Details page, click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and select the `PROVISION LOAD BALANCER` check box, then select the required `LOAD BALANCER SHAPE`.

The screenshot shows the 'Edit Stack' configuration page in Oracle Cloud. On the left, there is a navigation menu with three steps: 'Stack Information', 'Configure Variables' (the current step), and 'Review'. The main configuration area includes several dropdown menus: 'SUBNET STRATEGY' (Use Existing Subnet), 'SUBNET TYPE' (Use Public Subnet), 'SUBNET SPAN' (Regional Subnet), and 'EXISTING SUBNET' (MFT1-wls-subnet (Regional)). Below these, there is a section for 'PROVISION LOAD BALANCER' which is checked. This section includes an 'EXISTING SUBNET FOR LOAD BALANCER' dropdown (MFT1-wls-subnet (Regional)) and a 'LOAD BALANCER SHAPE' dropdown (100Mbps). A red rectangular box highlights the 'PROVISION LOAD BALANCER' section and its associated options.

4. Click **Next** to navigate to the Review page, then click **Save Changes**.
5. To complete the addition of the load balancer, refer to the following steps in [Add a New Load Balancer in a New Subnet](#):
  - [Execute the Terraform Plan operation](#)
  - [Execute the Terraform Apply operation](#)
  - [Get the load balancer details and validate results](#)
  - [Update the load balancer console URL in the WebLogic Server Administration Console](#)
  - [Restart the servers](#)

## Delete a Load Balancer When Added in a New Subnet

Follow these steps to delete a load balancer if you added it to a new subnet post-provisioning (that is, the `SUBNET STRATEGY` was set to **Create New Subnet** during provisioning of the Oracle SOA Suite on Marketplace instance).

To delete a load balancer when it was added in a new subnet:

- [Identify and remove the load balancer security list from the subnet](#)
- [Delete the load balancer console URL in the WebLogic Server Administration Console](#)
- [Restart the servers](#)
- [Edit the stack to deselect provisioning a load balancer](#)

- [Execute the Terraform Plan operation](#)
- [Execute the Terraform Apply operation](#)

### Remove the load balancer security list from the subnet

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Select the VCN for the instance.
4. On the Virtual Cloud Network Details page, select the subnet for the instance.
5. On the Subnet Details page, locate the security list for the instance.

Networking » Virtual Cloud Networks » soa\_examples\_vcn » Subnet Details

## SOALBR-wls-subnet

[Edit](#)
[Move Resource](#)
[Add Tags](#)
[Terminate](#)

Subnet Information | Tags

**OCID:** ...bf4xa [Show](#) [Copy](#)  
**CIDR Block:** 10.0.6.0/24  
**Virtual Router Mac Address:** 00:00:17:2D:18:B0  
**Subnet Type:** Regional

**Compartment:** SOACSDev  
**DNS Domain Name:** subpubsoabr... [Show](#)  
**Subnet Access:** Public Subnet  
**DHCP Options:** [SOALBR-dhcpOptions](#)  
**Route Table:** [SOALBR-routetable](#)

Resources

Security Lists (3)


Tag Filters [add](#) | [clear](#)

no tag filters applied

### Security Lists

[Add Security List](#)

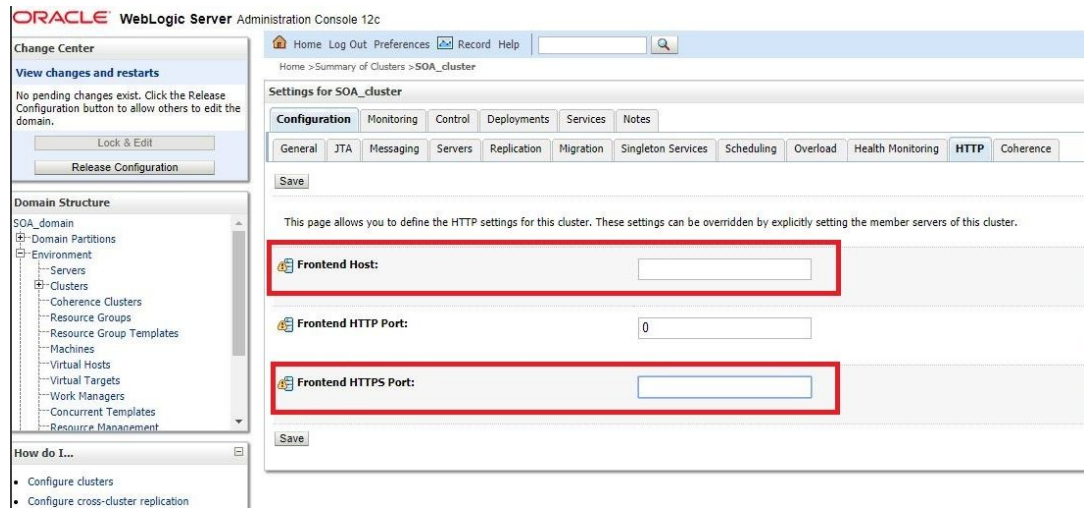
Name	State	Compartment
<a href="#">SOALBR-wls-lb-security-list-1</a>	Available	SOACSDev
<a href="#">SOALBR-internal-security-list</a>	Available	SOACSDev
<a href="#">SOALBR-wls-security-list</a>	Available	SOACSDev

6. At the far right of the row for the security list, click  and select **Remove**, then click **Remove** in the Remove Security List From Subnet dialog.

### Delete the load balancer console URL in the WebLogic Server Administration Console

1. Log in to the [WebLogic Server Administration Console](#) and under **Domain Structure**, expand **Environment**, select **Clusters**, and select your SOA cluster.
2. On the Configuration page, select the **HTTP** tab.
3. Delete the values set for **Frontend Host** and **Frontend HTTPS Port**.

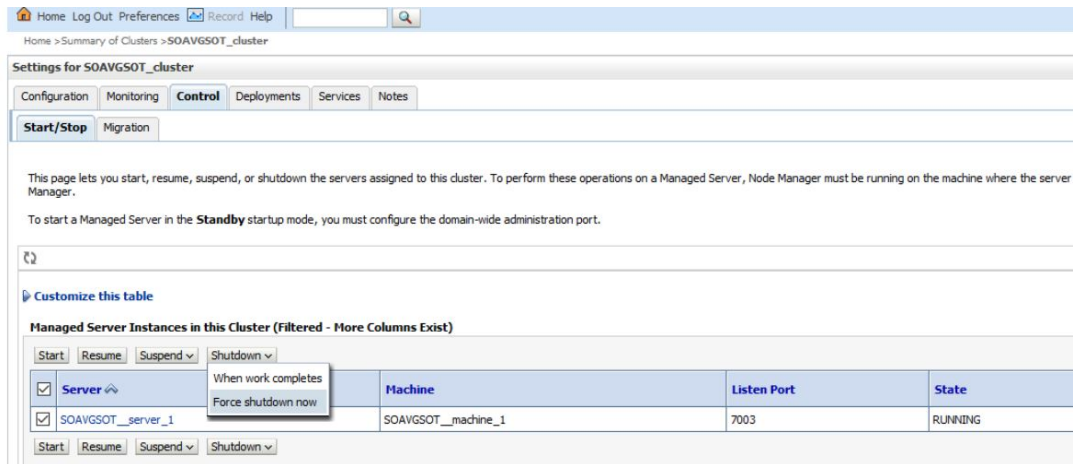




4. Click **Save**.

### Restart the servers

1. In the WebLogic Server Administration Console, select the **Control** tab, then the **Start/Stop** tab.
2. Select all Managed Servers, then click **Shutdown** and select **Force shutdown now**.



3. After shutdown completes, select all Managed Servers and click **Start**.

### Edit the stack to deselect provisioning a load balancer

1. Go to the Stack Details page of the instance for which you want to delete the load balancer, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. On the Stack Details page, click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and deselect the **PROVISION LOAD BALANCER** check box.

4. Click **Next** to navigate to the Review page, then click **Save Changes**.

#### Execute the Terraform Plan operation

1. Go to the Stack Details page of the instance, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. On the Stack Details page, click **Terraform Actions** and select **Plan**.

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

#### Execute the Terraform Apply operation

The Terraform Apply operation deletes the load balancer, along with the associated resources such as a listener, backend sets, and so on.

1. When the Terraform Plan job completes successfully, click **Terraform Actions** and select **Apply**.
2. In the Apply dialog, click **Apply**.

## Delete a Load Balancer When Added in an Existing Subnet

Follow these steps to delete a load balancer if you added it to an existing subnet post-provisioning (that is, the `SUBNET_STRATEGY` was set to **Use Existing Subnet** during provisioning of the Oracle SOA Suite on Marketplace instance).

To delete a load balancer in an existing subnet, refer to the following steps in [Delete a Load Balancer When Added in a New Subnet](#):

1. Delete the load balancer console URL in the WebLogic Server Administration Console.
2. Restart the servers.
3. Edit the stack to deselect provisioning a load balancer.

The screenshot shows the 'Edit Stack' interface in Oracle Cloud. On the left, there is a navigation pane with three steps: 'Stack Information', 'Configure Variables' (highlighted with a blue circle), and 'Review'. The main area displays configuration options for a stack. The 'PROVISION LOAD BALANCER' checkbox is checked and highlighted with a red box. Below it, the 'EXISTING SUBNET FOR LOAD BALANCER' dropdown is set to 'MFT1-wls-subnet (Regional)'. The 'LOAD BALANCER SHAPE' dropdown is set to '100Mbps'. Other options include 'SUBNET STRATEGY' (Use Existing Subnet), 'SUBNET TYPE' (Use Public Subnet), and 'SUBNET SPAN' (Regional Subnet).

4. Execute the Terraform Plan operation .
5. Execute the Terraform Apply operation.

## Access 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.
- 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:**

- [Connect to the Administration Server VM](#)
- [Connect to a Managed Server VM](#)
- [Create an SSH Tunnel](#)
- [Change VM Users](#)
- [Access a VM Through Virtual Network Computing \(VNC\)](#)
- [Access a VM Through PuTTY](#)
- [Run WLST Commands on a VM](#)

## Connect to the Administration Server VM

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

To access the Administration Server VM through SSH:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
3. Click the instance associated with the VM you want to access.
4. Note the **Public IP Address** of the Administration Server VM.

The screenshot shows the Oracle Cloud console interface for a VM instance. At the top, there are several action buttons: Start, Stop, Reboot, Move Resource, Apply Tag(s), and Actions. Below these buttons, there are two tabs: Instance Information (selected) and Tags. The Instance Information section displays the following details:

- Availability Domain: bcaH:US-ASHBURN-AD-1
- Fault Domain: FAULT-DOMAIN-2
- Region: iad
- Shape: VM.Standard2.2
- Virtual Cloud Network: [chef vcn](#)
- Maintenance Reboot: -

The Primary VNIC Information section displays the following details:

- Private IP Address: 10.0.0.2
- Public IP Address: 132.145.137.32 (highlighted with a red box)
- Network Security Groups: None [Edit](#)

5. 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
```

To connect to an instance provisioned in a private network through a Bastion host, use the following command syntax:

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

For example:

```
ssh -i /home/myuser/id_rsa -o ProxyCommand="ssh -W %h:%p -i /home/myuser/id_rsa opc@111.111.111.111" opc@10.0.0.1
```

6. 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.
7. 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.

## Connect 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. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
3. Click the instance associated with the VM you want to access.
4. Note the **Public IP Address** of the Administration Server VM (used as the proxy).

The screenshot shows the Oracle Cloud console interface for a VM instance. At the top, there are buttons for 'Start', 'Stop', 'Reboot', 'Move Resource', 'Apply Tag(s)', and 'Actions'. Below these are two tabs: 'Instance Information' (selected) and 'Tags'. The 'Instance Information' section displays the following details:

- Availability Domain:** bcaH:US-ASHBURN-AD-1
- Fault Domain:** FAULT-DOMAIN-2
- Region:** iad
- Shape:** VM.Standard2.2
- Virtual Cloud Network:** [chef vcn](#)
- Maintenance Reboot:** -

The 'Primary VNIC Information' section displays the following details:

- Private IP Address:** 10.0.0.2
- Public IP Address:** 132.145.137.32 (highlighted with a red box)
- Network Security Groups:** None [Edit](#)

5. On UNIX and UNIX-like platforms, use `ssh` to connect to the VM as the `opc` user:

```
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
```

where:

- `path_to_private_key` is the path to the private key corresponding to the public key used at the time of provisioning.
- `admin_server_VM_IP_address` is the Administration Server VM's public IP address.

For example:

```
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
```

To connect to an instance provisioned in a private network through a Bastion host, use the following command syntax:

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

For example:

```
ssh -i /home/myuser/id_rsa -o ProxyCommand="ssh -W %h:%p -i /home/myuser/id_rsa opc@111.111.111.111" opc@10.0.0.1
```

6. 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.

 **Note:**

You can optionally save this session configuration by navigating to the Session panel and clicking **Save**. When you open PuTTY the next time, you can load this configuration by selecting it and clicking **Load**.

When the VM command line appears, you can use any resource accessible from the VM.

## Create 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.

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

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
3. Click the instance associated with the VM you want to access.
4. Note the **Public IP Address** of the Administration Server VM.
5. On UNIX and UNIX-like platforms, use `ssh` to create an SSH tunnel to the VM:

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

where:

- *path\_to\_private\_key* is the path to the private key corresponding to the public key used at the time of provisioning.
- *VM\_IP\_address* is the VM's public IP address.
- *port* is 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.

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

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

6. On Windows, you can use PuTTY, an open source networking client for the Windows platform, to create an SSH tunnel to the VM.

To download PuTTY, go to <http://www.putty.org/> and click the link to download PuTTY.

- 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:**

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.

 **Note:**

You can optionally save this session configuration by navigating to the Session panel and clicking **Save**. When you open PuTTY the next time, you can load this configuration by selecting it and clicking **Load**.

7. 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, press Ctrl+C to shut down the SSH tunnel.

## Change 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 operating system (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:

```
sudo useradd myuser
```

**Note:**

There is no default password for the `opc` user.

### Changing to the `oracle` user

The `oracle` 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.

To change to the `oracle` user, enter the following command:

```
sudo su - oracle
```

**Note:**

There is no default password for the `oracle` user.

### Changing to the `root` user

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

To change to the `root` user, enter the following command:

```
sudo -s
```

**Note:**

Avoid using the `root` user except to perform privileged OS administration tasks.

## Access a VM Through Virtual Network Computing (VNC)

You can access the services and resources that an Oracle SOA Suite on Marketplace VM provides by logging into the VM through VNC.

You can use any VNC client utility to access a VM. For example, if you are using Windows, you might use [RealVNC](#) or [TightVNC](#); if you are using Linux, you might use the `vncviewer` utility included with your Linux distribution.

By default, the port used by the VNC server on an Oracle SOA Suite on Marketplace VM is not directly accessible through the Internet. An SSH tunnel enables access to the VNC server port on your local machine. An SSH tunnel also ensures that VNC communication is using a secure channel.

To create a VNC session on a VM:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

### Note:

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.

3. Disable the desktop screensaver lock for this user:

```
gconftool-2 -s -t bool /apps/gnome-screensaver/lock_enabled false
```

This Linux property controls whether or not the desktop prompts you for the user's password when in screensaver mode.

4. Start the VNC server on the VM:

```
vncserver :1 -nolisten tcp -localhost -geometry 1680x1050
```

Use the following command to confirm if the VNC server started or not:

```
ps -ef|grep vncserver
```

 **Note:**

The VNC server is not directly accessible from clients outside of this VM. An SSH tunnel will be used to enable external and secure access to the VNC server.

By default, the listen port for VNC session :1 is 5901, session :2 is 5902, and so on.

If your local machine has a smaller display resolution, use a different geometry setting such as 1024x768.

5. When prompted, enter a password for this VNC session.
6. Disconnect from the VM.
7. Create an SSH tunnel to `localhost:5901` on the VM.

```
ssh -i path_to_private_key -L 5901:localhost:5901 opc@VM_IP_address -N
```

For example:

```
ssh -i /home/myuser/id_rsa -L 5901:localhost:5901 opc@111.111.111.111 -N
```

8. Launch your VNC client application and connect to `localhost:5901`.
9. When prompted, enter the password that you previously configured for this VNC session.

You can use VNC to work with any resource accessible from the VM, including graphical applications. For example, you can launch the Fusion Middleware Configuration Wizard application on the Administration Server VM.

 **Note:**

After your VNC work is complete, you can perform a `<ctrl> C` to shut down the SSH tunnel.

 **Note:**

To terminate the VNC server on the VM, run `vncserver -kill :1`.

## Access a VM Through PuTTY

You can access the services and resources that an Oracle SOA Suite on Marketplace VM provides from a Windows platform by using PuTTY, an open source networking client.

In general, an SSH tunnel can map a remote port to any available port number on your local computer. Some protocols, such as Java Remote Method Invocation (RMI), require that the remote and local port numbers be the same value.

To download PuTTY, go to <http://www.putty.org/>.

1. Access your service console.
2. Click the name of the service instance that contains the node that you want to access.

3. On the Overview page, identify the **Public IP** address of the node that you want to access.  
For example, 203.0.113.13.
4. Start PuTTY on your Windows computer.  
The PuTTY Configuration window is displayed, showing the Session panel.
5. In the **Host Name (or IP address)** field, enter the public IP address of the node.
6. In the Category navigation tree, expand **Connection**, and then click **Data**.
7. In the **Auto-login username** field, enter `opc`.
8. In the **When username is not specified** field, select **Prompt**.
9. In the Category tree, expand **Connection**, and then click **SSH**.
10. Under **Protocol options**, select the check box **Don't start a shell command at all**.
11. In the Category tree, expand **SSH**, and then click **Auth**.
12. Under **Private key file for authentication**, click **Browse**.
13. Navigate to the location of your private key file, and select it. Click **Open**.

This private key corresponds to the public key that you specified when you created this service instance.

 **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 Oracle Cloud generated this key for your service instance, see the PuTTY documentation for information about converting the key format.

14. In the Category tree, expand **SSH**, and then click **Tunnels**.
15. In the **Destination** field, enter `IP:port`,  
where *IP* is the IP address of the node and *port* is the port number on the node to which you want to connect.
16. In the **Source Port** field, enter the same port number.
17. Click the **Add** button.
18. Optional: To save this session configuration, click **Session** in the Category tree, and then click **Save**.  
To load a saved configuration, select the configuration name, and then click **Load**.
19. Click **Open**.
20. If prompted, enter the passphrase for the private key.

Applications that are running on your local computer can now communicate with the node by using `localhost:port`, where *port* is the local port number.

After your work with the SSH tunnel is completed, press Ctrl+C to close the SSH tunnel.

## Run WLST Commands on a VM

You can run WLST commands from within any Oracle SOA Cloud Service VM that includes an Oracle WebLogic Server installation.

To run WLST commands on a VM:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Change the directory to the `bin` folder in `DOMAIN_HOME`:

```
cd $DOMAIN_HOME/bin
```

For example:

```
cd /u01/data/domains/soa_domain/bin
```

4. Set up the environment:

```
source setDomainEnv.sh
```

You must use `.` to ensure that the environment variables are set in the current shell.

5. Start WLST:

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

6. Connect to the Administration Server:

```
connect('username', 'password', 't3://admin-server-host:admin-server-port')
```

For example:

```
connect('weblogic', 'welcome', 't3://serviceName-wls-1:9071')
```

7. To deploy a composite, connect to the Managed Server using port 9073 and run the following command:

```
sca_deployComposite('http://admin-server-host:admin-server-port',  
'composite-jar')
```

For example:

```
sca_deployComposite('http://serviceName-wls-1:9073', '/tmp/  
sca_HelloWorld_rev1.0.jar')
```

Refer to [WLST Command and Variable Reference](#) in *WLST Command Reference for Oracle WebLogic Server*.

## Perform Lifecycle Operations on an Oracle SOA Suite on Marketplace Instance

### Topics:

- [Disable Server Restart During an Instance Reboot](#)
- [Stop or Start an Oracle SOA Suite on Marketplace Instance and Servers](#)
- [Scale an Oracle SOA Suite on Marketplace Instance Cluster Out or In](#)
- [Scale an Oracle SOA Suite on Marketplace Instance Up or Down](#)
- [Back Up the Domain Home](#)
- [Restore the Domain Home](#)
- [Back Up a Block Volume](#)
- [Restore a Block Volume](#)
- [Deprovision an Oracle SOA Suite on Marketplace Instance](#)

### Disable Server Restart During an Instance Reboot

For Oracle SOA Suite on Marketplace instances provisioned on or after 20.4.2, if you need to reboot an instance, you can optionally disable the default automatic restart of the Administration Server and Managed Servers.

To disable the automatic restart of the Administration Server and Managed Servers when you reboot an Oracle SOA Suite on Marketplace instance (provisioned on or after 20.4.2):

1. In the `DOMAIN_HOME` directory, open `soampRebootEnv.sh` in a text editor:

```
vi ${DOMAIN_HOME}/soampRebootEnv.sh
```

2. Set the `start_server_on_reboot` variable to `false`:

```
export start_server_on_reboot=false
```

3. Save `soampRebootEnv.sh`.

To enable the automatic restart of the servers again, open `soampRebootEnv.sh` and set the `start_server_on_reboot` variable to `true`:

```
export start_server_on_reboot=true
```

### Stop or Start an Oracle SOA Suite on Marketplace Instance and Servers

You can stop or start an Oracle SOA Suite on Marketplace instance, which automatically stops or starts the Administration Server and Managed Server running on the instance.

To achieve zero down time, you can stop and start one instance at a time in a multinode cluster. This stops or starts the corresponding Administration Server and Managed Server on one instance, leaving the servers on the other instances in the cluster running.



When an Oracle Cloud Infrastructure instance is stopped, billing depends on the compute shape used to create the instance. This means that stopping an Oracle SOA Suite on Marketplace instance may or may not pause billing. See [Resource Billing for Stopped Instances](#) in the Oracle Cloud Infrastructure documentation.

 **Note:**

When an Oracle SOA Suite on Marketplace instance is running, you can stop, start, and restart the Administration Server or Managed Server independently, without stopping the instance. You might want to do this if you have other processes besides the servers running on the instance and you do not want to shut down these other processes.

### Why Stop an Oracle SOA Suite on Marketplace Instance?

Stopping an Oracle SOA Suite on Marketplace instance frees up compute resources used by the instance.

### Why Stop, Start, or Restart an Administration Server or Managed Server?

When an Oracle SOA Suite on Marketplace instance is running:

- You can stop the Managed Server to free up resources. You might also want to stop the instance instead of scaling, keeping the server ready for a later time.
- You can start a Managed Server if it is stopped and you want to use it again.
- You can restart the Administration Server or Managed Server if you are experiencing problems with the server that would warrant a reboot. The restart operation is the same as stopping the server, then starting it immediately.


#### Topics:

- [Stop or Start an Oracle SOA Suite on Marketplace Instance](#)
- [Stop or Start WebLogic Servers](#)

## Stop or Start an Oracle SOA Suite on Marketplace Instance

Use the Oracle Cloud Infrastructure Console to stop or start an Oracle SOA Suite on Marketplace instance.

To stop or start an Oracle SOA Suite on Marketplace instance:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
3. On the Compute page, at the far right of the row for the instance, click  and select **Stop** or **Start**.

Repeat this step for all nodes in the cluster.

After you start (or reboot) the instance, if the servers are not running, complete the following steps:

1. Change to the `oracle` user:

```
sudo su - oracle
```

2. Run the restart script:

```
/opt/scripts/restart/restart_12c_servers.sh
```

Wait for the servers to start before proceeding.

## Stop or Start WebLogic Servers

You can stop or start WebLogic Servers using WebLogic Scripting Tool (WLST) commands and the WebLogic Server Administration Console.

To stop the WebLogic servers:

- [Stop the Managed Servers](#)
- [Stop the Administration Server](#)

To start the WebLogic servers:

- [Start the Administration Server](#)
- [Start the Managed Servers](#)

## Stop or Start the Managed Servers

You can stop or start the Managed Servers for an Oracle SOA Suite on Marketplace instance through the WebLogic Server Administration Console.

To stop or start the Managed Servers:

1. Log in to the [WebLogic Server Administration Console](#).
2. Under **Domain Structure**, expand **Environment** and select **Servers**.
3. On the Configuration page, note the state of the Administration Server and the Managed Servers.
4. Select the **Control** tab.
5. For each Managed Server:
  - Click the check box to the left of a Managed Server name.
  - To stop a Managed Server: Click **Shutdown**, and then select **Force Shutdown Now** or **When Work Completes**.
  - To start a Managed Server: Click **Start**.
6. On the Server Life Cycle Assistant, click **Yes**.  
The server state changes to `SHUTTING DOWN` (if stopping) or `STARTING` (if starting).
7. Click the **Refresh** icon.  
The server state changes to `SHUTDOWN` (if stopping) or `RUNNING` (if starting).

## Stop or Start the Administration Server

You stop or start the Administration Server for an Oracle SOA Suite on Marketplace instance through the Node Manager by using WLST commands.

To stop or start the Administration Server:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Check that the Node Manager is running:

```
ps -ef | grep NodeManager
```

You should receive messages showing that the Node Manager is running.

4. Change the directory to the `bin` folder in `DOMAIN_HOME`.

```
cd $DOMAIN_HOME/bin
```

For example, `/u01/data/domains/OurServi_domain/bin`

5. Set up the environment.

```
. ./setDomainEnv.sh
```

You must use the `.` to ensure that the environment variables are set in the current shell.

6. Start WLST:

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



#### Note:

If you see exceptions while starting the command, ignore them and continue to next step.

7. To connect to the Node Manager, use the WLST `nmConnect` command:

```
nmConnect  
( 'username', 'password', 'host', 'nmPort', 'domainName', 'domainDir', 'nmType' )
```

Parameter	Description	Example
<code>username</code>	WebLogic Server username you specified when you created the instance.	
<code>password</code>	WebLogic Server password you specified when you created the instance.	
<code>host</code>	The host name of the Node Manager. This is typically of the format <i>instanceName-wls-1</i> .	<code>ourserviceinstance-wls-1</code>
<code>nmPort</code>	Port number of the Node Manager.	<code>5556</code>

Parameter	Description	Example
domainName	Name of the domain, which is the name of the folder in /u01/data/domains/.	OurServi_domain
domainDir	Path to the domain. The domain directory is /u01/data/domains/domainName.	/u01/data/domains/OurServi_domain
nmType	Use SSL for Java-based SSL implementation.	SSL

For example:

```
nmConnect ('weblogic','welcome','ourserviceinstance-
wls-1','5556','OurServi_domain','/u01/data/domains/OurServi_domain','SSL')
```

#### 8. Stop or start the Administration Server:

- To stop the Administration Server, follow the steps in [Stop or Start the Managed Servers](#), selecting and shutting down the Administration Server. When you shut down the Administration Server, a message warns you that the browser session will end.
- To start the Administration Server, use nmStart:

```
nmStart ('server_name')
```

For example:

```
nmStart ('OurServi_adminserver')
```

#### 9. Exit WLST:

```
exit()
```

## Scale an Oracle SOA Suite on Marketplace Instance Cluster Out or In

Scale an Oracle SOA Suite on Marketplace instance cluster out or in to add or remove nodes 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.

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, as described in [Scale an Oracle SOA Suite on Marketplace Instance Up or Down](#).

 **Notes:**

- A scale out or in operation does not need down time and servers on the nodes in the Oracle SOA Cloud Service cluster are available during the scale operation.
- 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:**

- [Scale Out an Oracle SOA Suite on Marketplace Instance Cluster](#)
- [Scale In an Oracle SOA Suite on Marketplace Instance Cluster](#)

## Scale Out an Oracle SOA Suite on Marketplace Instance Cluster

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

 **Notes:**

- Adding a node to a cluster increases the billing of the Oracle SOA Suite on Marketplace instance.
- If an attempt to scale out a cluster fails, you will need to complete a scale in operation to revert the Oracle SOA Suite on Marketplace instance to its original state.
- Ensure that the WebLogic Server and Node Manager passwords are the same.
- If you have configured your WebLogic Server domain with custom certificates, ensure that they are not self-signed certificates.
- If any patches were applied after provisioning the Oracle SOA Suite on Marketplace instance, the new node will not include those patches. You will need to apply the patches to the newly added Managed Server. See [About Managing Patches for Instances Provisioned With Earlier Releases](#).

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

1. Go to the Stack Details page of the instance you want to scale out, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).

2. Click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables**.
4. Increment the **Cluster Node Count** value by 1.

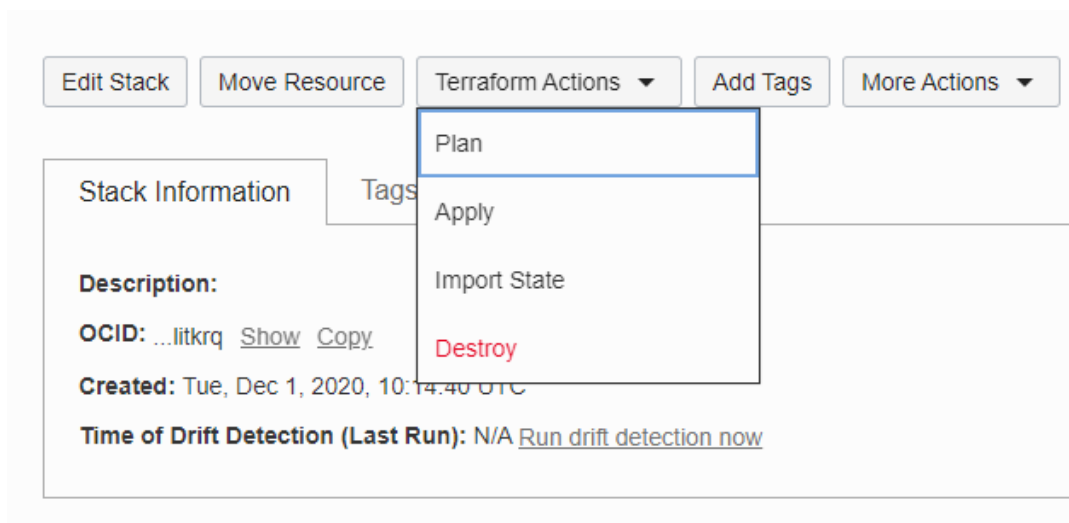
 **Note:**

Add only one node at a time.

5. (Optional) To copy Middleware Home and Oracle Home from the Administration Server VM to the newly added node, select **Copy Middleware Home and Oracle Home from Admin VM**.

When selected, the newly added node automatically receives all the patches that are manually applied post-provisioning on the Administration Server VM. However, the copy operation takes time, so the scale out operation may take a while to complete. Additionally, you must make sure that there is enough storage in the boot volume of the Administration Server to create the binaries ZIP.

6. Click **Next** to navigate to the Review page showing the new cluster node count value.
7. Click **Save Changes**.
8. On the Stack Details page, click **Terraform Actions** and select **Plan**.




9. In the Plan dialog, click **Plan**.
10. When the Terraform plan job completes successfully, click **Terraform Actions** and select **Apply**.
11. In the Apply dialog, click **Apply**.
12. After the Terraform Apply operation completes successfully, open the log to review the updated instance summary with the new node details:
  - a. Go to the Stack Details page of the instance, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
  - b. In the **Jobs** section, click the job name to display the Job Details page.

- c. Under **Resources** in the left pane, click **Outputs** to view the log. For example:

```
Apply complete! Resources: 8 added, 1 changed, 1 destroyed.

Outputs:

FMW Console = https://132.145.166.161:7002/em
Instance Subnet Id = [
  ocid1.subnet.oc1.iad.aaaaaaaaz7sjjpygvcvot2v3hz5yhh5sonk56cbbef5dafcr6gtwutmf7xa
]
Load Balancer Public Ip = [
  150.136.201.161
]
Loadbalancer Subnets Id = [
  ocid1.subnet.oc1.iad.aaaaaaaaz7sjjpygvcvot2v3hz5yhh5sonk56cbbef5dafcr6gtwutmf7xa
]
Service Consoles =
SOA Composer      : https://150.136.201.161/soa/composer
B2B Console       : https://150.136.201.161/b2bconsole
Service Bus Console : https://132.145.166.161:7002/servicebus
Worklist Application : https://150.136.201.161/integration/worklistapp
Service Instances = [
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwcljtnkmd4byc2jaoql6lendpku273xppru34xc6qql3g7gdsvglgka6a",
    "Instance name": "SOAScale-soa-0",
    "Private IP": "10.0.25.6",
    "Public IP": "132.145.166.161"
  },
  {
    "Instance Id": "ocid1.instance.oc1.iad.anuwcljtnkmd4bycdz4mi33h24aac7m7k4k7rbguwpabe5lrkn236i74saha",
    "Instance name": "SOAScale-soa-1",
    "Private IP": "10.0.25.7",
    "Public IP": "150.136.166.29"
  }
]
Version = 12.2.1.4 (JRF with OCI DB)
Virtual Cloud Network Id = ocid1.vcn.oc1.iad.aaaaaaaaz7y13pvv22qwg1k0xfmmqf3m13dha77eb3qaaywdkufln6q
Weblogic administration Console = https://132.145.166.161:7002/console
```

13. If you previously configured custom certificates for the instance, the scale out operation resets the load balancer to use the default certificate. To reconfigure the load balancer to use a custom certificate:
- Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
  - In the left pane, click **Load Balancers**.
  - Scroll down in the left pane and select the compartment where the load balancer exists.
  - Click the name of the load balancer you want to configure.
  - In the left pane of the Load Balancer Details screen, click **Listeners**, then click the  icon at the far right of the row for the listener you created, and select **Edit**.
  - In the Edit Listener dialog, select the custom certificate name.

**Edit Listener** [Help](#)

To allow your load balancer to accept ingress traffic, specify the protocol and port for your public IP address.

NAME  
httpsListener

There are no hostnames for this load balancer. [Create a hostname.](#)

PROTOCOL: HTTP | PORT: 443 | USE SSL:

CERTIFICATE NAME: cert\_lb\_2020-0501-1654 | VERIFY PEER CERTIFICATE:

BACKEND SET: httpBackend

IDLE TIMEOUT IN SECONDS OPTIONAL: 60  
The default timeout for HTTP is 60 seconds.

There are no path route sets for this load balancer. [Create a path route set.](#)

**Rule Sets**

ORDER	RULE SET
↑ ↓	SSLHeader

There are no more rule sets associated with this load balancer.

[+ Additional Rule Set](#)

**Save Changes** [Cancel](#)

g. Click **Save Changes**.

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

## Scale In an Oracle SOA Suite on Marketplace Instance Cluster

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

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 [Deprovision an Oracle SOA Suite on Marketplace Instance](#).

### Note:

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

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

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

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 Administration 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 WebLogic Server Administration 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:

```
$ ssh -i xperiment_rsa opc@150.136.139.125
The authenticity of host '150.136.139.125 (150.136.139.125)' can't be established.
ECDSA key fingerprint is SHA256:HsSIA03cs09wGmMmRQKHPT6w71k1hB6734oajnfUz2es.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '150.136.139.125' (ECDSA) to the list of known hosts.
Last login: Tue Mar 17 16:57:02 2020 from 150.136.199.107
[opc@soatest-soa-0 ~]$ sudo su oracle
[oracle@soatest-soa-0 opc]$ cd /opt/scripts/
[oracle@soatest-soa-0 scripts]$ ./delete_server.sh
Enter the managed server name you want to delete : SOATest_server_2
Enter the WLS Admin Password :
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

<Mar 18, 2020 4:19:59 AM GMT> <Info> <scale_in_domain.py> <BEA-000000> <(host:soatest-soa-0.subpubsoatest
in Extension on this instance>
<Mar 18, 2020 4:20:00 AM GMT> <Info> <scale_in_domain.py> <BEA-000000> <(host:soatest-soa-0.subpubsoatest
rver_2>
<Mar 18, 2020 4:20:00 AM GMT> <Info> <scale_in_domain.py> <BEA-000000> <(host:soatest-soa-0.subpubsoatest
>
```

After completing the prerequisite steps, perform the following steps to scale in an Oracle SOA Suite on Marketplace instance cluster:

1. Go to the Stack Details page of the instance you want to scale out, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. Click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables**.
4. Decrement the **Cluster Node Count** value by 1.

#### Note:

Remove only one node at a time.

5. Follow steps 5-13 in [Scale Out an Oracle SOA Suite on Marketplace Instance Cluster](#).

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

## Scale an Oracle SOA Suite on Marketplace Instance Up or Down

You can scale an Oracle SOA Suite on Marketplace instance up or down by changing its compute shape in response to changes in workload or to add storage to a node that is running out of storage.

The compute shape specifies the number of Oracle Compute Units (OCPU) and amount of memory (RAM) that you want to allocate to the node. See **Compute Shape** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

### Notes:

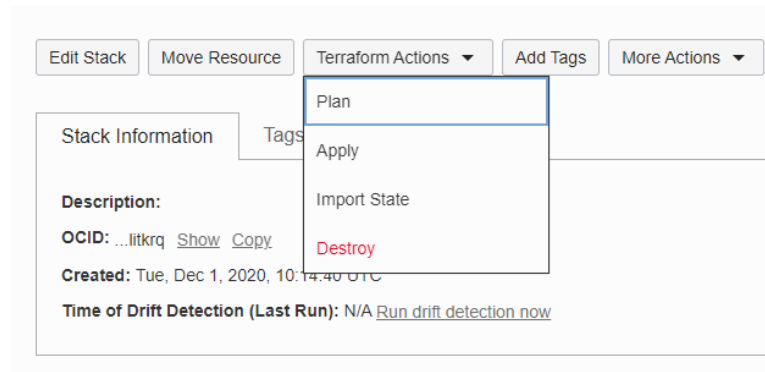
- Changing the compute shape to a higher value increases the billing of the Oracle SOA Suite on Marketplace instance.
- A scale up or down operation requires some down time as servers on the Oracle SOA Suite on Marketplace node are automatically restarted after the scale operation. In a multinode instance cluster, the node that is scaled is restarted, while the other nodes continue running. Before scaling, make sure that there are no active running processes on the servers of the node you are scaling up or down.

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

1. Go to the Stack Details page of the instance you want to scale up or down, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. Click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to the Configure Variables page.
4. 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.

For information about compute shapes, see:

- **Compute Shape** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).
  - [Compute - Virtual Machine Instances](#)
  - [Standard Shapes](#) in the Oracle Cloud Infrastructure documentation.
5. Click **Next** to go to the Review page showing the new compute shape value.
  6. Click **Save Changes**.
  7. On the Stack Details page, click **Terraform Actions** and select **Plan**.



8. In the Plan dialog, click **Plan**.
9. When the Terraform plan job completes successfully, click **Terraform Actions** and select **Apply**.
10. In the Apply dialog, click **Apply**.

## Back Up the Domain Home

The backup operation takes a backup of the domain homes for all nodes in an Oracle SOA Suite on Marketplace instance cluster.

### Prerequisites:

- Enable backup and restore either in the provisioning wizard, or by editing the Oracle SOA Suite on Marketplace instance. See **Enable Backup/Restore configuration** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).
- Make sure that you have enough space in the domain block volume to copy the domain home backups before running the backup script.

To back up the domain home for all nodes in an Oracle SOA Suite on Marketplace instance cluster:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Run the backup script to initiate the domain home backup:

```
/opt/scripts/runbooks/backup.sh
```

This command backs up the domain homes from all the nodes of the cluster, encrypts the backup ZIP file, and uploads the ZIP file to Oracle Cloud Infrastructure Object Storage under a folder named with the service name, and a subfolder named with timestamp of the backup.

	Name	Last Modified
<input type="checkbox"/>	SOAMP_SOAMPDemo	-
<input type="checkbox"/>	03082023_132526	-
<input type="checkbox"/>	SOAMPDemo_domain.enc	Wed, Mar 8, 2023, 13:26:12 UTC

## Restore the Domain Home

The restore operation shuts down all the running servers, along with Node Manager, and replaces the domain homes with the backup.

### Note:

The cluster size of the Oracle SOA Suite on Marketplace instance must be the same as the size of the domain backup. If the cluster size does not match, the restore is terminated with an error message.

**Prerequisite:** Enable backup and restore in the provisioning wizard or by editing the Oracle SOA Suite on Marketplace instance. See **Enable Backup/Restore configuration** in [Provision an Oracle SOA Suite on Marketplace Instance in the Oracle Cloud Infrastructure Console](#).

To restore the domain home for all nodes in an Oracle SOA Suite on Marketplace instance cluster:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

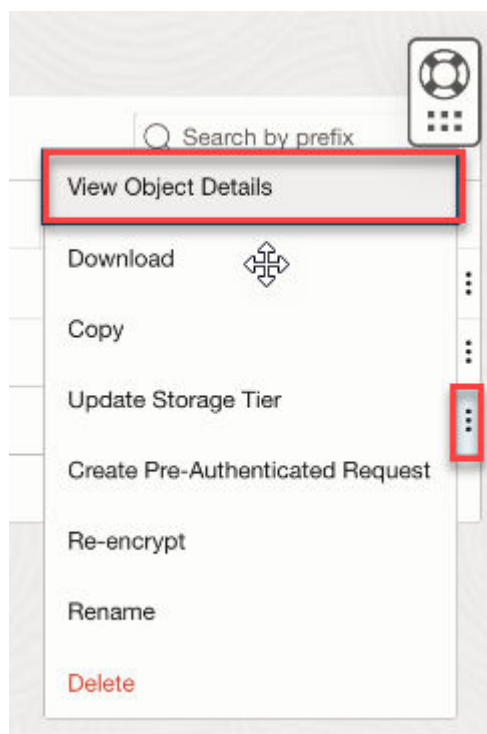
```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Retrieve the backup object name from the Oracle Cloud Infrastructure Object Storage console:

Click the **Actions**  icon for the backup file, then select **View Object Details**.



