

Oracle® Cloud

Administering Oracle SOA Cloud Service



F33533-39
November 2023



Oracle Cloud Administering Oracle SOA Cloud Service,

F33533-39

Copyright © 2015, 2023, 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, and MySQL 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

Preface

Audience	xi
Documentation Accessibility	xi
Diversity and Inclusion	xi
Related Resources	xi
Conventions	xii

1 What's New in Oracle SOA Cloud Service

2 Get Started with Oracle SOA Cloud Service

About Oracle SOA Cloud Service	2-1
About Platform Differences Between the On-Premises and Cloud Environments	2-2
About Oracle SOA Cloud Service Subscriptions and Licenses	2-4
About the Components of Oracle SOA Cloud Service	2-4
About Life Cycle Management of Oracle SOA Cloud Service Instances	2-7
Typical Workflow for Managing the Life Cycle of Oracle SOA Cloud Service Instances	2-8
About Oracle SOA Cloud Service Roles and User Accounts	2-10
SOA Administrator	2-10
Related Service Administrators	2-11
Service Instance Users	2-11
Oracle Cloud Infrastructure Policies	2-13
About Adapters for Oracle SOA Cloud Service	2-13
About the Oracle SOA Cloud Service User Interface	2-16
Explore the Oracle SOA Cloud Service Welcome Page	2-16
Explore the Oracle SOA Cloud Service Console	2-18
Explore the Oracle SOA Cloud Service Administration Page for Backups	2-21
Explore the Oracle SOA Cloud Service Administration Page for Patching	2-25
Explore the Oracle SOA Cloud Service Activity Page	2-26
Explore the Oracle SOA Cloud Service IP Reservations Page	2-27
About the Oracle SOA Cloud Service User Interface	2-28

About Oracle SOA Cloud Service Instances in Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic	2-39
About Managing Oracle SOA Cloud Service Instances	2-41
About Security	2-42
About Managing Patches for Instances Provisioned With Earlier Releases	2-44
About Oracle SOA Cloud Service Roles and Responsibilities between Oracle and Customer	2-46
About the Infrastructure Resources Used by Oracle SOA Cloud Service	2-47
About the Deployment Topology of Virtual Machines	2-47
About the Compute Nodes	2-49
About the Disk Volumes	2-50

3 Before You Begin

About Oracle SOA Cloud Service Architecture	3-1
About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure	3-1
Region	3-2
Availability Domain	3-2
Subnet	3-3
Software Release	3-3
Database	3-3
Backup Location	3-6
Load Balancer	3-6
About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure Classic	3-7
Region	3-8
IP Network	3-8
Software Release	3-9
User Authentication	3-9
Database	3-10
Backup Location	3-13
Load Balancer	3-13
Prerequisites	3-13
Prerequisites for Oracle Cloud Infrastructure	3-13
Create Infrastructure Resources	3-14
Configure Security Lists	3-15
Generate a Secure Shell (SSH) Public/Private Key Pair	3-16
Create an Oracle Database for Oracle SOA Cloud Service in Oracle Cloud Infrastructure	3-19
Prerequisites for Oracle Cloud Infrastructure Classic	3-23
Access the Oracle SOA Cloud Service Console	3-24

4 Provision an Oracle SOA Cloud Service Instance

About Provisioning an Oracle SOA Cloud Service Instance	4-1
Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure	4-2
Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure	4-3
Start the Provisioning Wizard	4-3
Specify Basic Service Instance Information	4-3
Specify the Service Instance Details	4-7
Provision an Oracle SOA Cloud Service Instance Using the REST API	4-14
Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet on Oracle Cloud Infrastructure	4-14
Create the Required Resources in Oracle Cloud Infrastructure	4-15
Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet	4-17
Post-Provisioning Tasks in Oracle Cloud Infrastructure	4-21
Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure	4-21
Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure	4-23
Register a Custom Domain Name with a Third-Party Registration Vendor	4-27
Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory	4-28
Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure Classic	4-28
Reserve IP Addresses for Oracle Database Exadata Cloud Service When Region Not Enabled	4-29
Create and Manage IP Reservations	4-30
Create an IP Reservation	4-31
Delete an IP Reservation	4-32
Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic	4-32
Provision Oracle SOA Cloud Service on an IP Network	4-35
Provision an Oracle SOA Cloud Service Instance with Stack Manager	4-37
Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure Classic	4-41
Start the Provisioning Wizard	4-41
Specify Basic Service Instance Information	4-41
Specify the Service Instance Details	4-47
Confirm Your Selections	4-54
Post-Provisioning Tasks in Oracle Cloud Infrastructure Classic	4-55
Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure Classic	4-55
Configure VPN as a Service on Oracle Cloud Infrastructure Classic	4-57
Register a Custom Domain Name with a Third-Party Registration Vendor	4-60
Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory	4-61

5 Deploy Applications to an Oracle SOA Cloud Service Instance

Deploy and Undeploy Applications to an Oracle SOA Cloud Service Instance	5-1
Use Oracle JDeveloper to Deploy an Application	5-1
Add an Ingress/Access Rule to Allow the JDeveloper Connection	5-2
Create an Application Server Connection in JDeveloper	5-5
Deploy a SOA Composite Application to Oracle SOA Cloud Service from JDeveloper	5-9
Deploy an Oracle Service Bus Application to Oracle SOA Cloud Service from JDeveloper	5-12
Use Oracle Enterprise Manager Fusion Middleware Control to Deploy an Application	5-14
Add a Managed Server IP in a Non-Proxy Host to Enable Deployment from Fusion Middleware Control	5-14
Use the WebLogic Server Administration Console to Deploy and Undeploy an Application	5-17
Use the WebLogic Server Administration Console to Deploy an Application	5-17
Use the WebLogic Server Administration Console to Undeploy an Application	5-18
Use WLST Commands to Deploy and Undeploy an Application	5-18
Access an Application Deployed to an Oracle SOA Cloud Service Instance	5-19
Use a Shared File System	5-20
Use an OTD Host Name with an Oracle Service Bus Business Service	5-21
Connect to MFT Embedded Servers Using Oracle Traffic Director	5-21
Access the WSDL of a Composite Deployed to a SOA Server	5-22
Use the Frontend Host and HTTPS Port Values in the WSDL URL for Inbound Cloud Adapters	5-23