In the Basic Information pane, copy the name of the backup file.



4. Run the restore script to initiate the domain home restore, responding to the prompts for the WebLogic Server administration password, Node Manager password, and backup object name that you retrieved in the previous step:

```
$ cd /opt/scripts/runbooks
$ ./restore.sh
Enter the weblogic admin password :
Enter the weblogic nodemanager password :
Do you want to start the servers after restore (yes/[no]) ?yes
<Mar 08, 2023 01:41:52 PM GMT> <INFO> <file_utils.py> <(host:soampdemo-
soa-0.mpsubnet.soacsvcn.oraclevcn.com) - Cannot delete the directory /u01/
data/SOAMP_SOAMPDemo as it does not exist>
Backup object name :
```

## Back Up a Block Volume

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


The backup functionality allows you to perform a backup of data on a block volume, either manually or automatically. You can then restore these backups to new volumes, immediately after a backup or later.

### Topics:

- [Back Up a Block Volume Manually](#)
- [Configure Automatic Block Volume Backups](#)

## Back Up a Block Volume Manually


To back up a block volume manually:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Storage**. Under **Block Storage**, click **Block Volumes**.
3. 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**.
4. In the Create Block Volume Backup dialog, enter a name for the backup and select the backup type, either **Full** or **Incremental**.
5. Click **Create Block Volume Backup**.

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

## Configure Automatic Block Volume Backups

To configure automatic block volume backups:

1. [Sign in to the Oracle Cloud Infrastructure Console](#).
2. Open the navigation menu and click **Storage**. Under **Block Storage**, click **Block Volumes**.
3. At the far right of the row for the block volume for which you want to create a backup, click  and select **Edit**.
4. In the Edit Volume dialog, scroll to the **Backup Policies** section, and select a policy from the drop-down list.
5. Click **Save Changes**.

## Restore 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 \(DBFS\)](#)
- [Unmount the old volume](#)

- [Disable the old volume](#)
- [Detach the old volume from Compute](#)
- [Create a new volume from the backup volume](#)
- [Attach the new volume to the SOA instance](#)
- [Connect to the new volume](#)
- [Mount the new volume](#)
- [Mount the Oracle Database File System \(DBFS\)](#)
- [\(Optional\) Delete the old volume](#)

### Unmount the Oracle Database File System (DBFS)

#### Note:

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

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Enter the following commands:

```
sudo fusermount -u /u01/data/dbfs
sudo fusermount -u /u01/data/dbfs_directio
```

### Unmount the old volume

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```


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. [Sign in to the Oracle Cloud Infrastructure Console](#).
3. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
4. Click the name of the instance to display the Instance Details page.
5. In the **Resources** section, click **Attached Block Volumes**.

- At the far right of the row for the block volume that you want to disconnect, click  and select **iSCSI Commands & Information**.

[help](#) [close](#)

Use OS tools to edit your /etc/fstab volume to have the \_netdev and nofail options from the OS. Failure to run commands will cause instance boot failure.

ATTACH COMMANDS

```
sudo iscsiadm -m node -o new -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169
sudo iscsiadm -m node -o update -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -n
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.
```

[Copy](#)

DETACH COMMANDS

```
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2:3
sudo iscsiadm -m node -o delete -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169
```

[Copy](#)

IP ADDRESS AND PORT

[Copy](#)

VOLUME IQN

[Copy](#)

- 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
iqn.2015-12.com.oracleiaas:d7ebe8-4ef7-430d-87cd-8127332bb0fd -p
169.254.2.2:3260 -u
Logging out of session [sid: 2, target:
iqn.2015-12.com.oracleiaas:d7ebe8-4ef7-430d-87cd-8127332bb0fd,
portal: 169.254.2.2,3260]
iscsiadm: Could not logout of [sid: 2, target:
iqn.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:
iqn.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418,
portal: 169.254.0.2,3260]
Logout of [sid: 2, target:
iqn.2015-12.us.oracle.com:c6acda73-90b4-4bbb-9a75-faux09015418,
portal: 169.254.0.2,3260] successful.
```



### Detach the old volume from Compute

1. Open the navigation menu and click **Compute**. Under **Compute**, 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**.

Detach Block Volume [help](#) [close](#)

Use OS tools to disable/delete and logoff the iSCSI targets to this volume before detaching. Remove this volume's entry from /etc/fstab if you have previously added it. Failure to do so may cause subsequent reboots to take longer.

DETACH COMMANDS

```
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2 -o delete
```

[Copy](#)

IP ADDRESS AND PORT

[Copy](#)


VOLUME IQN

[Copy](#)

[Continue Detachment](#)

5. In the Detach Block Volume dialog, click **Continue Detachment**.

### Create a new volume from the backup volume

1. Select the compartment in which the block volume backup you are restoring is saved.
2. Open the navigation menu and click **Storage**. Under **Block Storage**, 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. Open the navigation menu and click **Compute**. Under **Compute**, 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**.

Attach Block Volume [help](#) [cancel](#)

Choose how you want to attach your block volume.

ISCSI  
 PARAVIRTUALIZED

ACCESS

READ/WRITE  
Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.

READ/WRITE - SHAREABLE  
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances

READ-ONLY - SHAREABLE  
Select to configure the volume attachment as read-only, enabling attachment to multiple instances.

SELECT VOLUME  ENTER VOLUME OCID

BLOCK VOLUME COMPARTMENT

SOACSDev

oicpaas1 (root)/SOACSDev

BLOCK VOLUME

Select a Block Volume or a Boot Volume

REQUIRE CHAP CREDENTIALS

Attach

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. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
2. Click the name of the instance to display the instance details.
3. In the **Resources** section, click **Attached Block Volumes**.

- At the far right of the row for the block volume that you want to attach, click  and select **iSCSI Commands and Information**.

[help](#) [close](#)

Use OS tools to edit your /etc/fstab volume to have the \_netdev and nofail options from the OS. Failure to run commands will cause instance boot failure.

ATTACH COMMANDS

```
sudo iscsiadm -m node -o new -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2:3260
sudo iscsiadm -m node -o update -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -n
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2:3260
```

[Copy](#)

DETACH COMMANDS

```
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2:3260
sudo iscsiadm -m node -o delete -T iqn.2015-12.com.oracleiaas:d9dddfef-8816-4474-8b6b-1e72b6fcf6d0 -p 169.254.2.2:3260
```

[Copy](#)

IP ADDRESS AND PORT

[Copy](#)

VOLUME IQN

[Copy](#)

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.

- Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):
 

```
ssh -i private_key opc@Admin_VM_Public_IP
```
- Copy and paste the `ATTACH COMMANDS` into your instance session window to connect the volume and configure iSCSI to automatically connect to the authenticated block storage volumes after a reboot.

### Mount the new volume

- Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

- Enter the following commands:

```
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
```

- Restart the Administration Server 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 the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):



```
ssh -i private_key opc@AdminServerVM_IP_address
```

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

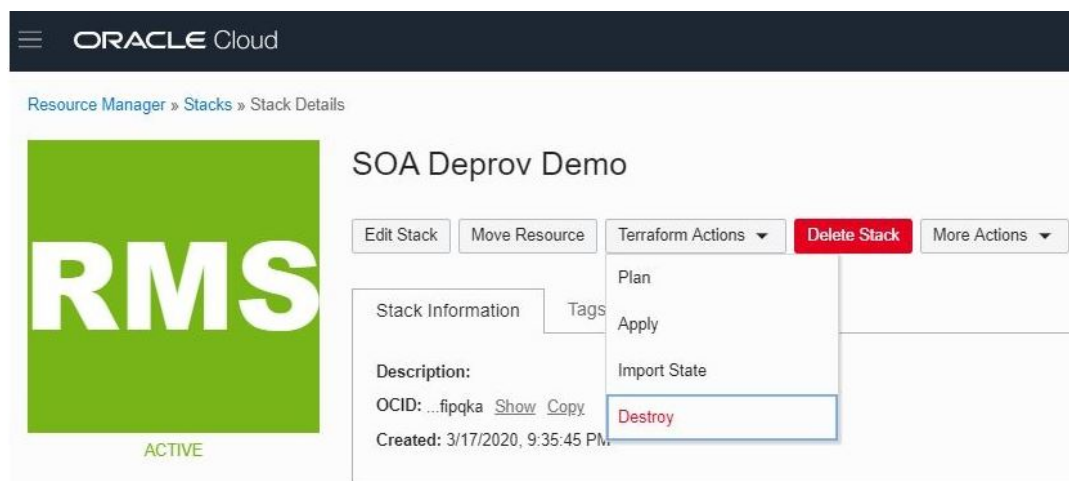
1. In the Oracle Cloud Infrastructure Console, click  in the top left corner. In the navigation menu, under **Core Infrastructure**, go to **Block Storage** and click **Block Volumes**.
2. At the far right of the row for the block volume backup you want to delete, click  and select **Terminate** and confirm when prompted.

## Deprovision an Oracle SOA Suite on Marketplace Instance

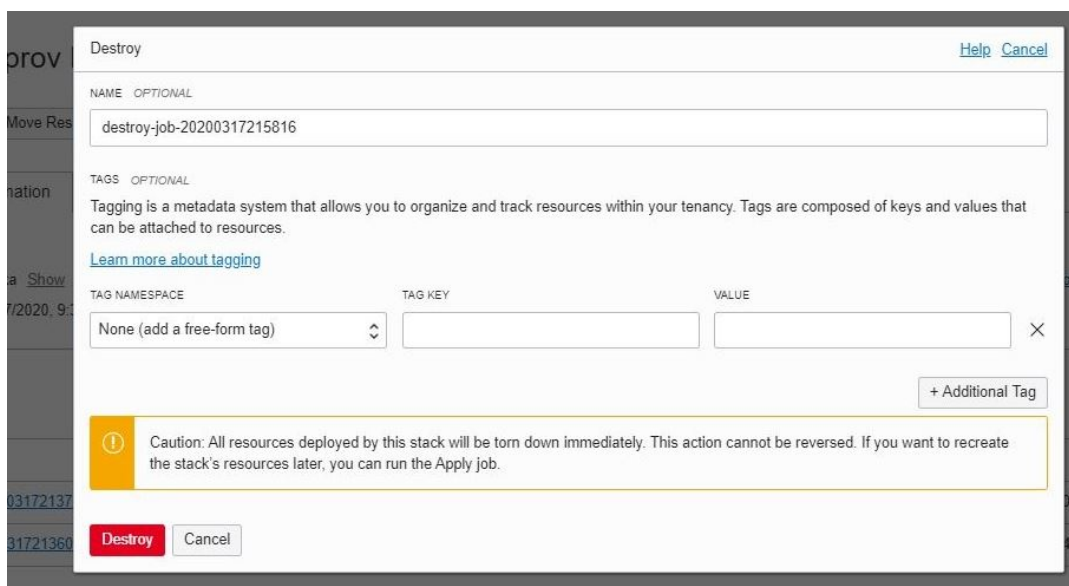
You can deprovision an Oracle SOA Suite on Marketplace instance using the Terraform Destroy action. Optionally, you can also delete the stack.

To deprovision an Oracle SOA Suite on Marketplace instance:

1. Go to the Stack Details page of the instance you want to deprovision, as described in [View Oracle SOA Suite on Marketplace 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:**

- Destroying the stack deletes compute instances and load balancers that were created using the stack.
- Deleting the stack deletes the associated jobs and the stack.
- 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.

## Perform Database Operations for an Oracle SOA Suite on Marketplace Instance

**Topics:**

- [Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database](#)
- [Discover the Default Database Schema Prefix and Password](#)
- [Change the Database Schema and Wallet Passwords](#)
- [Create a Data Source for an Oracle Autonomous Transaction Processing Database](#)
- [Unmount and Mount DBFS](#)

### Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database

**Best Practices:**

- This procedure is applicable only for Oracle SOA Suite on Marketplace instances, not for Oracle Managed File Transfer instances.
- Try these steps on a development or test environment before trying them on production servers.
- Initiate an on-demand backup to back up your Oracle SOA Suite domain.
- You should already have an Oracle SOA Suite environment provisioned with an Oracle Cloud Infrastructure native database.

To replace an existing Oracle Cloud Infrastructure database with a new Oracle Cloud Infrastructure database:

1. Create the new database from a backup of the existing database.
2. Identify the connect string of the existing database.

You can find the connect string using the WebLogic Server Administration Console. Go to **SOADDataSource** > **Configuration** tab > **Connection Pool** tab > **URL** field.

For example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=oldDB-scan.subnetname.vcnnname.oraclevcn.com)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=oldPDB.subnetname.vcnnname.oraclevcn.com)))
```

3. From the WebLogic Server Administration Console, stop the Administration Server and Managed Servers. See [Stop or Start WebLogic Servers](#).
4. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

5. Change to the `oracle` user:

```
sudo su - oracle
```

6. Identify all occurrences of the existing database connect string in your domain by using the `grep` command.

For example:

```
grep -rlw --exclude={*.txt,*.log,*.out} -e "olddb-
scan.subnetname.vcnnname.oraclevcn.com" SOATest_domain
```

7. Complete the following steps for all nodes of the Oracle SOA Suite cluster:
  - a. Back up the existing database connect string files. For example:

```
cp SOATest_domain/config/fmwconfig/jps-config-jse.xml SOATest_domain/
config/fmwconfig/jps-config-jse.xml_orig_date
cp SOATest_domain/config/fmwconfig/jps-config.xml SOATest_domain/config/
fmwconfig/jps-config.xml_orig_date
cp SOATest_domain/config/jdbc/ess-oracle-int-jdbc.xml SOATest_domain/
config/jdbc/ess-oracle-int-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/BamDataSource-mds-jdbc.xml SOATest_domain/
config/jdbc/BamDataSource-mds-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/BamDataSource-jdbc.xml SOATest_domain/
config/jdbc/BamDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/mds-ess-jdbc.xml SOATest_domain/config/
jdbc/mds-ess-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/ess-oracle-jdbc.xml SOATest_domain/config/
jdbc/ess-oracle-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/wlsbjmsrpDataSource-jdbc.xml
SOATest_domain/config/jdbc/wlsbjmsrpDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/mds-owsm-jdbc.xml SOATest_domain/config/
jdbc/mds-owsm-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/SOADDataSource-jdbc.xml SOATest_domain/
config/jdbc/SOADDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/LocalSvcTblDataSource-jdbc.xml
SOATest_domain/config/jdbc/LocalSvcTblDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/EDNLocalTxDataSource-jdbc.xml
SOATest_domain/config/jdbc/EDNLocalTxDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/opss-auditview-jdbc.xml SOATest_domain/
config/jdbc/opss-auditview-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/OraSDPMDDataSource-jdbc.xml SOATest_domain/
config/jdbc/OraSDPMDDataSource-jdbc.xml_orig_date
```

```

cp SOATest_domain/config/jdbc/EDNDataSource-jdbc.xml SOATest_domain/
config/jdbc/EDNDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/ess-oracle-xa-jdbc.xml SOATest_domain/
config/jdbc/ess-oracle-xa-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/BamNonJTADDataSource-jdbc.xml
SOATest_domain/config/jdbc/BamNonJTADDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/opss-audit-jdbc.xml SOATest_domain/config/
jdbc/opss-audit-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/WLSSchemaDataSource-jdbc.xml
SOATest_domain/config/jdbc/WLSSchemaDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/opss-datasource-jdbc.xml SOATest_domain/
config/jdbc/opss-datasource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/SOALocalTxDataSource-jdbc.xml
SOATest_domain/config/jdbc/SOALocalTxDataSource-jdbc.xml_orig_date
cp SOATest_domain/config/jdbc/mds-soa-jdbc.xml SOATest_domain/config/
jdbc/mds-soa-jdbc.xml_orig_date
cp SOATest_domain/dbfs/tnsnames.ora SOATest_domain/dbfs/
tnsnames.ora_orig_date

```

- b. Replace the existing database connect string with the new database connect string (newdb-scan):**

```

sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/fmwconfig/jps-
config-jse.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/fmwconfig/jps-
config.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/ess-
oracle-int-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
BamDataSource-mds-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
BamDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/mds-ess-
jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/ess-
oracle-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
wlsbjmsrpDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/mds-owsm-
jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
SOADatasource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
LocalSvcTblDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
EDNLocalTxDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/opss-
auditview-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
OraSDPMDatasource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
EDNDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/ess-
oracle-xa-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
BamNonJTADDataSource-jdbc.xml

```



```
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/opss-
audit-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
WLSSchemaDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/opss-
datasource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/
SOALocalTxDataSource-jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/config/jdbc/mds-soa-
jdbc.xml
sed -i 's/olddb-scan/newdb-scan/g' SOATest_domain/dbfs/tnsnames.ora
```

- c. If you use a different PDB name for the new database, then run the following command:

```
sed -i 's/oldPDB/newpdb/g' SOATest_domain/config/fmwconfig/jps-config-
jse.xml
```

8. Restart the Administration Server and Managed Servers. See [Stop or Start WebLogic Servers](#).
9. After restarting, confirm that your SOA servers connect to the new database. Your new connect string in the WebLogic Server Administration Console should look like this:  

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=newDB-scan.subnetname.vcnnam.oraclevcn.com)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=newPDB.subnetname.vcnnam.oraclevcn.com)))
```
10. Optionally, run the RCU utility to drop the old database schemas.

## Discover the Default Database Schema Prefix and Password

After provisioning, database schemas are created with a default prefix and password.

To find the default database schema and password:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user.