6 Administer Oracle SOA Cloud Service

Administer the Load Balancer for an Oracle SOA Cloud Service Instance	6-1
Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning	6-2
Configure an Oracle Traffic Director Load Balancer During Provisioning or Post-Provisioning	6-13
About Oracle Traffic Director Load Balancer Virtual Machines	6-13
Add an Oracle Traffic Director Load Balancer to an Oracle SOA Cloud Service Instance Post-Provisioning	6-13
Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance	6-17
Remove the Oracle Traffic Director Load Balancer from an Oracle SOA Cloud Service Instance	6-18
Access an Oracle SOA Cloud Service Instance After Provisioning	6-19
Access an Administration Console for Software that a Service Instance Is Running	6-19
Access a VM Through a Secure Shell (SSH)	6-20
Connect to the Administration Server or Load Balancer VM	6-21
Connect to a Managed Server VM	6-22

Create an SSH Tunnel	6-24
Switch VM Users	6-27
Add an SSH Public Key	6-28
Access a VM Through Virtual Network Computing (VNC)	6-28
Access a VM Through PuTTY	6-30
Run WLST Commands on a VM	6-31
Perform Lifecycle Operations on an Oracle SOA Cloud Service Instance	6-32
Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs	6-33
About Stopping or Starting an Oracle SOA Cloud Service Instance and Individual VMs	6-33
Stop, Start, or Restart an Oracle SOA Cloud Service Instance	6-34
Restart the Administration Server VM	6-35
Stop, Start, or Restart Managed Server and Load Balancer VMs	6-35
Stop or Start WebLogic Servers	6-35
Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance	6-38
Scale an Oracle SOA Cloud Service Instance	6-38
Scale Out or In	6-39
Scale Up or Down	6-43
View Scaling Requests	6-46
Add Storage to a Node	6-46
Manage Tags for a Service Instance	6-48
Create, Assign, and Unassign Tags	6-48
Find Tags and Instances Using Search Expressions	6-48
Change the License Type for an Oracle SOA Cloud Service Instance	6-51
Back Up and Restore an Oracle SOA Cloud Service Instance	6-52
About Backup and Restoration of Oracle SOA Cloud Service Instances	6-52
Typical Workflow for Backing Up and Restoring an Oracle SOA Cloud Service Instance	6-57
Update Backup and Recovery Credentials	6-58
Configure Automated Backups for an Oracle SOA Cloud Service Instance	6-60
Disable Backups for an Oracle SOA Cloud Service Instance	6-62
Disable Coordinated Backups for an Oracle SOA Cloud Service Instance	6-62
Delete a Backup	6-63
Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance	6-63
Restore an Oracle SOA Cloud Service Instance from a Backup	6-65
Return an Oracle SOA Cloud Service Instance to Service After Restoration from a Backup	6-66
Delete an Oracle SOA Cloud Service Instance	6-67
Perform a JNDI Lookup of JMS Resources Deployed on the Administration Server	6-68
Change JVM Heap Size Settings	6-69
Perform Database Operations for an Oracle SOA Cloud Service Instance	6-69

Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database	6-70
Tune the Database Parameters	6-73
Discover the Default Database Password	6-75
Change the Database Schema and Wallet Passwords	6-75
Change the Database Schema Password Using the Oracle SOA Cloud Service Console	6-77
Change the Database Schema Password Manually	6-78
Update the DBFS Wallet Password	6-84
Unmount and Mount DBFS	6-85
Configure User Messaging Service on a Cluster	6-87
Create the User Messaging Service JMS Server	6-89
Create a Persistent Store	6-89
Create a Subdeployment	6-90
Deploy a User Messaging Service Adapter	6-90
Configure Mail Sessions	6-91
Import a CA-Issued SSL Certificate into the Oracle SOA Cloud Service Instance	6-92
Configure the Mail Driver for Outgoing Mails	6-93
Update the Workflow Notification Properties	6-95
Verify Mail Configuration Settings	6-96

7 Secure an Oracle SOA Cloud Service Instance

About Security in Oracle SOA Cloud Service	7-1
About Authenticating Users	7-1
About Users in Oracle SOA Cloud Service	7-2
About Authentication Options	7-4
Manage Passwords for Oracle SOA Cloud Service	7-5
Relocate Oracle SOA Cloud Service to a Different Identity Domain	7-8
Configure Network Security	7-9
About the Default Access Ports	7-9
Manage Access Rules for an Oracle SOA Cloud Service Instance	7-11
Manage Access Rules for Instances in Oracle Cloud Infrastructure	7-11
Manage Access Rules for Instances in Oracle Cloud Infrastructure Classic	7-13
Enable HTTP Access to an Oracle SOA Cloud Service Instance	7-15
Enable the HTTP Port on the Load Balancer	7-15
Create an Access Rule for the HTTP Port	7-16
Enable Communication Between Oracle SOA Cloud Service Instances	7-17
Configure SSL for an Oracle SOA Cloud Service Instance	7-18
Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates (with OTD)	7-18
Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates (non-OTD)	7-22