```
sudo su - oracle
```

3. Enter the following command:

```
python /opt/scripts/dbpassword.py
```

### Note:

The `dbpassword.py` script is available in `/opt/scripts/` for recently created instances. If this script is not found, contact your Oracle Support representative.

4. In the command output, note the default database schema prefix and password:

```
RCU Schema Prefix : prefix
```

RCU Schema Password : `password`

## Change the Database Schema and Wallet Passwords

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

When your password is about to expire, make sure that you update it to avoid the following password expiration scenarios:

- The following Oracle SOA Suite on Marketplace instance-specific datasources fail:
  - EDNDataSource
  - mds-owsm
  - EDNLocalTxDataSource
  - mds-soa
  - OraSDPMDDataSource
  - SOADDataSource
  - SOALocalTxDataSource
- The following non-Oracle SOA Suite on Marketplace 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 an instance. To change the password for schemas hosted in an *Application* database in your 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:

- [Update the Database Schema Password](#)
- [Update the DBFS Wallet Password](#)

## Update the Database Schema Password

When the database schema password expires, it must be updated. You can update the database schema password using an automation script or perform the steps manually.

- [Update the Database Schema Password Using an Automation Script](#)
- [Update the Database Schema Password Manually](#)

**Note:**

The database schema password must be same for all database schemas.

**Update the Database Schema Password Using an Automation Script**

**Prerequisite:** The Administration Server must be up and running.

To update the database schema password using an automation script:

1. Test database connectivity using the following `ping` command:

```
java -classpath /u01/app/oracle/middleware/wlserver/server/lib/
weblogic.jar
    utils.dbping ORACLE_THIN username password HOST:PORT:DBNAME
```

2. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

3. Change to the `oracle` user:

```
sudo su - oracle
```

4. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

5. Run the script to update the database schema password and respond to the prompts for WebLogic Server administration password, RCU schema prefix, and RCU password:

```
./updateDBPassword.sh
```

6. Update the wallet password. See [Update the DBFS Wallet Password](#).
7. Stop and then restart the Managed Servers. It is not necessary to stop and start the Oracle SOA Suite on Marketplace instance. See [Stop or Start the Managed Servers](#).

**Update the Database Schema Password Manually**

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

1. Test database connectivity using the following `ping` command:

```
java -classpath /u01/app/oracle/middleware/wlserver/server/lib/
weblogic.jar
    utils.dbping ORACLE_THIN username password HOST:PORT:DBNAME
```

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

4. If the WebLogic Servers are not running and the WebLogic Server Administration Console is inaccessible, manually update the passwords in the WebLogic Server configuration.
5. Update the bootstrap credentials using the WebLogic Scripting Tool (WLST).
6. Start the Administration Server with the Node Manager, and then start the Managed Servers.

To update the database schema password manually:

1. Update each infrastructure repository schema's password on the database deployment.  
If the schema prefix is already known, go to Step c.

- a. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user) and get the value of the schema prefix.

```
ssh -i private_key opc@AdminServerVM_IP_address
cat /u01/app/oracle/private/schemaPrefix
```

The schema prefix value returned is similar to the following:

```
SP255951777
```

- b. Use the `ssh` command to connect to the Oracle Cloud Infrastructure database deployment node (as the `opc` user) and change to the `oracle` user.

```
ssh -i ssh_key opc@DMVM_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. Update the password for the infrastructure repository schema users:

```
schema_prefix_DBFS
schema_prefix_ESS
schema_prefix_IAU
schema_prefix_IAU_APPEND
schema_prefix_IAU_VIEWER
schema_prefix_MDS
schema_prefix_OPSS
schema_prefix_SOAINFRA
schema_prefix_STB
schema_prefix_UMS
schema_prefix_WLS
```

*schema\_prefix\_WLS\_RUNTIME*

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

```
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.

```
ALTER USER schema_prefix_IUA 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. If the WebLogic Servers are running and the WebLogic Server Administration Console is accessible, update the password for all the corresponding data sources from the WebLogic Server Administration Console:
  - 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 Servers are not running and the WebLogic Server Administration Console is inaccessible, manually update the passwords in the WebLogic Server configuration:
  - a. Encrypt the new schema password and update the data source configuration files:

Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user), change to the `oracle` user, and go to the `domain_name` directory:

```
ssh -i private_key opc@AdminServerVM_IP_address
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
```

Run the `setDomainEnv` script:

```
. 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: new_password
```

- c.** Note the encrypted password output for future reference.

The following example shows an encrypted password:

```
AES}JHyrhOMB5hVRuDU/pV0qX86qz98ZV0xWXBSEAANA4Gs=
```

- 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:

```
EDNDataSource-jdbc.xml  
EDNLocalTxDataSource-jdbc.xml  
ess-oracle-int-jdbc.xml  
ess-oracle-jdbc.xml  
ess-oracle-xa-jdbc.xml  
LocalSvcTblDataSource-jdbc.xml  
mds-ess-jdbc.xml  
mds-owsm-jdbc.xml  
mds-soa-jdbc.xml  
opss-audit-jdbc.xml  
opss-auditview-jdbc.xml  
opss-datasource-jdbc.xml  
OraSDPMDDataSource-jdbc.xml  
SOADataSource-jdbc.xml  
SOALocalTxDataSource-jdbc.xml  
wlsbjmsrpDataSource-jdbc.xml
```

```
WLSSchemaDataSource-jdbc.xml
```

4. Update the bootstrap credentials with the new password for the `SCHEMA_PREFIX_OPSS` user using the WebLogic Scripting Tool (WLST):

- a. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user) and change to the `oracle` user:

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

- b. Start 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(jpsConfigFile='/u01/data/domains/
domain_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 Servers:

- a. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user) and change to the `oracle` user:

```
ssh -i private_key opc@AdminServerVM_IP_address
```

- 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 — Go to the `servers` directory and look for the server name ending in `adminserver`.

```
cd /u01/data/domains/domain_name/servers
```

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. 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**.
6. Update the wallet password. See [Update the DBFS Wallet Password](#).
7. Stop and then restart the Managed Servers. It is not necessary to stop and start the Oracle SOA Suite on Marketplace instance. See [Stop or Start the Managed Servers](#).

## Update the DBFS 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 regenerate the DBFS wallet with a new password. You can update the DBFS wallet password using an automation script or perform the steps manually.

- [Update the Wallet Password Using an Automation Script](#)
- [Update the Wallet Password Manually](#)

### Update the Wallet Password Using an Automation Script

To update the wallet password using an automation script:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@VM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

4. Run the script to update the DBFS wallet password and respond to the prompts RCU schema prefix and RCU password:

```
./updateDBFSWallet.sh
```

5. To verify if the wallet is updated with the new password, enter the following command:

```
$middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/  
domain_name/dbfs/wallet -listCredential
```

The output should list the DBFS user name and look as follows:

```
Oracle Secret Store Tool : Version 12.2.1.3.1  
Copyright (c) 2004, 2019, Oracle and/or its affiliates.  
All rights reserved.  
Enter wallet password:  
List credential (index: connect_string username)  
1: ORCL SP12944567290_DBFS
```



6. Repeat these steps on all nodes of the Managed Server.

### Update the Wallet Password Manually

To update the wallet password manually:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

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

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Go to the DBFS directory:

```
/u01/data/domains/domain_name/dbfs
```

4. Back up the old wallet:

```
mv wallet wallet_bckup
```

5. Create a new wallet directory:

```
mkdir wallet
```

6. Create a temp file to store the `prefix_DBFS` user credentials. For example:

```
vi /var/tmp/dbfsp
```

7. In the file, enter the new database credentials three times in the `dbfsp` file on three different lines.

```
ab#$12CDaf40f1c  
ab#$12CDaf40f1c  
ab#$12CDaf40f1c
```

If you need to find out the default database credentials, see [Discover the Default Database Schema Prefix and Password](#).

8. Save the file.

9. Enter the following commands to generate the Oracle Wallet at `/u01/data/domains/domain_name/dbfs`:

```
$middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/  
domain_name  
/dbfs/wallet -create < /var/tmp/dbfsp
```

 **Note:**

If you see the following exception, rerun the `mkstore` command from a new terminal:

```
Exception in thread "main" java.lang.UnsupportedClassVersionError:
oracle/security/pki/OracleSecretStoreTextUI : Unsupported
major.minor version 51.0 at
java.lang.ClassLoader.defineClass1(Native Method)
```

10. Enter the following commands to add the new credentials in the wallet. In this example, `SchemaPrefix_DBFS` is the DBFS user name:

```
$middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/
domain_name/dbfs/wallet
-createCredential ORCL SchemaPrefix_DBFS < /var/tmp/dbfsp
```

11. To verify if the wallet is updated with the new password, enter the following command:

```
$middleware_home/oracle_common/bin/mkstore -wrl /u01/data/domains/
domain_name/dbfs/wallet -listCredential
```

The output should list the DBFS user name and look as follows:

```
Oracle Secret Store Tool : Version 12.2.1.3.1
Copyright (c) 2004, 2019, Oracle and/or its affiliates.
All rights reserved.
Enter wallet password:
List credential (index: connect_string username)
1: ORCL SP12944567290_DBFS
```

12. Repeat these steps on all nodes of the Managed Server.

## Create a Data Source for an Oracle Autonomous Transaction Processing Database

Oracle WebLogic Server for OCI provides two utility scripts to help you create Oracle Autonomous Transaction Processing (ATP) data sources:

- A download script that downloads the ATP wallet files to a node
- A create script that creates the data source using the downloaded ATP wallet files and data source properties you provide

To run the scripts, you need to access the nodes in your WebLogic domain as the `opc` user. The scripts are located in `/opt/scripts/utills` and can only be run as the `oracle` user.

The ATP database must allow the WebLogic Server compute instances to access the database listen port (1521 by default). Update your access control list (ACL), if necessary. See [Security Tools for Serverless Deployments](#) in the Oracle Cloud Infrastructure documentation.

**Topics:**

- [Download the ATP Wallet](#)
- [Configure a Data Source for an ATP Database](#)

## Download the ATP Wallet

The download script unpacks and copies the ATP wallet contents to a node.

**Note:**

The download script must be run before the create script that configures a data source.

If the data source target is the domain cluster, you must run the download script on every node in the cluster. If the target is individual servers, then run the script on those servers.

You need the public IP address of each node on which you plan to run the download script. Find the IP address on the compute instance details page in the Oracle Cloud Infrastructure console. Look up the bastion's public IP address and the private IP address of a node if the WebLogic domain is in a private subnet.

1. Open an SSH connection to a node as the `opc` user.

```
ssh -i path_to_private_key opc@node_public_ip
```

Or,

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

2. Change to the `oracle` user.

```
sudo su oracle
```

3. Run the script `download_atp_wallet.sh` by providing the following parameters:

- OCID of the ATP database - You can find the OCID from the ATP database details page in the Oracle Cloud Infrastructure console.
- Password for the ATP wallet - The password must be at least 8 characters long, and includes at least 1 letter and either 1 numeric character or 1 special character.
- Path to save the extracted ATP wallet files - The path to a directory on the domain where the script saves the extracted ATP wallet files. For example:  
`/u01/data/domains/thestack_domain/config/atp`

The directory must be identical on every node where you run the script.

Command:

```
/opt/scripts/Utils/download_atp_wallet.sh atp_database_ocid  
atp_wallet_password path_to_extract_wallet_files
```

**Example:**

```
/opt/scripts/utils/download_atp_wallet.sh
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v password /u01/data/
domains/servicename_domain/config/atp
```

The download script creates a subdirectory in the path you provide using the ATP database OCID value. For example:

```
/u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v
```

Seven files are extracted to the subdirectory. The following is an example of the script response:

```
<Aug 22, 2020 10:39:50 PM GMT> <INFO> <oci_utils> <(host:servicename-
wls-0.subnet_dns_domain_name) - <WLSC-VM-INFO-001> ATP Wallet downloaded>
Archive: /tmp/atp_wallet.zip
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/cwallet.sso
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/tnsnames.ora
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/truststore.jks
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/ojdbc.properties
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/sqlnet.ora
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/ewallet.p12
  inflating: /u01/data/domains/servicename_domain/config/atp/
ocid1.autonomousdatabase.oc1.phx.alb2c3d4e56z7y8x9w10v/keystore.jks
```

4. Repeat steps 1 through 3 on each node where you have to run the download script. Depending on the data source target, run the download script on every node in the cluster or on individual servers.

## Configure a Data Source for an ATP Database

The create script configures a JDBC data source using the downloaded ATP wallet files and the data source properties you provide.

 **Notes:**

- The data source that you configure must not point to the SOAINFRA schema used to SOA servers to store metadata.
- To perform this task, you need Create Session permission (that is, GRANT CREATE SESSION TO ATPUSER).
- You must run the download script before you run the create script to configure the data source.

To configure a data source for an ATP database:

1. Open an SSH connection to any node as the `opc` user, then change to the `oracle` user.
2. Run the script `create_atp_datasource.sh` and follow user prompts:

```
/opt/scripts/utils/create_atp_datasource.sh
```

At each prompt, enter a value or press Enter to accept the default value. The following is an example of the script response after entering the values:

```
INFO: Found wallet config file
INFO: Verifying existing datasources.
INFO: Verified that no existing data source has the same name.
INFO: Created datasource configuration file /tmp/.ds_config
INFO: Creating the datasource ==> datasourcel
INFO: Connecting to the admin server [t3://servicename-wls-0:7001]...
INFO: Adding properties to datasource
INFO: Target Type : Server
INFO: Targets : servicename_server_1
INFO: Setting targets [[com.bea:Name=servicename_server_1,Type=Server]]
INFO: Successfully create datasource [datasourcel]
INFO: Validating the Datasource [datasourcel]
INFO: Verify datasource on Server AdminServer
-- Datasource datasourcel not found on server AdminServer.
INFO: Verify datasource on Server servicename_server_1
-- datasourcel:      State[Running] Connection Test is OK
```

## Unmount and Mount DBFS

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:

1. Set up your environment by running the following `export` commands:

```
export ORACLE_HOME=/u01/app/oracle/suite/dbclient
export LD_LIBRARY_PATH=/u01/app/oracle/suite/dbclient/lib
export TNS_ADMIN=/u01/data/domains/SOA_domain/dbfs
```

where `SOA_domain` is your domain name.

2. Unmount `dbfs` directories:

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

3. Mount `dbfs` directories and check trace log files to ensure there are no errors:

```
/u01/app/oracle/suite/dbclient/bin/dbfs_client -o wallet /@ORCL -o
direct_io /u01/soacs/dbfs_directio -otrace_file=/tmp/db1.txt
/u01/app/oracle/suite/dbclient/bin/dbfs_client -o wallet /@ORCL /u01/soacs/
dbfs -otrace_file=/tmp/db2.txt
```

These commands create the trace files in the `/tmp` directory.

#### 4. Verify the status of the mount directory again:

```
ls -ltr /u01/soamp
```

The output should look similar to:

```
drwxr-xr-x. 3 root  root    0 May 15 00:06 dbfs
drwxr-xr-x. 3 root  root    0 May 15 00:06 dbfs_directio
```

### Troubleshoot DBFS Mount Issues

If `dbfs` is still not mounted, perform the following checks:

- Check for error messages in the `/tmp` trace log files from the mount command.
- SSH to the database VM, connect to the DBFS schema as the `sys` user and make sure the `dbfs` user is not locked. If locked, then unlock the `dbfs` user:

```
sqlplus / as sysdba
alter session set container=pdb1;
SELECT username, account_status FROM dba_users;
ALTER USER prefix_DBFS IDENTIFIED BY password ACCOUNT UNLOCK;
```

- If the WebLogic Server VM is not able to connect to the database, SSH to the Administration Server VM or Managed Server node, then run the following `ping` command to test database connectivity:

```
java -classpath /u01/app/oracle/middleware/wlserver/server/lib/
weblogic.jar utils.dbping ORACLE_THIN username password HOST:PORT:DBNAME
```

- Run the following command to ensure there are no previous `dbfs` processes running:

```
ps -ef|grep dbfs
```

If there are any `dbfs` processes running, then kill the processes:

```
kill -9 DBFSpid
```

After troubleshooting the mounting issues, perform the following steps:

1. Repeat the mount commands.
2. Change to the `oracle` user:
 

```
sudo su - oracle
```
3. Enter the following command to confirm if `dbfs` is mounted correctly:
 

```
df -h
```

If correctly mounted, the output should look similar to:

```
/dev/mapper/vg_domain-lv_domain    50G  736M  46G   2% /u01/data/
domains
/dev/sdc2                          22G  324M  21G   2% /u01/app/
oracle/tools
/dev/mapper/vg_middleware-lv_middleware  24G  4.5G  18G  20% /u01/app/
oracle/middleware
/dev/mapper/vg_jdk-lv_jdk          3.9G  409M  3.3G  11% /u01/jdk
/dev/mapper/vg_suite-lv_suite      50G   53M  47G   1% /u01/app/
oracle/suite
```

```

dbfs-@ORCL:/          957M  120K  956M   1% /u01/soacs/
dbfs
dbfs-@ORCL:/          957M  120K  956M   1% /u01/soacs/
dbfs_directio

```

4. If mounts are still failing and you see the following error in the trace file output:

```

Unable to resolve ORA-12154: TNS:could not resolve the connect identifier
specified

```

A likely cause is there is no entry on `tnsnames` for `ORCL` in your DBFS client installation. To fix this, either use the correct name in `-o wallet /@NEWSID` from `tnsnames.ora` or make an entry for `ORCL` in `tnsnames.ora` of the DBFS client installation.

## Increase the Domain Volume Size Post-Provisioning

You can increase the domain volume size defined during provisioning of an instance. You cannot decrease the domain volume size.

The steps to increase the domain volume size include:

- Update the **Domain Volume Size (GB)** value using the Edit Stack wizard in the Oracle Cloud Infrastructure Console.
- Run the `resizeDomainVolume.sh` script to resize the mounted domain volume.

To increase the domain volume size:

1. Go to the Stack Details page of the instance for which you want to increase the domain volume size, as described in [View Oracle SOA Suite on Marketplace Instance Details](#).
2. On the Stack Details page, click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and select the In the Edit Stack wizard, increase the **Domain Volume Size (GB)** value as required.
4. Click **Next** to navigate to the Review page, then click **Save Changes**.
5. On the Stack Details page, click **Terraform Actions** and select **Plan**. In the Plan dialog, click **Plan**.
6. When the Terraform Plan job completes successfully, click **Terraform Actions** and select **Apply**. In the Apply dialog, click **Apply**.
7. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@Admin_VM_Public_IP
```

8. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

9. Run the script to resize the mounted domain volume as the `opc` user:

```
./resizeDomainVolume.sh
```

10. Confirm that the domain volume size is increased:

```
df -h
```

## Update the JVM Heap Size Parameter Values for Managed Servers

For improved performance, you may need to increase the JVM heap size for all Managed Servers in a cluster.



### Note:

After changing the JVM heap size, whenever there is a scale out operation, newly added nodes have default JVM heap size parameters. To update the newly added nodes with the new JVM heap size parameter values, you must follow these steps to rerun the automation script.

To update the JVM heap size parameters:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@Admin_VM_Public_IP
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Navigate to the directory containing automation scripts:

```
cd /opt/scripts/runbooks
```

4. Run the script to update the JVM heap size parameters and respond to the prompts for WebLogic Server administration password, Min JVM Heap Size, and Max JVM Heap Size:

```
./updateJVMHeapSizeParameters.sh
```

Example settings:

```
Min JVM Heap Size (MB): 1024
```

```
Max JVM Heap Size (MB): 4096
```

5. Restart the Managed Servers in the cluster for the updates JVM parameter values to take effect. See [Stop or Start the Managed Servers](#).

The JVM parameters are updated in the Managed Server startup parameters, which can be reviewed in the WebLogic Server Administration Console on the Server Start tab in the Arguments field. See [Servers : Configuration : Server Start](#) in the WebLogic Server Administration Console online help.

## Enable OS Management for Oracle SOA Suite on Marketplace Instances

To assist you with managing patches, Oracle SOA Suite on Marketplace supports the Oracle Cloud Infrastructure OS Management service.

OS Management offers the capability to view and install the available CPU fixes, security patches, and bug fixes on your compute instances. You can create instance groups and add all the nodes of a SOA cluster to a group and manage all the patches and updates of all the instances in the group. This can be done through the **OS Management** tab in the Oracle Cloud



Infrastructure Console. For more information, see [OS Management](#) in the Oracle Cloud Infrastructure documentation.

### Prerequisites

To prepare for enabling OS Management:

1. Create a dynamic group and add all your existing Oracle SOA Suite on Marketplace instances to this dynamic group. See [Managing Dynamic Groups](#) in the Oracle Cloud Infrastructure documentation.
2. Add the appropriate rules to add the Oracle SOA Suite on Marketplace instances to the dynamic group.
3. Create policies to grant the instances of the dynamic group to use OS Management:

```
ALLOW dynamic-group <dynamic_group_name> to use osms-managed-instances in
compartment <compartment_name>
ALLOW dynamic-group <dynamic_group_name> to read instance-family in
compartment <compartment_name>
```

4. (Optional) Create the following policy to grant OS Management to emit metrics:

```
ALLOW service osms to read instances in tenancy
```

5. To use the OS Management service on Oracle Linux 8 instances provisioned before 9 September 2020, you must manually install the OS Management Service Agent (`osms-agent`) using the following command:

```
sudo yum install osms-agent
```

For more information, see [To install the Agent in Oracle Linux 8 instances](#) in the Oracle Cloud Infrastructure documentation.

### Enable OS Management

To enable OS Management on Oracle SOA Suite on Marketplace instances:

1. If the Oracle SOA Suite on Marketplace instances were created before the policies under **Prerequisites** were added, you must restart the Oracle Cloud Agent on the VM:

- a. Use the `ssh` command to connect to the Linux VM as the `opc` user:

```
ssh -i private_key opc@VM_IP_address
```

- b. Enter the following command to restart the Oracle Cloud Agent:

```
sudo systemctl restart oracle-cloud-agent.service
```

2. Create managed instance groups as described in [Administering Managed Instance Groups](#) in the Oracle Cloud Infrastructure documentation.

Add all the compute instances of the SOA cluster in the managed instance group. You can apply patches and updates on all the nodes of the cluster in a single click, which ensures all the nodes of the cluster are in synch.

## Manage an Oracle SOA Suite on Marketplace Instance in Oracle Cloud Infrastructure

You can install and remove packages and software on the Linux operating system from the **OS Management** tab in the Oracle Cloud Infrastructure Console. You can install new patches and upgrades on individual SOA compute instances or an entire instance group (cluster) that you created.

You can schedule the upgrades to be run daily, weekly, or monthly to keep the operating system up to date.

# Perform a JNDI Lookup of JMS Resources Deployed on the Administration Server

For a Java client to perform a JNDI lookup of JMS resources deployed on the Administration Server, an SSH tunnel must be established between the client and the Administration Server that has a public IP address.

To perform a JNDI lookup of JMS resources:



### Note:

An SSH tunnel *cannot* be established between a client and a host that does not have a public IP address. This prevents a Java client from performing a JNDI lookup of JMS resources deployed on the servers.

1. Create an SSH tunnel to the Administration Server:

```
ssh -v -i opc_rsa -L 7001:AdminHostIP:7001 opc@AdminHostIP -N
```

where *AdminHostIP* is the IP address of the Administration Server.

2. Create an SSH tunnel to the Managed Server.

```
ssh -v -i opc_rsa -L 8001:MS1IP:8001 opc@MS1HOSTNAME -N
```

where *MS1IP* is the IP address of the Managed Server and *MS1HOSTNAME* is the host name of the Managed Server.

See [Creating an SSH Tunnel to a Port in the Virtual Machine](#).

## Unmount and Mount File Storage Service

You can use File Storage Service (FSS) as a shared file system while provisioning the Oracle SOA Suite on Marketplace instance created using the Oracle Autonomous Transaction Processing (ATP) database. The FSS is mounted in the same path as that of the DBFS mount, which is `/u01/soacs/dbfs/share`.

Execute the following commands, if you choose to configure the file storage in the provisioning UI.

## Unmount FSS

Run the following command as the `opc` user on the Oracle SOA Suite on Marketplace Virtual Machine (VM).

```
$ sudo umount /u01/soacs/dbfs/share
```

## Mount FSS

1. Verify if the status of the mount directory, `/u01/soacs/dbfs/share`, is empty.

```
$ cd /u01/soacs/dbfs/share  
$ ls -ltr
```

The output should look similar to:

```
total 0  
drwxrwxr-x. 2 oracle oracle  6 Jun  5 08:15 .  
drwxrwxr-x. 3 oracle oracle 19 Jun  5 08:15 ..
```

2. Run the following command as the `opc` user on the Oracle SOA Suite on Marketplace Virtual Machine (VM).

```
$ sudo /opt/scripts/fssMount.sh
```

# 7

## Secure an Oracle SOA Suite Instance

Oracle SOA Suite on Marketplace security includes configuring SSL and importing external web service certificates.

### Topics:

- [About Security in Oracle SOA Suite on Marketplace](#)
- [Set Up Oracle SOA Suite to Use CA-Verified SSL Certificates \(without load balancer\)](#)
- [Import Certificates of External Web Services with HTTPS in Oracle SOA Suite](#)

## About Security in Oracle SOA Suite on Marketplace

Learn how to secure applications deployed to your Oracle SOA Suite on Marketplace instance through the capabilities of Oracle Cloud and Oracle WebLogic Server.

An Oracle SOA Suite on Marketplace instance includes an Oracle WebLogic Server domain, which is comprised of an Administration Server and one or more Managed Servers. A domain also defines a security realm that controls authentication, authorization, role mapping, credential mapping and security auditing across all of the servers in the domain. Java applications deployed to this WebLogic Server domain can be associated with security roles and policies that protect the applications against unauthorized access. WebLogic Server supports various security providers that assign an identity to the requesting user. By default, users, groups, roles and policies are all maintained in WebLogic Server's embedded LDAP server.

To provide the highest level of network security, Oracle SOA Suite on Marketplace implements an "access by exception" architecture. You must explicitly grant network access to your service instance for administrators, application users or other cloud services. By default, a service instance is accessible only through secure protocols like HTTPS and SSH, and only using specific ports. You're also able to customize the default network security configuration to support different access rules and security policies.

## Set Up Oracle SOA Suite to Use CA-Verified SSL Certificates (without load balancer)

You can replace the identity and trust of Oracle SOA Suite with custom identity and custom trust and register the Oracle SOA Suite server with digital certificates procured from public certificate authorities like digicert or any other third party authority.

As a prerequisite, register Oracle SOA Suite domain with the public DNS for CA verification. For the documentation purposes, the public IP of the Oracle SOA Suite domain is registered with `mydomain.com` and takes the CA signed certificates from `mydomain`.

The Enterprise Manager (EM) console needs to be accessible using the public domain name.

### Topics:

- [Register a Domain Name for Oracle SOA Suite](#)

- [Create Custom Identity and Custom Trust Keystores and Generate a CSR](#)
- [Share the CSR with CA to Get CA-Signed Certificates](#)
- [Import CA Certificates](#)
- [Synchronize the Local Keystore with the Security Store](#)
- [Update WebLogic Keystores with Custom Identity and Trust](#)
- [Update the Node Manager and boot.properties File](#)
- [Verify the Environment](#)
- [Set Two-Way SSL Authentication](#)

## Register a Domain Name for Oracle SOA Suite

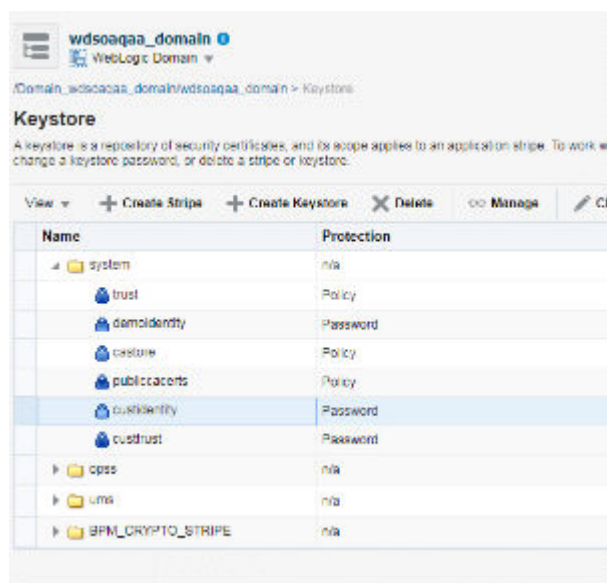
To register a domain name for Oracle SOA Suite:

1. Register a domain for Oracle SOA Suite server with a public DNS server. You can register your domain with any public DNS Server of your choice, mapping it to the public IP of Oracle SOA Suite. For example register `soacs.oraclecloud.co.in` domain in `mydomain.com`, mapping to the public IP of Oracle SOA Suite server.
2. Test access to the Enterprise Manager (EM) Console and the WebLogic Server Console through the domain name registered.

## Create Custom Identity and Custom Trust Keystores and Generate a CSR

To create custom identity and custom trust keystores and generate a Certificate Signing Request (CSR):

1. Log in to the Enterprise Manager (EM) Console and access the Keystores page by opening WebLogic domain > **Security** > **Keystore**.
2. Under the `system` stripe, click **Create Keystore**.
3. Provide the following details for custom identity:
  - a. **Keystore Name:** `custIdentity`
  - b. **Protection:** select the **Password** option
  - c. **Keystore Password:** enter the password
  - d. **Confirm Password:** reenter the password
4. Click **Create Keystore** to create another new keystore.
5. Provide the following details for custom trust:
  - a. **Keystore Name:** `custTrust`
  - b. **Protection:** select the **Password** option
  - c. **Keystore Password:** enter the password
  - d. **Confirm Password:** reenter the password



6. Click **Manage** on the `custIdentity` keystore name, click **Generate Keypair** to create a new key pair, and provide the following details:
  - a. **Alias Name:** `custIdentity`
  - b. **Common Name:** common name; for example, `soacs.mydomain.com` (domain name registered with public DNS)
  - c. **Organizational Unit:** name of the organizational unit
  - d. **Organization:** organization name
  - e. Enter City, State, and Country names
  - f. **Key Type:** RSA
  - g. **Key Size:** 2048
7. Click **OK** to generate the key pair.
8. Select the newly created key pair and click **Generate CSR**.
9. Export the created CSR, share it with Certificate Authority, such as digicert CA, and get **root**, **intermediate**, and **signed** certificates.

The certificate is generated for the domain name you specified in the **Common Name** field.

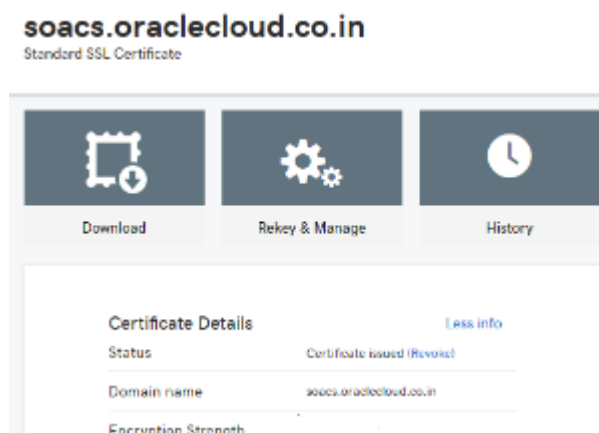
10. Download the certificates shared in the zip file from CA.

It is not mandatory to create identity and trust keystore under the `system` stripe that comes with Oracle SOA Cloud Service provisioning by default. You can create a new custom stripe and create identity and trust keystores under it.

## Share the CSR with CA to Get CA-Signed Certificates

To share the CSR with CA to get CA-signed certificates:

1. Select the new key pair you created under the `custIdentity` and click **Generate CSR**.
2. Export the created CSR and share it with the Certificate Authority and get root, intermediate, and signed certificates. The certificate is generated for the domain name you specified in the **Common Name** field.



3. Download the certificates shared in the zip file from the CA.  
The zip file contains either of the following:
  - the three certificates individually - root, intermediate, and signed certificates
  - two root and intermediate certificates in one chain and the signed certificate separately
4. Double-click the certificate chain for the root and intermediate certificates. You can see the full chain when you click on certification path.
5. Extract the root and intermediate certificates individually by going to the certification path, select the certificate to be extracted (root or intermediate), and click **View Certificate**.
6. In the View Certificates popup, select the **Details** tab and click **Copy to File**.
7. In the Certificate Export wizard, click **Next**, select **Base 64 encoded X.509 (CER)**, then click **Next**. Export the certificate.
8. Name the exported certificate as root and intermediate certificates respectively.

## Import CA Certificates

Certificate Authority (CA) certificates must be imported in the following order: first the signed server certificate, then the intermediate certificate, and then the root certificate.

To import CA certificates:

1. Use WLST commands to import the certificate chain into the identity keystore (custIdentity):
  - a. Combine the three certificates into a single text file called `chain.pem` in the following order: signed server certificate, followed by intermediate certificate, followed by root certificate:

```

-----BEGIN CERTIFICATE-----
<signed server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<root certificate>
-----END CERTIFICATE-----

```

- b. As the `opc` user, use an FTP client such as WinSCP to copy `chain.pem` to the `/tmp` directory of the Administration Server VM.
- c. Enter the following command to change the file ownership to the `oracle:oracle` user/group:

```
sudo chown oracle:oracle /tmp/chain.pem
```

- d. Use the `ssh` command to connect to the Administration Server VM:

```
ssh -i private_key opc@AdminServerVM_IP_address
```

- e. Change to the `oracle` user:

```
sudo su - oracle
```

- f. Start WLST and access the Oracle Platform Security Services (OPSS) key store service:

```
/u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh  
connect('username','password','t3s://SOACS_hostname:7002')  
svc = getOpssService(name='KeyStoreService')
```

 **Note:**

If connecting to port 7002 does not work, try port 9071 or 9074 with the `SOACS_hostname`, or alternatively the internal hostname (as reported by the `uname -n` command at the Linux prompt).

- g. Use the WLST `importKeyStoreCertificate` command to import `chain.pem`:

```
svc.importKeyStoreCertificate(appStripe='stripe', name='keystore',  
password='password', alias='alias', keypassword='keypassword',  
type='entrytype', filepath='absolute_file_path')
```

For example:

```
svc.importKeyStoreCertificate(appStripe='system', name='custIdentity',  
password=welcomel, alias='custIdentity', keypassword='welcomel',  
type='CertificateChain', filepath='/tmp/chain.pem')
```

- h. Exit WLST:

```
exit()
```

- 2. Use Oracle Enterprise Manager to import the certificate chain into the trust keystore (`custTrust`):
  - a. Log in to the Enterprise Manager Console and access the Keystores page by opening WebLogic domain > **Security** > **Keystore**.
  - b. Select the trust keystore (`custTrust`) and click **Manage**.
  - c. Click **Import Certificate** and import the certificates in this order:



- i. the signed server certificate as a trusted certificate (alias `mySignedCert`)
- ii. the intermediate certificate from CA as a trusted certificate (alias `myInterCA`)
- iii. the root certificate from CA as a trusted certificate (alias `myRootCA`)

3. Set up `cacerts`:

- a. Use the `ssh` command to connect to the Administration Server VM:

```
ssh -i private_key opc@AdminServerVM_IP_address
```

- b. Open `/u01/jdk/jre/lib/security`.

- c. Import the root and intermediate certificates into `cacerts` using the following commands:

```
keytool -import -keystore cacerts -storepass keystorepassword -file
rootCA.crt
keytool -import -keystore cacerts -storepass keystorepassword -file
interCA.crt
```

- d. Take a backup of the `cacerts` file for future use (for example, in case of JDK upgrade).

Whenever there is an upgrade in the JDK, the backup copy needs to be copied back after upgrade as `cacerts`. Since all the upgrades are handled automatically, this is a critical step and all the upgrades need to be tracked.

## Synchronize the Local Keystore with the Security Store

Synchronize keystores to synchronize information between the domain home and the Oracle Platform Security Services (OPSS) store in the database.

To synchronize keystores:

1. Use the `ssh` command to connect to the Administration Server VM:

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Start WLST and access the Oracle Platform Security Services (OPSS) key store service:

```
/u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh
connect('username','password','t3s://hostname:7002')
svc = getOpssService(name='KeyStoreService')
```

 **Note:**

If connecting to port 7002 does not work, try port 9071 or 9074 with the `hostname`, or alternatively the internal hostname (as reported by the `uname -n` command at the Linux prompt).

4. Enter the following commands to synchronize the custom identity and custom trust keystores:

 **Note:**

This step is necessary only if you are using the `system` stripe. You do not need to synchronize the keystores if you are using a custom stripe:

```
svc. listKeyStoreAliases (appStripe="system", name="custIdentity",  
password="*****", type="*")  
syncKeyStores (appStripe='system', keystoreFormat='KSS')  
svc. listKeyStoreAliases (appStripe="system", name="myKSSTrust",  
password='*****', type="*")  
syncKeyStores (appStripe='system', keystoreFormat='KSS')
```

## Update WebLogic Keystores with Custom Identity and Trust

To update the WebLogic keystores with custom identity and custom trust:

1. Log in to the WebLogic Server Administration Console.
2. Navigate to **Servers > Admin Server > Configurations > Keystores** tab.
3. Change the **Keystores** to **Custom Identity** and **Custom Trust** and **Save**.
4. Provide the values for **Custom Identity**:
  - **Custom Identity Keystore:** `kss://system/custidentity`
  - **Custom Identity KeyStore Type:** KSS
  - **Custom Identity PassPhrase:** enter the password given while creating the `custIdentity` keystore
  - **Confirm Custom Identity PassPhrase:** reenter the password
5. Provide the values for **Custom Trust**:
  - **Custom Trust Keystore:** `kss://system/custTrust`
  - **Custom Trust KeyStore Type:** KSS
  - **Custom Trust PassPhrase:** enter the password given while creating the `custIdentity` keystore
  - **Confirm Custom Trust PassPhrase:** reenter the password
6. Click **Save** and then activate changes.

Home > Summary of Servers > wdssoaqa\_adminserver > Summary of Servers > wdssoaqa\_server\_1

Settings for wdssoaqa\_server\_1

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Concurrency He

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define va

**Keystores:** Custom Identity and Custom Trust Change

**Identity**

**Custom Identity Keystore:** kss://system/custidentity

**Custom Identity Keystore Type:** KSS

**Custom Identity Keystore Passphrase:** .....

**Confirm Custom Identity Keystore Passphrase:** .....

**Trust**

**Custom Trust Keystore:** kss://system/custtrust

**Custom Trust Keystore Type:** KSS

**Custom Trust Keystore Passphrase:** .....

**Confirm Custom Trust Keystore Passphrase:** .....

Save

7. On the **SSL** tab, provide the following details:
  - **Private Key Alias:** `custIdentity` (this is the alias given while creating keypair in the `custIdentity` keystore)
  - **Private Key PassPhrase:** enter the password given while creating the key pair under the `custIdentity` keystore.
  - **Confirm Private Key PassPhrase:** reenter the password.
8. In the **Advanced** section, change **Hostname Verification** to **None**. Click **Save** and activate changes.
 

The Managed Server steps do not require a restart. Therefore, after activating the changes, you can check if the SSL URLs that open on Managed Server ports show the updated certificates.
9. Repeat steps 1 to 7 for the Administration Server. Administration Server changes require a restart.
10. Stop the Administration Server, Managed Server, and Node Manager.
 

Before restart, make sure that the Node Manager changes are done.

## Update the Node Manager and boot.properties File

To update the Node Manager and `boot.properties` file:

1. Access the Node Manager:

```
cd /u01/data/domains/DomainName/nodemanager
```

2. Edit `nodemanager.properties` and add the following properties:

```
# added for custom identity and custom trust
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityAlias=custIdentity
CustomIdentityKeyStoreFileName=kss://system/custIdentity
CustomIdentityKeyStorePassPhrase=*****
CustomIdentityKeyStoreType=KSS
CustomIdentityPrivateKeyPassPhrase=*****
CustomTrustKeyStoreFileName=kss://system/custTrust
```

3. Edit `startNodeManager.sh` under `/u01/data/domains/YourDomain/bin/` to add the following properties during startup in `JAVA_OPTIONS`:

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dweblogic.nodemanager.sslHostNameVerificationEnabled=false -
Djava.security.egd=file:/dev/./urandom"
```

The `JAVA_OPTIONS` for a 12.2.1.2 environment is as follows:

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Doracle.security.jps.config=/u01/data/domains/TPLSOADE_domain/config/
fmwconfig/jps-config-jse.xml
-Dcommon.components.home=/u01/app/oracle/middleware/oracle_common -
Dopss.version=12.2.1.2
-Dweblogic.nodemanager.sslHostNameVerificationEnabled=false -
Djava.security.egd=file:/dev/./urandom"
```

4. Use the `ssh` command to connect to the VM as the `opc` user:

```
ssh -i private_key opc@VM_IP_address
```

5. Change to the `oracle` user:

```
sudo su - oracle
```

6. Access the `boot.properties` file:

```
cd /u01/data/domains/YourDomain/servers/YourManagedServer/security
```

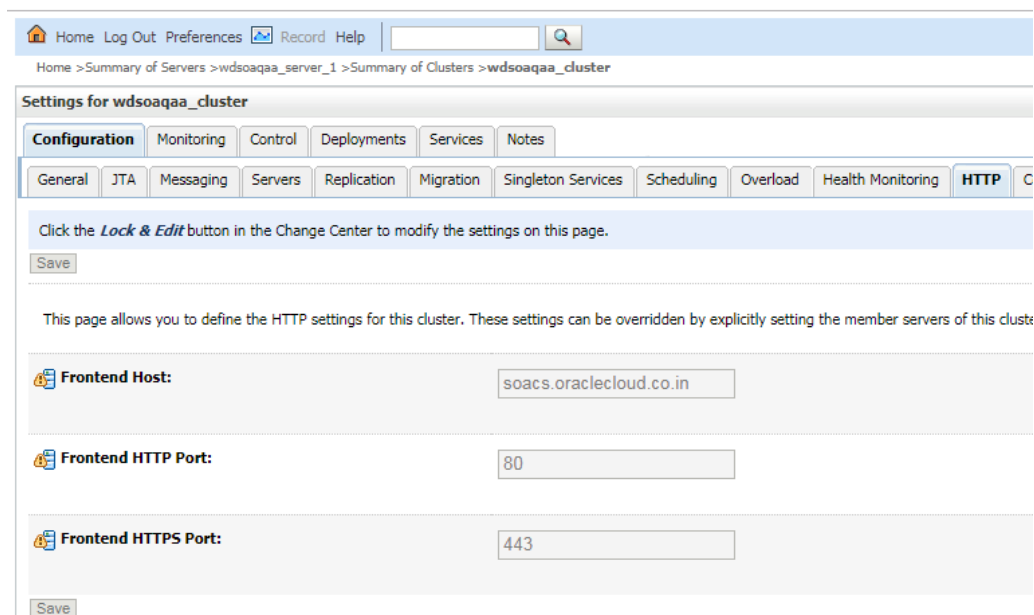
7. Take a backup of `boot.properties`.
8. Open `boot.properties` and comment the line `#TrustKeyStore=DemoTrust` (if present) and save.
9. Update the managedServer boot properties by accessing the `nodemanager`:

```
cd /u01/data/domains/YourDomain/servers/YourManagedServer/data/nodemanager
```

10. Take a backup of `boot.properties`.
11. Edit the `boot.properties` file, comment the line `#TrustKeyStore=DemoTrust`
12. Add the following lines at the end of `boot.properties` in the Managed Server:

```
CustomTrustKeyStoreFileName=kss://system/custTrust
TrustKeyStore=CustomTrust
CustomTrustKeyStorePassPhrase=****
CustomTrustKeyStoreType=KSS
```

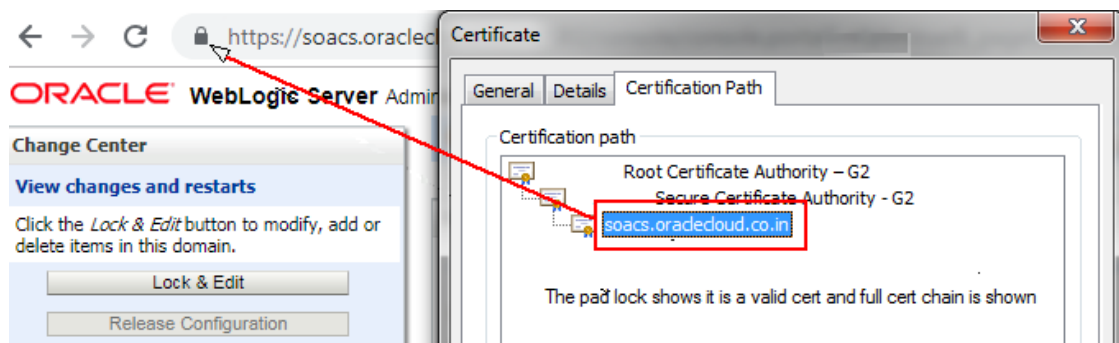
13. Save `boot.properties`.
14. To make changes in `SetDomainEnv.sh`, remove the following property:  
`Djavax.net.ssl.trustStore=%WL_HOME%\server\lib\DemoTrust.jks`
15. To update the **Frontend Host Port**, update the host and port in the WebLogic Server Console to reflect the domain name and ports:
  - a. In the WebLogic Server Console, navigate to **Environments > Clusters > Cluster Name > HTTP** tab.
  - b. Update the **Frontend Host** as the domain name.
  - c. Update the **Frontend HTTP Port**, default is port 80.
  - d. Update the **Frontend HTTPS Port**, default is port 443.



16. Start the Node Manager, Administration Server, and Managed Server, in this order.

## Verify the Environment

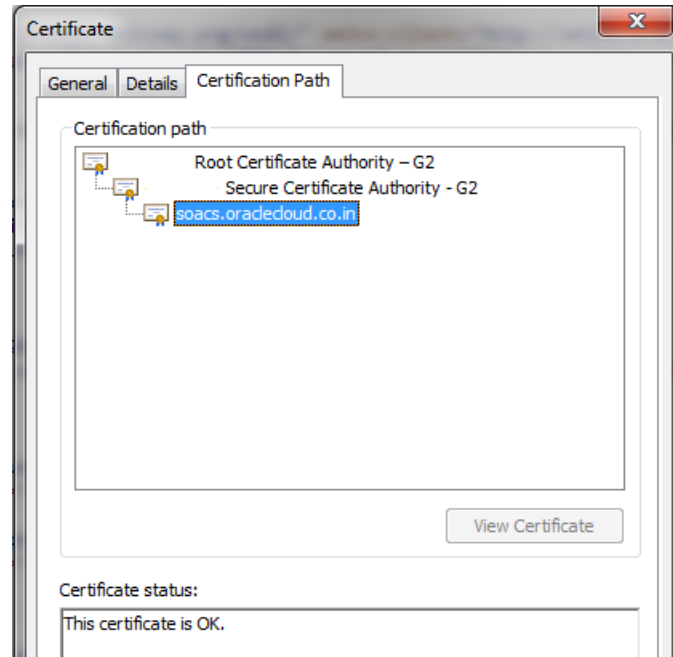
When you restart the environment, the Administration Server and Managed Server user interface shows the certificates as trusted:



To verify the environment:

1. Deploy a HelloWorld composite and verify that the client endpoint URL can be opened on https host and port.

The valid certificate chain is present on the client endpoint URL:



2. To invoke the client end point from any other composite, import all the certificates (signed server, intermediate, and root) present in the WSDL into the truststore of the server from where the parent composite is deployed.

## Set Two-Way SSL Authentication

Two-way SSL authentication creates a truststore and a keystore on both the client and the server. It is not mandatory to set the two-way authentication.

To set the two-way authentication:

1. Log in to the WebLogic Server Administration Console.
2. On the Managed Server, select the **SSL** tab and click **Advanced**.
3. Select **Lock and Edit**.
4. For **Two Way Client Cert Behavior**, select **Client Certs Requested and Enforced** from the drop-down list.
5. Click **Save** and activate the changes.

This change in the property does not require a WebLogic Server restart.

## Import Certificates of External Web Services with HTTPS in Oracle SOA Suite

To import the certificate chain, which prevents a `SSLHandshakeException` error from occurring while invoking an HTTPS service, complete the following steps:

- [Export the Certificate Chain of the HTTPS WSDL Called in Oracle SOA Suite](#)
- [Import the Certificate Chain of the HTTPS WSDL Called in the Oracle SOA Suite Trust Store](#)
- [Import the Certificate Chain of the HTTPS WSDL Called in the Java Trust Store](#)
- [Restart the Administration and Managed Servers](#)
- [Troubleshoot Issues](#)

## Export the Certificate Chain of the HTTPS WSDL Called in Oracle SOA Suite

To export the certificate chain of the HTTPS WSDL:

1. Open the HTTPS URL that is called from the Oracle SOA/Oracle Service Bus composite in the Firefox browser.
2. Click the **padlock** icon to the left of the URL.
3. Under **Secure Connection**, select **More Information**.
4. Go to the **Security** tab and click **View Certificates**.
5. In Certificate Viewer dialog, click the **Details** tab and select each certificate.
6. Click **Export**.  
Once the certificates are exported, you can use secure copy (SCP) to copy them onto the virtual machines where the Oracle SOA/Oracle Service Bus servers are running.

## Import the Certificate Chain of the HTTPS WSDL Called in the Oracle SOA Suite Trust Store

### Note:

In a multinode cluster, the certificate chain must be imported to the keystores on all nodes of the cluster.

To import the certificate chain of the HTTPS WSDL called in the Oracle SOA Suite trust store:

1. Check the `setDomainEnv.sh` file to see if you have a `DemoTrust.jks` entry in `EXTRA_JAVA_PROPERTIES` present under `DOMAIN_HOME`.
2. If a `DemoTrust.jks` entry exists, use the `keytool` command to import the certificates in the JKS-based trust store:

```
keytool -import -alias rootcrt1 -keystore
/u01/app/oracle/middleware/wlserver/server/lib/DemoTrust.jks -file
RootcertFile.crt -
storepass DemoTrustKeyStorePassPhrase
```

```
keytool -import -alias intercrt2 -keystore
/u01/app/oracle/middleware/wlserver/server/lib/DemoTrust.jks -file
```

```
InterMedCertFile.crt -
storepass DemoTrustKeyStorePassPhrase
```

```
keytool -import -alias cert3 -keystore
/u01/app/oracle/middleware/wlserver/server/lib/DemoTrust.jks -file
cert3file.crt -storepass
DemoTrustKeyStorePassPhrase
```

3. If a `DemoTrust.jks` entry does not exist, use Oracle Enterprise Manager Fusion Middleware Control to import certificates in the KSS-based trust store:
  - a. Go to the **Keystore > Weblogic Domain** drop down list, and select **Security > Keystore**.
  - b. In the navigation tree, click **trust**.
  - c. Click the **Manage** button.
  - d. Click the **Import** button.
  - e. In the Import Certificate dialog, select **Trusted Certificate** from the **Certificate Type** list.
  - f. Provide the root certificate you previously exported from the WSDL URL.
  - g. Repeat the same steps for other certificates in the WSDL URL chain.

Synchronizing the keystores copies the certificates from the central repository to the local domain file. Perform the following commands:

- a. Start WLST:

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

- b. Enter the administrator password and public IP address (the IP address used to access Oracle Enterprise Manager Fusion Middleware Control/Oracle WebLogic Server Console).

```
connect('username', 'password', 'admin-server-host:admin-server-port')
```

For example:

```
connect('weblogic', 'welcome', 't3s://public IP:7002')
```

- c. Run the following commands:

```
svc = getOpssService(name='KeyStoreService')
syncKeyStores(appStripe='system', keystoreFormat='KSS')
```



## Import the Certificate Chain of the HTTPS WSDL Called in the Java Trust Store



### Note:

In a multinode cluster, the certificate chain must be imported into the `cacerts` location on all nodes of the cluster.

To import the certificate chain of the HTTPS WSDL called in the Java trust store:

- Add the certificate chain into the `cacerts` location. Sample `keytool` commands for importing certificates into the `cacerts` location are as follows:

```
keytool -import -alias rootcrt1 -keystore /u01/jdk/jre/lib/security/  
cacerts -storepass changeit -file  
RootcertFile.crt
```

```
keytool -import -alias intercrt2 -keystore /u01/jdk/jre/lib/security/  
cacerts -storepass changeit -file  
InterMedCertFile.crt
```

```
keytool -import -alias cert3 -keystore /u01/jdk/jre/lib/security/cacerts -  
storepass changeit -file  
cert3file.crt
```

## Restart the Administration and Managed Servers

Restart the Administration Server and Managed Servers once the certificates are imported. This is required for both JKS- and KSS-based certificates. See [Stop or Start WebLogic Servers](#).

## Troubleshoot Issues

### Issue:

The following error occurs when invoking external Web Services:

```
Caused By: javax.xml.ws.WebServiceException: Could not determine wsdl ports.  
WSDLException: faultCode=PARSER_ERROR: Failed to read wsdl file at:  
https://abc.xxx.com/...Service?WSDL%22, caused by:  
java.security.NoSuchAlgorithmException: Error constructing implementation
```

### Workaround:

1. Back up `$DOMAIN_HOME/bin/setDomainEnv.sh`.

2. Edit `$DOMAIN_HOME/bin/setDomainEnv.sh` and remove the following entries:

```
-Djavax.net.ssl.trustStore=kss://system/xxx  
-Djavax.net.ssl.trustStoreType=kss
```

**Before:**

```
EXTRA_JAVA_PROPERTIES="-Djavax.net.ssl.trustStore=kss://system/xxx  
-Djavax.net.ssl.trustStoreType=kss ${EXTRA_JAVA_PROPERTIES}  
-Dsoa.archives.dir=${SOA_ORACLE_HOME}/soa  
...
```

**After:**