8 Troubleshoot Oracle SOA Cloud Service

Find Diagnostic Information to Help with Troubleshooting	8-1
Use the WebLogic Server Administration Console to Find Diagnostic Information	8-2
Use the WebLogic Server Administration Console to Find Log Files	8-2
Find Status Messages for Oracle SOA Cloud Service Instances	8-2
Problems Using IDCS as the Authentication Provider	8-3
Problems with Creating Service Instances	8-3
Problems with Deploying and Accessing Applications	8-6
Problems with Failure of a Running Service When the Schema User Password Expires	8-7
Problems with Scaling	8-7
Problems with Patching and Rollback	8-8
Problems with Backup and Restoration	8-9
Problems with Restart	8-11
Problems with Connectivity	8-12
Problems with the Node Manager	8-12
Problems with Database File System Mounting on Second Managed Server Node	8-14
Problems with a Database Deployment	8-15
Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control	8-16
Problems Adding Block Storage to an Existing Oracle SOA Cloud Service	8-17
Problems with Oracle Traffic Director Timing Out	8-17

A Patches Installed By Release

Patches Applied During Provisioning — 23.3.1	A-3
Patches Applied During Provisioning — 23.2.2	A-4
Patches Applied During Provisioning — 23.1.1 and 23.1.3	A-5
Patches Applied During Provisioning — 22.4.2	A-6
Patches Applied During Provisioning — 22.3.3	A-7
Patches Applied During Provisioning — 22.1.3	A-9
Patches Applied During Provisioning — 22.1.1	A-10
Patches Applied During Provisioning — 21.4.3	A-11
Patches Applied During Provisioning — 21.3.2 and 21.4.1	A-12
Patches Applied During Provisioning — 21.2.1	A-13
Patches Applied During Provisioning — 21.1.1	A-14
Patches Applied During Provisioning — 20.4.1	A-15
Patches Applied During Provisioning — 20.3.1	A-16
Patches Applied During Provisioning — 20.2.3	A-17
Patches Applied During Provisioning — 20.2.1	A-18

Patches Applied During Provisioning — 19.4.3	A-19
Patches Applied During Provisioning — 19.4.1	A-20
Patches Applied During Provisioning — 19.3.2	A-20
Patches Applied During Provisioning — 19.2.2	A-21
Patches Applied During Provisioning — 19.2.1	A-22
Patches Applied During Provisioning — 19.1.5	A-27
Patches Applied During Provisioning — 19.1.3	A-32
Patches Applied During Provisioning — 18.4.5	A-37
Patches Applied During Provisioning — 18.4.3	A-42
Patches Applied During Provisioning — 18.3.5	A-47
Patches Applied During Provisioning — 18.3.3	A-51
Patches Applied During Provisioning — 18.3.1	A-56
Patches Applied During Provisioning — 18.2.5	A-60
Patches Applied During Provisioning — 18.2.3	A-65
Patches Applied During Provisioning — 18.2.1	A-69
Patches Applied During Provisioning — 18.1.5	A-74
Patches Applied During Provisioning — 18.1.3	A-78
Patches Applied During Provisioning — 18.1.1	A-82
Patches Applied During Provisioning — 17.4.5	A-86
Patches Applied During Provisioning — 17.4.3	A-90
Patches Applied During Provisioning — 17.4.1	A-95
Patches Applied During Provisioning — 17.3.5	A-99
Patches Applied During Provisioning — 17.3.3	A-103
Patches Applied During Provisioning — 17.3.1	A-107
Patches Applied During Provisioning — 17.2.5	A-111
Patches Applied During Provisioning — 17.2.1	A-114
Patches Applied During Provisioning — 17.1.3	A-118
Patches Applied During Provisioning — 16.4.5	A-122
Patches Applied During Provisioning — 16.4.1	A-127
Patches Applied During Provisioning — 16.3.5	A-132
Patches Applied During Provisioning — 16.3.3	A-137
Patches Applied During Provisioning — 16.1.5	A-140
Patches Applied During Provisioning — 15.4.5	A-141

Preface

Administering Oracle SOA Cloud Service describes how to use Oracle SOA Cloud Service to manage and monitor your SOA composite applications in the cloud.

Audience

This guide is intended for users who want to manage and monitor SOA composite applications in the cloud.

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

See these related Oracle resources:

- Oracle SOA Cloud Service documentation in the [Oracle Cloud Library on the Oracle Help Center](#).
- Oracle Cloud information at <http://www.oracle.com/>.
- *Getting Started with Oracle Cloud*
- *Using Oracle Managed File Transfer Cloud Service*

Conventions

The following text conventions are used in this document:

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

1

What's New in Oracle SOA Cloud Service

For an overview of new and changed features in Oracle SOA Cloud Service, see *What's New in Oracle SOA Cloud Service*.

2

Get Started with Oracle SOA Cloud Service

Review the following topics to learn about how Oracle SOA Cloud Service works. These topics provide information about Oracle SOA Cloud Service concepts and components to help you get started with creating your own integrations.

Topics:

- [About Oracle SOA Cloud Service](#)
- [About Platform Differences Between the On-Premises and Cloud Environments](#)
- [About Oracle SOA Cloud Service Subscriptions and Licenses](#)
- [About the Components of Oracle SOA Cloud Service](#)
- [About Life Cycle Management of Oracle SOA Cloud Service Instances](#)
- [About Oracle SOA Cloud Service Roles and User Accounts](#)
- [About Adapters for Oracle SOA Cloud Service](#)
- [About the Oracle SOA Cloud Service User Interface](#)
- [About Oracle SOA Cloud Service Instances in Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic](#)
- [About Managing Oracle SOA Cloud Service Instances](#)
- [About Security](#)
- [About Managing Patches for Instances Provisioned With Earlier Releases](#)
- [About Oracle SOA Cloud Service Roles and Responsibilities between Oracle and Customer](#)
- [About the Infrastructure Resources Used by Oracle SOA Cloud Service](#)

About Oracle SOA Cloud Service

Oracle SOA Cloud Service provides a PaaS (Platform as a Service) computing platform solution for designing, deploying, and managing composite applications in the cloud.



Note:

Oracle SOA Cloud Service is no longer available for new accounts. Instead, use our newer Oracle Cloud Infrastructure offering, Oracle SOA Suite on Marketplace. If you're looking for our newest integration functionality and adapters, go to [Oracle Integration 3](#) on the Oracle Help Center.

See [About the Components of Oracle SOA Cloud Service](#).

Oracle SOA Cloud Service uses the *Active* high availability (HA) policy when it provisions instance compute nodes. Using the Active policy causes the virtual machine (VM) to automatically fail over to another physical compute node in the same compute zone in case the primary compute node fails.

The rich variety of features of Oracle SOA Cloud Service 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 Cloud Service is subscription-based, meaning you only pay when using the service. No large investment in hardware and IT expertise is required. This lets you fully concentrate on design, test, and deployment of integration solutions.
- **Create test environments in the cloud.** You can quickly subscribe to Oracle SOA Cloud Service 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 backups, patching, scaling, and recoveries with minimal configuration from the cloud. These tasks are handled for you by Oracle.

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 CX Sales new customer account with a Siebel application. This enables a customer that purchases a product through Oracle CX Sales to receive support for that product through the Siebel system. For this same Oracle CX Sales 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.


You can connect to on-premises applications through Oracle Messaging Cloud Service for asynchronous messaging, with web services to an on-premises Oracle Service Bus or Oracle SOA Suite infrastructure through a web proxy in the DMZ, or through a virtual private network.

About Platform Differences Between the On-Premises and Cloud Environments

This table describes high-level differences between running Oracle SOA on-premises and in the cloud.

Oracle SOA Suite On-Premises	Oracle SOA Cloud Service
You install Oracle SOA Suite on your own hardware.	Available by subscription.
You create the complete domain.	Provisioning of Oracle SOA Cloud Service automatically includes Oracle Java Cloud Service, which provides an Oracle WebLogic Server domain.
You must develop your own archival infrastructure.	Oracle SOA Cloud Service provides OPC-based backup services.

Oracle SOA Suite On-Premises	Oracle SOA Cloud Service
You must install a database.	<p data-bbox="841 275 1380 327">During Oracle SOA Cloud Service provisioning, you select the database to use.</p> <p data-bbox="841 338 1380 394">Note: You must provision the database prior to provisioning Oracle SOA Cloud Service.</p>
You must set up an environment based on your high availability requirements.	High availability functionality is provided by default using a virtual machine restart.
Oracle HTTP Server serves as the load balancer.	Supports the Oracle Traffic Director (OTD) load balancer during provisioning. Also supports Oracle Cloud Infrastructure load balancer, which must be configured manually post-provisioning.
You typically use shared storage.	<p data-bbox="841 611 1380 690">Shared storage is available through Database File System (DBFS) or OCI File Storage Service (FSS) in the cloud:</p> <ul data-bbox="841 695 1380 1486" style="list-style-type: none"> <li data-bbox="841 695 1380 779">• You can use a combination of database direct configuration for JMS and JTA logs and use DBFS for other shared file use cases. <li data-bbox="841 783 1380 867">• Any custom software or “one-off” patches must be installed on each virtual machine in the cloud. <li data-bbox="841 871 1380 903">• Log files are local to each virtual machine. <li data-bbox="841 907 1380 1026">• 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 data-bbox="841 1031 1380 1486">• Ephemeral storage vs. block storage vs. Oracle Cloud Infrastructure Object Storage Classic: <ul style="list-style-type: none"> <li data-bbox="889 1115 1380 1194">– Ephemeral storage is built every time the virtual machine is started — nothing is saved (stateless). <li data-bbox="889 1199 1380 1318">– Block storage is similar to regular file storage. The Oracle SOA code and your data is written from your virtual machine (stateful) to file storage. <li data-bbox="889 1323 1380 1486">– The Oracle Cloud Infrastructure Object Storage Classic is used for long term storage and backups. This service is accessible through the Oracle Cloud Infrastructure Object Storage Classic Console. <p data-bbox="938 1497 1380 1724">Note: You must provision Oracle Cloud Infrastructure Object Storage Classic prior to provisioning Oracle SOA Cloud Service. During Oracle SOA Cloud Service provisioning, you select the storage container (Oracle Cloud Infrastructure Object Storage Classic) to use.</p>
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 data-bbox="841 1745 1380 1824">• External network access must be configured at the virtual machine level and the Oracle Traffic Director level. <li data-bbox="841 1829 1380 1879">• Logins to the virtual machine can be done through an SSH tunnel.

Oracle SOA Suite On-Premises	Oracle SOA Cloud Service
There should not be any connectivity issues blocking Oracle SOA Cloud Service and your on-premises applications.	Connectivity between Oracle SOA Cloud Service adapters and on-premises applications may be blocked by your corporate firewall. Connections can be established by using an SSH tunnel from the application server to which the adapter connects.
When using the File Adapter, each Managed Server can read from a shared directory.	When using the File Adapter, each Managed Server should be configured to read files from File Storage Server (FSS).
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 with Oracle SOA Cloud Service. Instead, you can subscribe to Oracle Process Cloud Service or run Oracle Business Process Management Suite on Oracle Java Cloud Service.
	 Tutorial

About Oracle SOA Cloud Service Subscriptions and Licenses

Oracle SOA Cloud Service is no longer available for new accounts. Instead, use our newer Oracle Cloud Infrastructure offering, Oracle SOA Suite on Marketplace.

If you're looking for our newest integration functionality and adapters, go to [Oracle Integration 3](#) on the Oracle Help Center.

About the Components of Oracle SOA Cloud Service

Oracle SOA Cloud Service supports releases 12.2.1.4, 12.2.1.3, 12.2.1.2 (deprecated), and 12.1.3 (deprecated) of Oracle SOA Suite and its constituent components. Only releases 12.2.1.4 and 12.2.1.3 can be provisioned for new instances.