```
EXTRA_JAVA_PROPERTIES=" ${EXTRA_JAVA_PROPERTIES}  
-Dsoa.archives.dir=${SOA_ORACLE_HOME}/soa  
...
```

# 8

## Configure 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 on Marketplace instance. You can then configure the User Messaging Service to send emails to SSL-configured external mail servers using Oracle SOA Suite on Marketplace with Oracle Service Bus and Oracle B2B.

### Topics:

- [Configure User Messaging Service on a Cluster](#)
- [Configure Mail Sessions](#)

## Configure User Messaging Service on a Cluster

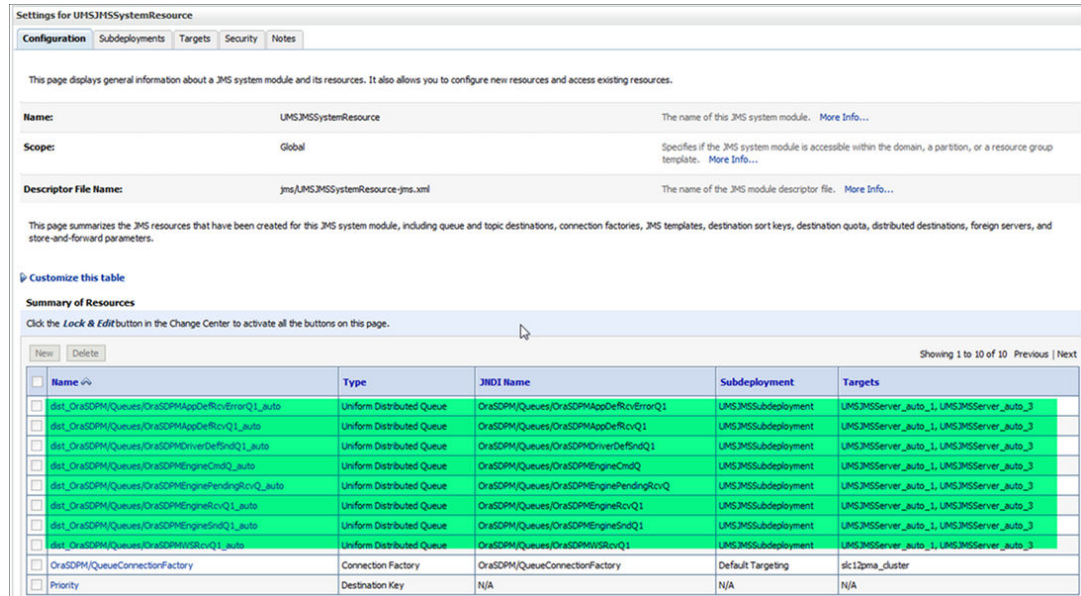
To configure email settings using User Messaging Service (UMS), UMS must be set up on your SOA servers and the UMS adapter configured for your Oracle SOA Suite on Marketplace instance.

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 [Create 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.

Queue Name	JNDI Name
dist_OraSDPM/Queues/ OraSDPMAAppDefRcvErrorQ1_auto	OraSDPM/Queues/OraSDPMAAppDefRcvErrorQ1
dist_OraSDPM/Queues/ OraSDPMAAppDefRcvQ1_auto	OraSDPM/Queues/OraSDPMAAppDefRcvQ1
dist_OraSDPM/Queues/ OraSDPMDriverDefSndQ1_auto	OraSDPM/Queues/OraSDPMDriverDefSndQ1
dist_OraSDPM/Queues/ OraSDPMEngineCmdQ_auto	OraSDPM/Queues/OraSDPMEngineCmdQ
dist_OraSDPM/Queues/ OraSDPMEnginePendingRcvQ_auto	OraSDPM/Queues/ OraSDPMEnginePendingRcvQ
dist_OraSDPM/Queues/ OraSDPMEngineRcvQ1_auto	OraSDPM/Queues/OraSDPMEngineRcvQ1

Queue Name	JNDI Name
dist_OraSDPM/Queues/ OraSDPMEngineSndQ1_auto	OraSDPM/Queues/OraSDPMEngineSndQ1
dist_OraSDPM/Queues/ OraSDPMWSRcvQ1_auto	OraSDPM/Queues/OraSDPMWSRcvQ1



8. Select the **UMSJMSSubdeployment** from the dropdown list. If the subdeployment is not created, follow the steps in [Create 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 [Deploy 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*.

## Create 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 [WebLogic Server Administration 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 [Create a Persistent Store](#) to create a persistent store.
5. Select a target for the UMS JMS server and save the changes.

**JMS Servers (Filtered - More Columns Exist)**

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New Delete Showing 1 to 13 of 13 Previous | Next

Name	Persistent Store	Target	Current Target	Health	Scope	Domain Partitions
BPMJMServer_auto_1	BPMJMSJDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
BPMJMServer_soacs_3	BPMJMSJDBCStore_soacs_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	
ProdMonJMServer_auto_1	ProdMonJMSJDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
ProdMonJMServer_soacs_3	ProdMonJMSJDBCStore_soacs_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	
SOAJMServer_auto_1	SOAJMSJDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
SOAJMServer_soacs_3	SOAJMSJDBCStore_soacs_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	
UMSJMServer_auto_1	UMSJMSJDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
UMSJMServer_auto_3	UMSJMSJDBCStore_auto_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	
wlbbJMServer	FileStore				OSBRuntimeResourceGroupTemplate template	
wlbbJMServer	FileStore				OSBTemplate template	
wlbbJMServer_auto_1	JDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
wlbbJMServer_soacs_3	wlbbJMSJDBCStore_soacs_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	
WseeJMServer_soacs_3	WseeJMSJDBCStore_soacs_3	slc12pma_server_3 (migratable)	slc12pma_server_3	OK	Global	

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

## Create 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**.

**Persistent Stores**

New Delete Showing 1 to 20 of 20 Previous | Next

Name	Type	Target	Scope	Domain Partitions
BPMJMSFileStore_auto_1	FileStore	slc12pma_server_1	Global	
BPMJMSJDBCStore_auto_1	JDBCStore	slc12pma_server_1 (migratable)	Global	
BPMJMSJDBCStore_soacs_3	JDBCStore	slc12pma_server_3 (migratable)	Global	
FileStore	FileStore		OSBRuntimeResourceGroupTemplate template	
FileStore	FileStore		OSBTemplate template	
FileStore_auto_1	FileStore	slc12pma_server_1 (migratable)	Global	
JDBCStore_auto_1	JDBCStore	slc12pma_server_1 (migratable)	Global	
nds-ess_MDS_DS	FileStore		Global	
nds-ovsm	FileStore		Global	
nds-soa	FileStore		Global	
ProdMonJMSFileStore_auto_1	FileStore	slc12pma_server_1 (migratable)	Global	
ProdMonJMSJDBCStore_auto_1	JDBCStore	slc12pma_server_1 (migratable)	Global	
ProdMonJMSJDBCStore_soacs_3	JDBCStore	slc12pma_server_3 (migratable)	Global	
SOAJMSFileStore_auto_1	FileStore	slc12pma_server_1	Global	
SOAJMSJDBCStore_auto_1	JDBCStore	slc12pma_server_1 (migratable)	Global	
SOAJMSJDBCStore_soacs_3	JDBCStore	slc12pma_server_3 (migratable)	Global	
UMSJMSJDBCStore_auto_1	JDBCStore	slc12pma_server_1 (migratable)	Global	
UMSJMSJDBCStore_auto_3	JDBCStore	slc12pma_server_3 (migratable)	Global	
wlbbJMSJDBCStore_soacs_3	JDBCStore	slc12pma_server_3 (migratable)	Global	
WseeJMSJDBCStore_soacs_3	JDBCStore	slc12pma_server_3 (migratable)	Global	

New Delete Showing 1 to 20 of 20 Previous | Next

Repeat the steps for other persistent stores based on the servers available in the cluster.

## Create 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**.

## Deploy 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 [Stop or Start WebLogic Servers](#).

<input type="checkbox"/>	SocketAdapter	Installed		Resource Adapter		Global
<input type="checkbox"/>	state-management-provider-memory-rar	Active	✔ OK	Resource Adapter	slc12pma_adminserver, slc12pma_cluster	Global
<input type="checkbox"/>	UMSAdapter	Active	✔ OK	Resource Adapter	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-apns	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-email	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-extension	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-gcm	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-mpmp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-twitter	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingdriver-xmpp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	usermessagingserver	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	worklistapp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
<input type="checkbox"/>	wsm-gm	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global

## Configure Mail Sessions

You can configure the User Messaging Service to send mails to SSL configure external mail servers using Oracle SOA Suite on Marketplace 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 on Marketplace instance and User Messaging Service to send mails, make a note of the yahoo mail server SSL settings.

Field	Value
Server	smtp.mail.yahoo.com
Port	465 or 587
Requires SSL	Yes
Requires TLS	Yes (if available)
Requires authentication	Yes

**Note:**

For Oracle SOA Suite on Marketplace 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:**

- [Import a CA-Issued SSL Certificate into the Oracle SOA Suite on Marketplace Instance](#)
- [Configure the Mail Driver for Outgoing Mails](#)
- [Update the Workflow Notification Properties](#)
- [Verify Mail Configuration Settings](#)

## Import a CA-Issued SSL Certificate into the Oracle SOA Suite on Marketplace 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 Administration Server node as an `oracle` user.
2. Run an `openssl` command for the yahoo mail server:

Mail Server	Command Used
Yahoo	<code>openssl s_client -connect smtp.mail.yahoo.com:465 &gt; yahocert.pem</code>
Office 365	<code>openssl s_client -showcerts -starttls smtp -crlf -connect smtp.office365.com:587</code>
Microsoft Outlook	<code>openssl s_client -showcerts -starttls smtp -connect smtp-mail.outlook.com:587</code>

Mail Server	Command Used
Gmail	<code>openssl s_client -connect smtp.gmail.com:465 &gt; gmail-smtp-cert.pem</code>

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:

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 Administration 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
```

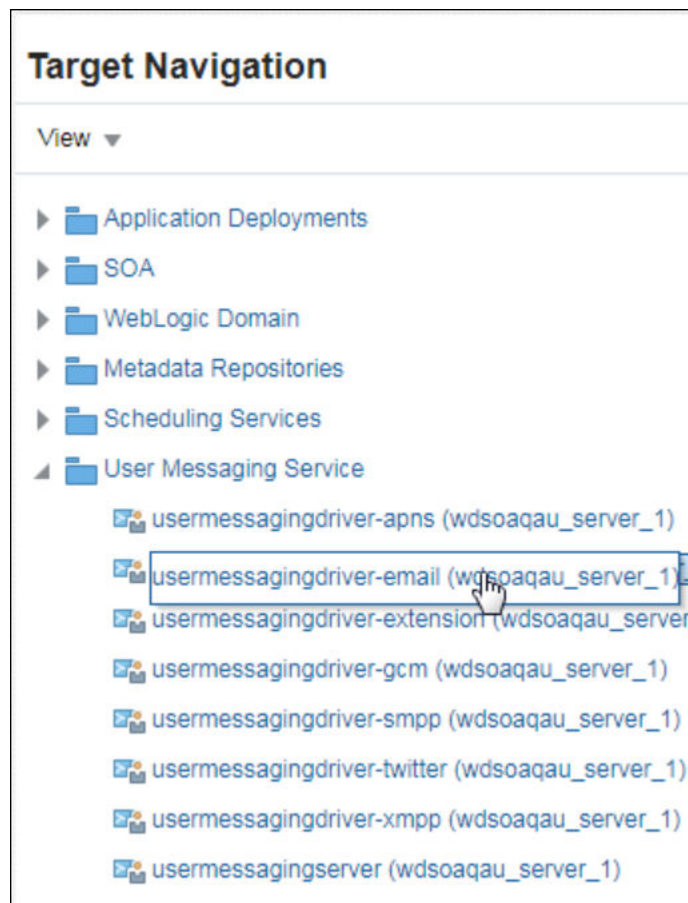
5. Stop and then restart the Administration Server and Managed Servers. See [Stop or Start WebLogic Servers](#).

## Configure 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:

Field	Value
Name	Email driver name. For example, yahooss1
Sender address	EMAIL: <i>YourMail@yahoo.com</i>
Capability	Send
EMAIL Receiving protocol	IMAP
Message Retrieval Frequency	30
Message Folder	INBOX
Outgoing mail Server port	smtp.mail.yahoo.com
Outgoing Mail Server port	465
Outgoing Mail Server Security	SSL
Outgoing Username	Your email user name which you give for authentication. For Office 365, test the driver settings to verify that your email use rname 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, myuser@mydomain.com.

Field	Value
Outgoing Password	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.
Enable SSL	Select this option

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

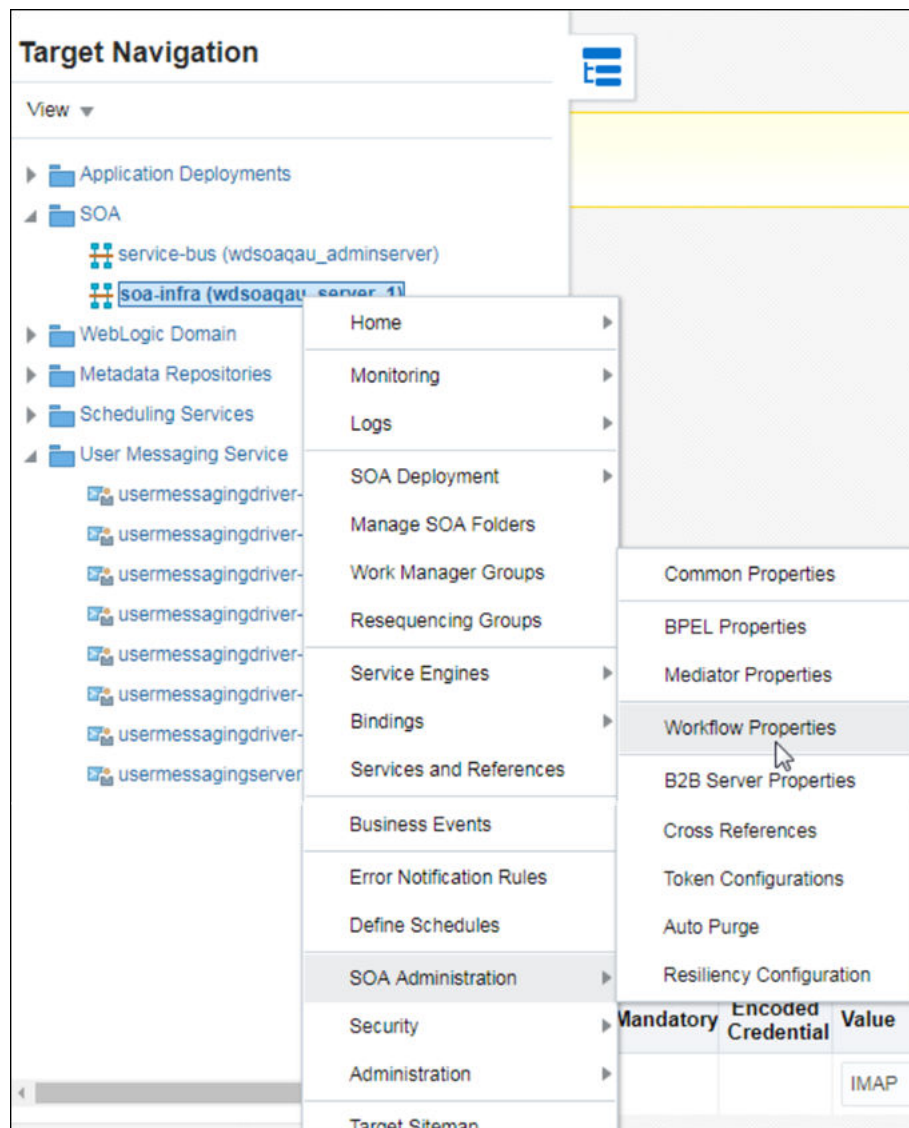
 **Note:**

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.

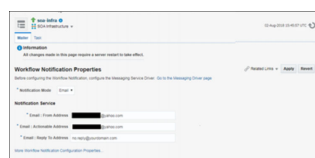
## Update the Workflow Notification Properties

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.



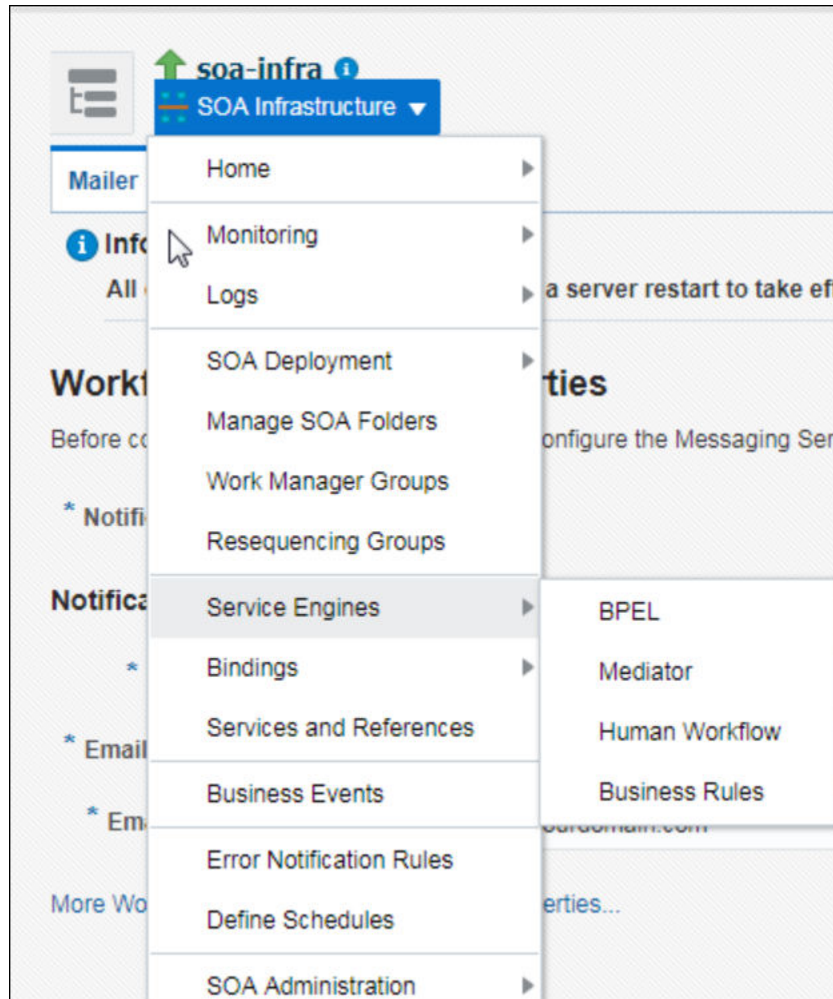
5. Click **Apply**.

## Verify Mail Configuration Settings

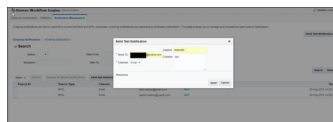
You can test your mail server configuration by sending a test mail.

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

# 9

## Troubleshoot Oracle SOA Suite on Marketplace

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



### Note:

To apply patches noted in this appendix, sign in to [My Oracle Support](#) and search for the patch numbers to locate and download the patches.

### Topics:

- [Find Diagnostic Information to Help with Troubleshooting](#)
- [Problems Using IDCS as the Authentication Provider](#)
- [Problems with Oracle Business Activity Monitoring \(BAM\)](#)
- [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](#)

## Find 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:

- [Use the WebLogic Server Administration Console to Find Diagnostic Information](#)
- [Use the WebLogic Server Administration Console to Find Log Files](#)

## Use 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. Log in to the [WebLogic Server Administration Console](#).
2. Under **Domains**, expand **Diagnostics**.
3. Click on the diagnostics that interests you.

For information on the diagnostic choices, click on **Diagnostics**.

## Use 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 [Access an Oracle SOA Suite on Marketplace 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 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 Using IDCS as the Authentication Provider

Oracle SOA Suite on Marketplace does not support Oracle Identity Cloud Service (IDCS), which provides identity management, Single Sign-On (SSO) and identity governance for applications.

For authentication, Oracle SOA Suite on Marketplace supports Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

## Problems with Oracle Business Activity Monitoring (BAM)

Problems related to the BAM Cluster service type in Oracle SOA Suite on Marketplace can occur.

The following issues are present in Oracle SOA Suite on Marketplace in a multinode BAM cluster environment:

- A BAM dashboard is blank, displaying no data.  
**Workaround:** Create and use ADF-based BAM dashboards. JET-based dashboards are not certified for a multinode BAM cluster.

- Time-based and KPI alerts do not trigger.  
This issue occurs when a node fails in a multinode BAM cluster.  
**Workaround:** None. As soon as all nodes are active again, all alerts will trigger.
- Data in BAM dashboards does not update.  
**Workaround:** Use a supported browser: Chrome or Internet Explorer 11+. Other browsers, such as Firefox, are not certified for a multinode BAM cluster.

The following issues are present in both Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure and Oracle SOA Suite on-premises:

- When creating a new Key Performance Indicator (KPI) in BAM Composer, if you change the Threshold value to a non-default value, then you may receive an error when you click **create message** or **select user**.  
**Workaround:** Apply patch 31466508.
- If JET-based business views are used in a BAM dashboard, then enabling active data will not reflect any changes made to data objects in the BAM dashboard.  
**Workaround:** None.
- Oracle SOA Suite does not support BAM time-based alerts associated with business queries.  
**Workaround:** Apply patch 30334074.

## 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

1. Sign in to the Worklist Application at `https://hostname:port/integration/worklistapp`.
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.

To correct this problem, follow the steps in [Update the Database Schema Password](#).

## 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 [Access 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 [Access 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. 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
```

4. Change the permission on the `/tmp/dbfswa.sh` script file.

```
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. Change to user `oracle`.

```
sudo su - oracle
```

2. Run the following commands:

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

3. ssh to the Administration Server VM.

```
ssh -i opc_rsa opc@AdminServer_IP
```

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

If you see the test file on VM 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`.

```
sudo su - oracle
```

3. Start `sqlplus`.

```
cd $ORACLE_HOME/bin  
./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:

1. From the WebLogic Domain drop-down menu, select Security — Security Realms.
2. Select **myrealm**.
3. Select Settings for Security Realm.
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
```

# A

## Patches Installed By Release

The bundle patches listed in this appendix are installed in instances provisioned with releases of Oracle SOA Suite on Marketplace.

When you provision a new instance, it contains all of the latest patches associated with the product. However, existing instances are not automatically updated with the latest bundle patches from subsequent releases. You are responsible for keeping the patch levels current. See [About Managing Patches for Instances Provisioned With Earlier Releases](#).

### Note:

- Oracle SOA Suite on Marketplace 23.2.2 and later versions support *SOA Stack Patch Bundles (SPBs)*.
- Oracle SOA Suite on Marketplace 23.1.1 or earlier versions do not support *SOA Stack Patch Bundles (SPBs)*. Use the *SOA bundle patch* instead of the SOA SPB to patch your existing Oracle SOA Suite on Marketplace instances.

### How to Determine What Patches are Installed

The list of patches is contained in a file on the Administration Server. You can also consult this appendix for a list of patches. To determine what patches are installed:

1. Use the `ssh` command to [connect to the Administration Server VM](#) (as the `opc` user):

```
ssh -i private_key opc@AdminServerVM_IP_address
```

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Enter the following command based on your Oracle SOA Suite on Marketplace instance version.