- **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 with 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, like approvals or manual routing decisions.
- **Business Rules** — Defines flexible business rules to direct actions in an integration process, such as approval routing decisions.
- **Mediator** — Mediates messages and provides routing and the capability to transform simple message flows.

See:

- "Overview of Oracle SOA Suite" in *Understanding Oracle SOA Suite* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- "Introduction to Building Applications with Oracle SOA Suite" in *Developing SOA Applications with Oracle SOA Suite* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- **Oracle WebLogic Suite.** Oracle WebLogic Suite is the flagship Oracle WebLogic Server edition. It is included with Oracle SOA Cloud Service.

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 Cloud Service, 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 management features are deployed on the Administration Server, and Oracle Service Bus runtime is deployed to all Managed Servers.

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

See:

- "About Oracle Service Bus Administration" in *Administering Oracle Service Bus* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- "About Oracle Service Bus" in *Developing Services with Oracle Service Bus* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- **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 Cloud Service

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 "Introduction to Oracle B2B" in *Using Oracle B2B* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

- **Oracle Managed File Transfer Cloud Service.** Oracle MFT Cloud Service 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 Cloud Service with the **MFT Cluster** service type.

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

- **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.

Beginning with 12c ([12.2.1.3](#)), you can provision Oracle BAM with the **Business Activity Monitoring** service type.

 **Note:**

In the current release of Oracle SOA Cloud Service, only single-node Oracle BAM [12.2.1.4](#) can be provisioned. For [12.2.1.3](#), both single-node and multi-node Oracle BAM can be provisioned.

See "Understanding Oracle Business Activity Monitoring" in *Monitoring Business Activity with Oracle BAM* ([12.2.1.4](#) | [12.2.1.3](#)).

- **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 "Introduction to Oracle JCA Adapters" in *Understanding Technology Adapters* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))

- **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 Cloud Service](#).

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

See:

- "Introduction to Oracle Enterprise Scheduler" in *Administering Oracle Enterprise Scheduler* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- "Introduction to Oracle Enterprise Scheduler" in *Developing Applications for Oracle Enterprise Scheduler* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))

- **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* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- *Administering Web Services* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- *Securing Web Services and Managing Policies with Oracle Web Services Manager* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))

About Life Cycle Management of Oracle SOA Cloud Service 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 Cloud Service instances.

When you create an Oracle SOA Cloud Service 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 Cloud Service instance has one server instance that hosts the Administration Server.

Resources	Description
Managed Servers	<p>Host business applications, application components, Web services, and their associated resources.</p> <p>When creating an Oracle SOA Cloud Service instance, you can configure up to four Managed Servers, then scale out, as needed.</p> <p>By default, the Managed Servers are named as follows: <code>first8charsOfDomainName_server_n</code> (where <i>n</i> starts with 1 and is incremented by 1 for each additional Managed Server to guarantee unique names).</p>
Cluster	<p>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 Oracle SOA Cloud Service instance.</p> <p>By default, the cluster name is generated from the first eight characters of the Oracle SOA Cloud Service instance name using the following format: <code>first8charsOfInstanceName_cluster</code>.</p>
Load Balancer	<p>Employs Oracle Traffic Director for load balancing to manage routing requests across all Managed Servers and provide failover and replication.</p> <p>It is recommended that you enable the load balancer when you configure more than one Oracle SOA Cloud Service in your environment. Enabling the load balancer is optional.</p>

If you want more information about Oracle WebLogic Server domains, see "WebLogic Server Domains" in *Understanding Oracle WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#)).

After the Oracle SOA Cloud Service 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 Traffic Director Console.



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 Cloud Service Instances

To manage the life cycle of Oracle SOA Cloud Service instances, follow the typical workflow shown in the following table.

 **Note:**

The table provides links to information about how to perform each task using the web browser-based Oracle SOA Cloud Service Console. For information about using the REST API to manage the life cycle of Oracle SOA Cloud Service instances, see REST API for Oracle SOA Cloud Service.

Task	More Information
Access the Oracle SOA Cloud Service Console after you have signed in.	See Access the Oracle SOA Cloud Service Console
Create a new Oracle SOA Cloud Service instance by stepping through the Oracle SOA Cloud Service provisioning wizard.	For Oracle Cloud Infrastructure, see Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure For Oracle Cloud Infrastructure Classic, see Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure Classic
View status, resource allocation, and other details for all Oracle SOA Cloud Service instances.	Explore the Oracle SOA Cloud Service Console
View status, resource allocation, and other details for an individual Oracle SOA Cloud Service instance.	About the Oracle SOA Cloud Service User Interface
Deploy and undeploy applications to an Oracle SOA Cloud Service instance using JDeveloper, Fusion Middleware Control, the WebLogic Server Administration Console, and WLST commands. You cannot deploy and undeploy applications directly through the Oracle SOA Cloud Service Console.	Deploy and Undeploy Applications to an Oracle SOA Cloud Service Instance
Stop Oracle SOA Cloud Service instances or individual Managed Servers. Restart the Administration Server or individual Managed Servers if reboot is needed.	Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs
Disable the load balancer to block any new traffic to an Oracle SOA Cloud Service instance temporarily while maintenance is performed.	Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance
Scale an Oracle SOA Cloud Service instance by scaling a cluster or a node.	Scale an Oracle SOA Cloud Service Instance
Add storage to a node that is running out of space. An Oracle Compute Cloud Service storage volume is created and attached to the node's VM.	Add Storage to a Node
Change the license type of an Oracle SOA Cloud Service instance from BYOL to Cloud License or vice versa after the instance is created.	Change the License Type for an Oracle SOA Cloud Service Instance
Back up your Oracle SOA Cloud Service instances to preserve them in a particular state. If necessary, undo changes by restoring the instance's configuration data from a backup. You can also restore the software to its current official patch set update (PSU) level.	Back Up and Restore an Oracle SOA Cloud Service Instance
Manage access to an Oracle SOA Cloud Service instance by deleting the instance.	Delete an Oracle SOA Cloud Service Instance
Use tags to organize and categorize your Oracle SOA Cloud Service instances, and to search for them.	Manage Tags for a Service Instance

About Oracle SOA Cloud Service Roles and User Accounts

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

The following role is created for Oracle SOA Cloud Service: *SOA Administrator*.

When the Oracle SOA Cloud Service account is first set up, the service administrator is given the SOA Administrator role. User accounts with the role must be added before anyone can access and use Oracle SOA Cloud Service.

The identity domain administrator can create more SOA administrators by creating user accounts and assigning the role to users. For information about how to add user accounts in Oracle Cloud, see:

- For Oracle Cloud Infrastructure: [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.
- For Oracle Cloud Infrastructure Classic: Managing Users, User Accounts, and Roles in *Managing and Monitoring Oracle Cloud*

Topics:

- [SOA Administrator](#)
- [Related Service Administrators](#)
- [Service Instance Users](#)
- [Oracle Cloud Infrastructure Policies](#)

SOA Administrator

The primary role in Oracle SOA Cloud Service is SOA Administrator.

The following table summarizes the privileges given to the SOA Administrator role.

Description of Privilege	More Information
Can create and delete service instances	Provision an Oracle SOA Cloud Service Instance Delete an Oracle SOA Cloud Service Instance
Can stop and start service instances, and VMs	Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs
Can suspend and enable service instances by disabling and enabling the load balancer	Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance
Can scale, patch, and back up or restore service instances	Scale an Oracle SOA Cloud Service Instance About Managing Patches for Instances Provisioned With Earlier Releases Back Up and Restore an Oracle SOA Cloud Service Instance
Can administer load balancers for service instances	Administer the Load Balancer for an Oracle SOA Cloud Service Instance

Description of Privilege	More Information
Can monitor and manage service usage in Oracle Cloud	<ul style="list-style-type: none"> For Oracle Cloud Infrastructure: See the Oracle Cloud Infrastructure documentation. For Oracle Cloud Infrastructure Classic: Performing Service-Specific Tasks in <i>Managing and Monitoring Oracle Cloud</i>
Can grant the SOA Administrator role to existing users	<ul style="list-style-type: none"> For Oracle Cloud Infrastructure: Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console in the Oracle Cloud Infrastructure documentation. For Oracle Cloud Infrastructure Classic: Managing Users, User Accounts, and Roles in <i>Managing and Monitoring Oracle Cloud</i>

Related Service Administrators

The following table summarizes the privileges given to other related service administrator roles in Oracle Cloud.

Role	Privileges
Compute_Operations	Create Oracle SOA Cloud Service instances on Oracle Cloud Infrastructure Classic regions.
DBaaS_Administrator	<p>Create and manage Oracle Database Classic Cloud Service deployments.</p> <p>A database deployment must exist prior to creating an Oracle SOA Cloud Service instance, unless you create the service instance by using a QuickStart template. See Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic.</p>
Storage_ReadWriteGroup	Enable backups for an Oracle SOA Cloud Service instance, and store the backups in an existing Oracle Cloud Infrastructure Object Storage Classic container.
Storage_Administrator	Create Oracle Cloud Infrastructure Object Storage Classic containers to use as backup storage locations for Oracle SOA Cloud Service instances.

Service Instance Users

Learn about the operating system and Oracle WebLogic Server administrative user accounts that are created when you create an Oracle SOA Cloud Service instance.

Account	Description	More Information
VM OS User	<p>The <code>opc</code> user has root privileges on the OS running on a VM:</p> <ul style="list-style-type: none"> • Can connect to a VM through SSH for direct VM-level access to an Oracle SOA Cloud Service instance. • Can create other OS accounts on a VM using the appropriate OS tool through the SSH interface. <p>The <code>oracle</code> user cannot be used to log into a host:</p> <ul style="list-style-type: none"> • Only has regular user permissions to start and stop Oracle products that have been installed on the host. <p>Note that there are no default passwords for either the <code>opc</code> or <code>oracle</code> user.</p> <p>NOTE: Do <i>not</i> update the <code>oracle</code> user password or password expiration policy. The PaaS Service Manager uses the <code>oracle</code> user for administrative access and counts on the password being stable.</p> <p>SSH access to the VM by the <code>opc</code> user is based on the public key provided at the time the Oracle SOA Cloud Service instance was provisioned.</p> <p>You provide the private key when you log in to the VM as <code>opc</code>. Once logged in, as a root user you can switch to the <code>oracle</code> user with:</p> <pre>sudo su - oracle</pre>	Access a VM Through a Secure Shell (SSH)
WebLogic Administrator	<p>Can manage Oracle WebLogic Server in Oracle SOA Cloud Service.</p> <p>Can access and use the WebLogic Server Administration Console.</p> <p>Can manage users and groups in the embedded LDAP.</p> <p>Can configure other identity providers.</p> <p>Can deploy and undeploy applications using the WebLogic Server Administration Console.</p>	Access an Administration Console for Software that a Service Instance Is Running Use the WebLogic Server Administration Console to Deploy and Undeploy an Application

 **Note:**

The Oracle WebLogic Server administrator account and VM OS User accounts are not stored or managed in Oracle Cloud.

You provide the user name and password for the WebLogic Administrator when you create an Oracle SOA Cloud Service instance.

The credentials and permissions for the WebLogic Administrator and all end user accounts that the administrator creates are stored and managed in Oracle WebLogic Server.

Oracle Cloud Infrastructure Policies

Learn about how to create and manage resources in Oracle Cloud Infrastructure, administrators define policies that grant privileges to users and groups.