- For Oracle SOA Suite on Marketplace instances created on 23.2.2 and later versions:

```
/u01/app/oracle/middleware/OPatch/opatch lsinventory
```

- For Oracle SOA Suite on Marketplace instances created on 23.1.1 or earlier versions:

```
/u01/app/oracle/suite/OPatch/opatch lsinventory
```

### Patch Releases

- [Patches Applied During Provisioning — 24.1.2](#)
- [Patches Applied During Provisioning — 23.4.2](#)
- [Patches Applied During Provisioning — 23.3.2](#)

- [Patches Applied During Provisioning — 23.2.2](#)
- [Patches Applied During Provisioning — 23.1.1](#)
- [Patches Applied During Provisioning — 22.4.1 and 22.4.2](#)
- [Patches Applied During Provisioning — 22.3.1](#)
- [Patches Applied During Provisioning — 22.2.2.1 and 22.2.3.1](#)
- [Patches Applied During Provisioning — 22.1.2.1 and 22.2.1.1](#)
- [Patches Applied During Provisioning — 22.1.1.2](#)
- [Patches Applied During Provisioning — 21.4.5](#)
- [Patches Applied During Provisioning — 21.4.1 and 21.4.3](#)
- [Patches Applied During Provisioning — 21.3.2 and 21.3.2.1](#)
- [Patches Applied During Provisioning — 21.2.2 and 21.2.3](#)
- [Patches Applied During Provisioning — 21.2.1](#)
- [Patches Applied During Provisioning — 21.1.2 and 21.1.3](#)
- [Patches Applied During Provisioning — 21.1.1](#)
- [Patches Applied During Provisioning — 20.4.3](#)
- [Patches Applied During Provisioning — 20.4.2 and 20.4.2.1](#)
- [Patches Applied During Provisioning — 20.3.3 and 20.3.3.1](#)
- [Patches Applied During Provisioning — 20.3.2](#)
- [Patches Applied During Provisioning — 20.3.1.1](#)
- [Patches Applied During Provisioning — 20.3.1](#)
- [Patches Applied During Provisioning — 1.0.11.1](#)

## Patches Applied During Provisioning — 24.1.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 24.1.2.

**OEL Version:** Oracle-Linux-7.9-2024.01.23-0

**JDK Version:** 8.0.401

**Table A-1 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA Stack Patch Bundle	p36179936_122140_Generic.zip
SOA	p36038320_122140_Generic.zip
OSB	p35950186_122140_Generic.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-2 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-3 WebLogic Server**

Component	Bundle Names
ADF/JDev	p34809489_122140_Generic.zip

**Table A-4 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 23.4.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 23.4.2.

**OEL Version:** Oracle-Linux-7.9-2023.09.26-0

**JDK Version:** 8.0.391

**Table A-5 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA Stack Patch Bundle	p35908106_122140_Generic.zip
SOA	p35748499_122140_Generic.zip
OSB	p35815693_122140_Generic.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-6 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-7 WebLogic Server**

Component	Bundle Names
ADF/JDev	p34809489_122140_Generic.zip

**Table A-8 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 23.3.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 23.3.2.

**OEL Version:** Oracle-Linux-7.9-2023.07.31-1

**JDK Version:** 8.0.381

**Table A-9 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA Stack Patch Bundle	p35603170_122140_Generic.zip
SOA	p30922431_122140_Generic.zip
OSB	p35720109_12214230501_Generic.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-10 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-11 WebLogic Server**

Component	Bundle Names
ADF/JDev	p34809489_122140_Generic.zip

**Table A-12 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 23.2.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 23.2.2.

**OEL Version:** Oracle-Linux-7.9-2023.04.27-0



**JDK Version:** 8.0.371**Table A-13 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA Stack Patch Bundle	p35268643_122140_Generic.zip
SOA	p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip
ESS	p33351665_122140_Generic.zip

**Table A-14 MFT Cluster Service Type**

Component	Patch Names
MFT	p35305956_12214230404_Generic.zip p32463347_12214230404_Generic.zip p30686755_122140_Generic.zip

**Table A-15 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-16 WebLogic Server**

Component	Bundle Names
OVD	p33903365_122140_Generic.zip
EM	p34542329_122140_Generic.zip p34765492_122140_Generic.zip

**Table A-17 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 23.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 23.1.1.

**OEL Version:** Oracle-Linux-7.9-2023.01.31-2**JDK Version:** 8.0.361

**Table A-18 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA	p34824004_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip
ESS	p33351665_122140_Generic.zip

**Table A-19 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214220827_Generic.zip p32463347_12214220827_Generic.zip p30686755_122140_Generic.zip

**Table A-20 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-21 WebLogic Server**

Component	Bundle Names
WLS Stack Patch Bundle	p34974729_122140_Generic.zip
ADF/JDev	p34944256_122140_Generic.zip
OPSS	p33950717_122140_Generic-24677093.zip
OWSM	p34839859_122140_Generic.zip
OVD	p33903365_122140_Generic.zip
EM	p34542329_122140_Generic.zip p34765492_122140_Generic.zip
CIE	p34988073_122140_Generic.zip

**Table A-22 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 22.4.1 and 22.4.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 22.4.1 and 22.4.2.

**OEL Version:** Oracle-Linux-7.9-2022.10.04-0

**JDK Version:** 8.0.351

**Table A-23 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p34540715_122140_Generic.zip
	p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip
ESS	p33351665_122140_Generic.zip

**Table A-24 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214220827_Generic.zip
	p32463347_12214220827_Generic.zip
	p30686755_122140_Generic.zip

**Table A-25 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-26 WebLogic Server**

Component	Bundle Names
WLS Stack Patch Bundle	p34689215_122140_Generic.zip
	WLS: p34653267_122140_Generic.zip
	Coherence: p34545596_122140_Generic.zip
	RDA: p34546887_122140_Generic.zip
	ADR: p33639718_122140_Linux-x86-64.zip
FMW Platform:	p33093748_122140_Generic.zip
ADF/JDev	p34535558_122140_Generic.zip
OPSS	p33950717_122140_Generic-24677093.zip
OWSM	p34566592_122140_Generic.zip
FMW Thirdparty	p34604561_122140_Generic.zip
OVD	p33903365_122140_Generic.zip

**Table A-26 (Cont.) WebLogic Server**

Component	Bundle Names
EM	p34542329_122140_Generic.zip p34765492_122140_Generic.zip

**Table A-27 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 22.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 22.3.1.

**OEL Version:** Oracle-Linux-7.9-2022.06.30-0

**JDK Version:** 8.0.341

**Table A-28 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p34195608_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip
ESS	p33351665_122140_Generic.zip

**Table A-29 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214220520_Generic.zip p32463347_12214220520_Generic.zip p30686755_122140_Generic.zip

**Table A-30 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-31 WebLogic Server**

Component	Bundle Names
WLS Stack Patch Bundle	p34373563_122140_Generic.zip WLS: p34236279_122140_Generic.zip Coherence: p34248976_122140_Generic.zip RDA: p34212770_122140_Generic.zip ADR: p33639718_122140_Linux-x86-64.zip FMW Platform: p33093748_122140_Generic.zip
ADF/JDev	p34247006_122140_Generic.zip
OPSS	p33950717_122140_Generic-24677093.zip
OWSM	p34341032_122140_Generic.zip
FMW Thirdparty	p34287807_122140_Generic.zip
OVD	p33903365_122140_Generic.zip

**Table A-32 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 22.2.2.1 and 22.2.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 22.2.2.1 and 22.2.3.1.

**OEL Version:** Oracle-Linux-7.9-2022.04.26-0

**JDK Version:** 8.0.331

**Table A-33 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p33965482_122140_Generic-24684630.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip
ESS	p33351665_122140_Generic.zip

**Table A-34 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214220315_Generic.zip p32463347_12214220315_Generic.zip p30686755_122140_Generic.zip

**Table A-35 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-36 WebLogic Server**

Component	Bundle Names
WLS	p34012040_122140_Generic-24705947.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p33902201_122140_Generic-24662161.zip
ADF/JDev	p33958532_122140_Generic-24682001.zip
OPSS	p33950717_122140_Generic-24677093.zip
OWSM	p32905339_122140_Generic-24240122.zip
FMW Thirdparty Patches	p34044738_122140_Generic-24719205.zip

**Table A-37 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 22.1.2.1 and 22.2.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 22.1.2.1 and 22.2.1.1.

### OEL Version:

- 22.1.2: Oracle-Linux-7.9-2022.01.24-0
- 22.2.1: Oracle-Linux-7.9-2022.02.25-0

**JDK Version:** 8.0.321

**Table A-38 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p33696548_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p31192457_12214211221_Generic.zip p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-39 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214211221_Generic.zip p30686755_122140_Generic.zip p32463347_122140_Generic.zip

**Table A-40 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-41 WebLogic Server**

Component	Bundle Names
WLS	p33727616_122140_Generic.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p33591019_122140_Generic.zip
ADF/JDev	p33697227_122140_Generic.zip
OPSS	p32784652_122140_Generic-24182560.zip
OWSM	p32905339_122140_Generic-24240122.zip

**Table A-42 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 22.1.1.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 22.1.1.2.

**OEL Version:** Oracle-Linux-7.9-2021.12.08-0

**JDK Version:** 8.0.321

**Table A-43 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p33696548_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-44 MFT Cluster Service Type**

Component	Patch Names
MFT	p32395225_12214211221_Generic.zip p30686755_122140_Generic.zip p32463347_122140_Generic.zip

**Table A-45 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-46 WebLogic Server**

Component	Bundle Names
WLS	p33727616_122140_Generic.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p33591019_122140_Generic.zip
ADF/JDev	p33697227_122140_Generic.zip
OPSS	p32784652_122140_Generic-24182560.zip
OWSM	p32905339_122140_Generic-24240122.zip

**Table A-47 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 21.4.5

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.4.5.

**OEL Version:** Oracle-Linux-7.9-2021.10.20-0

**JDK Version:** 8.0.311



**Table A-48 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32957445_122140_Generic-24262864.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-49 MFT Cluster Service Type**

Component	Patch Names
MFT	p33672131_122140_Generic.zip p30686755_122140_Generic.zip p32395225_12214210602_Generic.zip p32463347_122140_Generic.zip

**Table A-50 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-51 WebLogic Server**

Component	Bundle Names
WLS	p33671996_12214210930_Generic.zip p33416868_122140_Generic-24444013.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p33286160_122140_Generic-24406034.zip
ADF/JDev	p33313802_122140_Generic-24409663.zip
OPSS	p32784652_122140_Generic-24182560.zip
OWSM	p32905339_122140_Generic-24240122.zip

**Table A-52 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 21.4.1 and 21.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.4.1 and 21.4.3.

**OEL Version:** Oracle-Linux-7.9-2021.10.04-0

**JDK Version:** 8.0.311**Table A-53 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32957445_122140_Generic-24262864.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-54 MFT Cluster Service Type**

Component	Patch Names
MFT	p30686755_122140_Generic.zip p32395225_12214210602_Generic.zip p32463347_122140_Generic.zip

**Table A-55 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-56 WebLogic Server**

Component	Bundle Names
WLS	p33416868_122140_Generic-24444013.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p33286160_122140_Generic-24406034.zip
ADF/JDev	p33313802_122140_Generic-24409663.zip
OPSS	p32784652_122140_Generic-24182560.zip
OWSM	p32905339_122140_Generic-24240122.zip

**Table A-57 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 21.3.2 and 21.3.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.3.2 and 21.3.2.1.

**OEL Version:** Oracle-Linux-7.9-2021.08.27-0**JDK Version:** 8.0.301

**Table A-58 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32957445_122140_Generic-24262864.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-59 MFT Cluster Service Type**

Component	Patch Names
MFT	p30686755_122140_Generic.zip p32395225_12214210602_Generic.zip p32463347_122140_Generic.zip

**Table A-60 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-61 WebLogic Server**

Component	Bundle Names
WLS	p33059296_122140_Generic-24309498.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p32973297_122140_Generic-24279604.zip
ADF/JDev	p33084721_122140_Generic-24321804.zip
OPSS	p32784652_122140_Generic-24182560.zip
OWSM	p32905339_122140_Generic-24240122.zip

**Table A-62 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 21.2.2 and 21.2.3

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.2.2 and 21.2.3.

**OEL Version:** Oracle-Linux-7.9-2021.05.12-0

**JDK Version:** 8.0.291

**Table A-63 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32656931_122140_Generic-24131129.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-64 MFT Cluster Service Type**

Component	Patch Names
MFT	p30686755_122140_Generic.zip p32395225_12214210319_Generic.zip p32463347_122140_Generic.zip

**Table A-65 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-66 WebLogic Server**

Component	Bundle Names
WLS	p32698246_122140_Generic-24165861.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p32581859_122140_Generic-24146474.zip
ADF/JDev	p32684757_122140_Generic-24154534.zip
OPSS	p32784652_122140_Generic-24182560.zip

**Table A-67 DBFS**

Component	Bundle Names
DBFS	p23273686_121020_Linux-x86-64.zip p31170082_12102160719ProactiveBP_Linux-x86-64.zip

## Patches Applied During Provisioning — 21.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.2.1.

**OEL Version:** Oracle-Linux-7.9-2021.04.09-0

**JDK Version:** 8.0.291

**Table A-68 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32656931_122140_Generic-24131129.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-69 MFT Cluster Service Type**

Component	Patch Names
MFT	p30686755_122140_Generic.zip p32395225_12214210319_Generic.zip p32463347_122140_Generic.zip

**Table A-70 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-71 WebLogic Server**

Component	Bundle Names
WLS	p32698246_122140_Generic-24165861.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p32581859_122140_Generic-24146474.zip
ADF/JDev	p32684757_122140_Generic-24154534.zip
OPSS	p32784652_122140_Generic-24182560.zip

## Patches Applied During Provisioning — 21.1.2 and 21.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.1.2 and 21.1.3.

### OEL Version:

- 21.1.2: Oracle-Linux-7.9-2021.01.12-0
- 21.1.3: Oracle-Linux-7.9-2021.03.17-0

**JDK Version:** 8.0.281

**Table A-72 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32337168_122140_Generic-23995890.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-73 MFT Cluster Service Type**

Component	Patch Names
MFT	p30686755_122140_Generic.zip p32395225_12214210102_Generic.zip p32463347_122140_Generic.zip

**Table A-74 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-75 WebLogic Server**

Component	Bundle Names
WLS	p32253037_122140_Generic-23959534.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p32124456_122140_Generic-23929885.zip
ADF/JDev	p32264996_122140_Generic-23963542.zip
OPSS	p31666198_122140_Generic-23725588.zip

## Patches Applied During Provisioning — 21.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 21.1.1.

**OEL Version:** Oracle-Linux-7.9-2021.01.12-0

**JDK Version:** 8.0.281

**Table A-76 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p32337168_122140_Generic-23995890.zip p30922431_122140_Generic.zip
OSB	p32121987_122140_Generic-23905468.zip

**Table A-76 (Cont.) SOA with SB & B2B Service Type**

Component	Bundle Names
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-77 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-78 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-79 WebLogic Server**

Component	Bundle Names
WLS	p32253037_122140_Generic-23959534.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p32124456_122140_Generic-23929885.zip
ADF/JDev	p32264996_122140_Generic-23963542.zip
OPSS	p31666198_122140_Generic-23725588.zip

## Patches Applied During Provisioning — 20.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.4.3.

**OEL Version:** Oracle-Linux-7.9-2020.12.16-0

**JDK Version:** 8.0.271

**Table A-80 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31903409_122140_Generic-23817000.zip p31799397_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p31700519_122140_Generic-23739907.zip p30549478_122140_Generic.zip
B2B	p31713053_122140_Linux-x86-64.zip

**Table A-81 MFT Cluster Service Type**

Component	Patch Names
MFT	p31381037_122140_Generic.zip p30686755_122140_Generic.zip

**Table A-82 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Names
BAM	p30334074_122140_Generic.zip p31799375_122140_Generic.zip

**Table A-83 WebLogic Server**

Component	Bundle Names
WLS	p32097167_12214201001_Generic-23892455.zip p31960985_122140_Generic-23842278.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p31806259_122140_Generic-23808394.zip
ADF/JDev	p31762739_122140_Generic-23765676.zip
OPSS	p31666198_122140_Generic-23725588.zip

## Patches Applied During Provisioning — 20.4.2 and 20.4.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.4.2 and 20.4.2.1.

**OEL Version:** Oracle-Linux-7.9-2020.10.26-0

**JDK Version:** 8.0.271

**Table A-84 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31903409_122140_Generic-23817000.zip p31799397_122140_Generic.zip p30922431_122140_Generic.zip
OSB	p31700519_122140_Generic-23739907.zip p30549478_122140_Generic.zip
B2B	p31713053_122140_Linux-x86-64.zip



**Table A-85 MFT Cluster Service Type**

Component	Patch Names
MFT	p31381037_122140_Generic.zip p30686755_122140_Generic.zip

**Table A-86 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Names
BAM	p30334074_122140_Generic.zip p31799375_122140_Generic.zip

**Table A-87 WebLogic Server**

Component	Bundle Names
WLS	p32097167_12214201001_Generic-23892455.zip p31960985_122140_Generic-23842278.zip p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p31806259_122140_Generic-23808394.zip
ADF/JDev	p31762739_122140_Generic-23765676.zip
OPSS	p31666198_122140_Generic-23725588.zip

## Patches Applied During Provisioning — 20.3.3 and 20.3.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.3.3 and 20.3.3.1.

**OEL Version:** Oracle-Linux-7.8-2020.08.26-0

**JDK Version:** 8.0.261

**Table A-88 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31396632_122140_Generic-23590093.zip p30922431_122140_Generic.zip
OSB	p30549478_122140_Generic.zip

**Table A-89 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-90 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-91 WebLogic Server**

Component	Bundle Names
WLS	p31537019_122140_Generic-23654622.zip
	p31544353_122140_Linux-x86-64-23673193.zip
Coherence	p31470730_122140_Generic-23658977.zip

## Patches Applied During Provisioning — 20.3.2

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.3.2.

**OEL Version:** Oracle-Linux-7.8-2020.08.26-0

**JDK Version:** 8.0.261

**Table A-92 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31396632_122140_Generic-23590093.zip
	p30922431_122140_Generic.zip
OSB	p30549478_122140_Generic.zip

**Table A-93 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-94 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-95 WebLogic Server**

Component	Bundle Names
WLS	p31537019_122140_Generic-23654622.zip
Coherence	p31470730_122140_Generic-23658977.zip

## Patches Applied During Provisioning — 20.3.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.3.1.1.

**OEL Version:** Oracle-Linux-7.8-2020.06.30-0

**JDK Version:** 8.0.261

**Table A-96 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31396632_122140_Generic-23590093.zip p30922431_122140_Generic.zip
OSB	p30549478_122140_Generic.zip

**Table A-97 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-98 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-99 WebLogic Server**

Component	Bundle Names
WLS	p31537019_122140_Generic-23654622.zip
Coherence	p31470730_122140_Generic-23658977.zip

## Patches Applied During Provisioning — 20.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 20.3.1.

**OEL Version:** Oracle-Linux-7.8-2020.06.30-0

**JDK Version:** 8.0.261

**Table A-100 SOA with SB & B2B Service Type**

Component	Bundle Names
SOA	p31396632_122140_Generic-23590093.zip p30922431_122140_Generic.zip p30549478_122140_Generic.zip

**Table A-101 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-102 BAM Cluster Service Type — 12.2.1.4.0**

Component	Patch Name
BAM	p30334074_122140_Generic.zip

**Table A-103 WebLogic Server**

Component	Bundle Names
WLS	p31537019_122140_Generic-23654622.zip
Coherence	p31470730_122140_Generic-23658977.zip

## Patches Applied During Provisioning — 1.0.11.1

The following patches are applied to instances when they are provisioned using Oracle SOA Suite on Marketplace 1.0.11.1.

**Table A-104 SOA with SB & B2B Cluster Service Type**

Component	Bundle Names
SOA	p30638101_122140_Generic.zip p30995852_122140_Generic-23427063.zip
OSB	p30549478_122140_Generic.zip

**Table A-105 MFT Cluster Service Type**

Component	Patch Name
MFT	p30686755_122140_Generic.zip

**Table A-106 BAM Cluster Service Type**

Component	Patch Names
BAM	p30334074_122140_Generic.zip p31047981_122140_Generic.zip

**Table A-107 WebLogic Server**

Component	Bundle Name
WLS	p30970477_122140_Generic-23416256.zip