To create and manage resources in Oracle Cloud Infrastructure, administrators define policies that grant privileges to users and groups. For example, to create a database for use with Oracle SOA Cloud Service in either an Oracle Autonomous Transaction Processing or Oracle Cloud Infrastructure database, an administrator must create policies that grant you access to these services. See [Securing IAM in the Oracle Cloud Infrastructure documentation](#).

In order to create Oracle SOA Cloud Service instances in an Oracle Cloud Infrastructure region, an administrator must create policies that grant specific privileges to Oracle SOA Cloud Service.

For example, the administrator must specify the following policy to grant Oracle SOA Cloud Service access to the Autonomous Transaction Processing or Oracle Cloud Infrastructure database:

- **Autonomous Transaction Processing database**
`Allow service PSM to inspect autonomous-database in compartment Autonomous Transaction Processing database compartment`
- **Oracle Oracle Cloud Infrastructure database**
`Allow service PSM to inspect database-family in compartment Oracle Cloud Infrastructure database compartment`

See [Prerequisites for Oracle Platform Services on Oracle Cloud Infrastructure](#) in the Oracle Cloud Infrastructure documentation.

About Adapters for Oracle SOA Cloud Service

Oracle SOA Cloud Service includes a number of adapters.

All of the adapters delivered with Oracle SOA Suite are available for Oracle SOA Cloud Service, Oracle Service Bus, and Oracle SOA Suite domain types. 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 the [Oracle Integration Adapters Certification Matrix](#) for certification information about the various integration adapters.

Oracle Technology Adapters

See *Understanding Technology Adapters* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))

Oracle Cloud Adapters

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

See the Oracle SOA Cloud Service supports the following cloud adapters for the SOA and OSB service types:

12.2.1.4:

- [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](#)

12.2.1.3:

- [Oracle Sales Cloud Adapter](#)
- [Oracle RightNow Cloud Adapter](#)
- [Oracle Eloqua Cloud Adapter](#) (outbound from Oracle SOA Cloud Service to Eloqua only)
- [Salesforce Adapter](#)
- [Oracle ERP Cloud Adapter](#)
- [Oracle NetSuite Cloud Adapter](#) (outbound from Oracle SOA Cloud Service to NetSuite only)
- [Ariba Adapter](#)
- [SuccessFactors Adapter](#)
- [ServiceNow Adapter](#)

12.2.1.2:

- [Oracle Sales Cloud Adapter](#)
- [Oracle RightNow Cloud Adapter](#)
- [Oracle Eloqua Cloud Adapter](#) (outbound from Oracle SOA Cloud Service to Eloqua only)
- [Salesforce Adapter](#)

- [Oracle ERP Cloud Adapter](#)
- [Oracle NetSuite Cloud Adapter](#) (outbound from Oracle SOA Cloud Service to NetSuite only)
- [Ariba Adapter](#)
- [SuccessFactors Adapter](#)

12.1.1.3:

- [Oracle Sales Cloud Adapter](#)
- [Oracle RightNow Cloud Adapter](#)
- [Oracle Eloqua Cloud Adapter](#)
- [Salesforce Cloud Adapter](#)
- Oracle HCM connectivity (For integration with HCM, please refer to the following blogs.)
 - [Integrating with HCM using MFT](#)
 - [HCM File integration using Oracle SOA Cloud Service](#)

Certified Application Adapters

The following enterprise application adapters are available:

- Oracle E-Business Suite Adapter ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#))
- Integration Adapter for SAP R/3 ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#))
- JD Edwards World Adapter ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- Siebel Adapter ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#))

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 as an additionally metered amount on the Oracle SOA Cloud Service OCPUs at the instance level during provisioning or scaling. After provisioning, the B2B Adapter for EDI cannot be disabled from an existing Oracle SOA Cloud Service instance. The adapter can only be set during the initial provisioning process and can only be removed by deleting the instance. Billing can be paused by stopping the instance, which stops the entire Oracle SOA Cloud Service VM. Another option is to create a new Oracle SOA Cloud Service instance without the B2B Adapter for EDI and migrate Oracle SOA Cloud Service projects and artifacts to the new instance. To migrate from an old Oracle SOA Cloud Service instance to a new Oracle SOA Cloud Service 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 Cloud Service customers that have metered or non-metered Oracle SOA Cloud Service instances, the recommended path forward for using the B2B Adapter for EDI, is to provision a new Oracle SOA Cloud Service instance in the Universal Credits account, and then use that instance exclusively for B2B processing. This allows you to run an existing SOA instance in parallel with your B2B instance.

You can download the B2B Document Editor to use with Oracle B2B from the [Oracle SOA Suite Download page](#).

To download the B2B Document Editor:

1. Accept the license agreements.
2. Expand **Free Oracle SOA Suite 12c Installations** and then expand **Recommended Install Process**.
3. Under **Additional Components**, click **Download** next to the B2B Document Editor components.

About the Oracle SOA Cloud Service User Interface

Explore the Oracle SOA Cloud Service user interface pages.

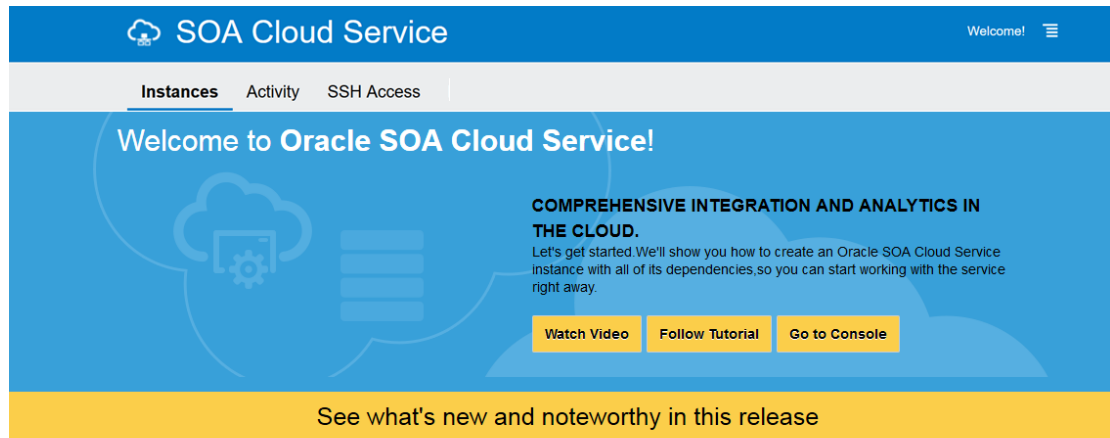
Topics:

- [Explore the Oracle SOA Cloud Service Welcome Page](#)
- [Explore the Oracle SOA Cloud Service Console](#)
- [About the Oracle SOA Cloud Service User Interface](#)
- [Explore the Oracle SOA Cloud Service Administration Page for Backups](#)
- [Explore the Oracle SOA Cloud Service Administration Page for Patching](#)
- [Explore the Oracle SOA Cloud Service Activity Page](#)
- (Oracle Cloud Infrastructure Classic only) [Explore the Oracle SOA Cloud Service IP Reservations Page](#)


Explore the Oracle SOA Cloud Service Welcome Page


You can use the Oracle SOA Cloud Service Welcome page to get started using Oracle SOA Cloud Service.


When you access Oracle SOA Cloud Service the first time for an account, you will see the Welcome page, where you can explore videos and tutorials about Oracle SOA Cloud Service.



Discover

- 

Overview of Oracle SOA Cloud Service
Overview of features and capabilities of Oracle SOA Cloud Service
2:38
- 

Provisioning Oracle SOA Cloud Service
Detailed walkthrough of steps to provision Oracle SOA Cloud Service
2:46
- 

Deploying a Service Bus Application to Oracle SOA Cloud Service
Learn how to deploy a Service Bus application from your local machine to the Oracle SOA Suite Cloud Service
1:54

Learn

Select the role that best describes you, and we'll suggest the best way to learn about Oracle SOACS Cloud Service



Service Administrator

"I create service instances and keep them updated."

Use the Oracle SOA Cloud Service Welcome page to perform the following tasks:

- Get started by stepping through the tutorials.
- Discover Oracle SOA Cloud Service by watching video demonstrations of key tasks.
- Learn what's new and noteworthy in the current release of Oracle SOA Cloud Service.
- Learn about Oracle SOA Cloud Service by selecting your role to customize your learning path.
- Navigate to the Oracle SOA Cloud Service Console.

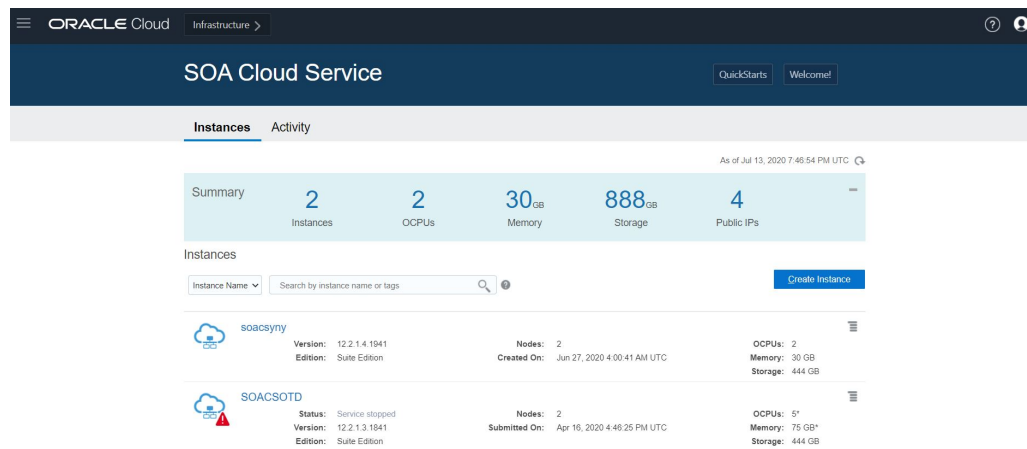
The following table describes the key information shown on the Oracle SOA Cloud Service Welcome page.

Element	Description
Instances	Click to navigate to the Oracle SOA Cloud Service Console. See Explore the Oracle SOA Cloud Service Console .
Welcome!	Click to redisplay this page.
Watch Video	Click to see a video about how to get started with Oracle SOA Cloud Service.
Follow Tutorial	Click to complete tutorials about how to get started with Oracle SOA Cloud Service.
Go to Console	Click to navigate to the Oracle SOA Cloud Service Console. See Explore the Oracle SOA Cloud Service Console .

Element	Description
See what's new and noteworthy in this release	Click to read What's New for Oracle SOA Cloud Service.
Discover	Watch videos that demonstrate how to perform key tasks.
Learn	Click your role to customize your learning path.

Explore the Oracle SOA Cloud Service Console






You can use the Oracle SOA Cloud Service Console to view all existing Oracle SOA Cloud Service instances and to create new instances.



The following table describes the key information shown on the Oracle SOA Cloud Service Console.

Element	Description
Instances tab	Click to navigate to the Oracle SOA Cloud Service Console (this page).
Activity tab	Click to navigate to the Oracle SOA Cloud Service Console Activity page .
QuickStarts	(Oracle Cloud Infrastructure Classic only) Click to create a QuickStart instance. See Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic .
Welcome!	Click to display the Welcome page.
Summary panel	Shows the following information: <ul style="list-style-type: none"> Instances: Number of Oracle SOA Cloud Service instances in the identity domain. OCPUs: Total number of Oracle Compute Units (OCPUs) allocated across all Oracle SOA Cloud Service instances. Memory: Total amount of memory in GBs allocated across all Oracle SOA Cloud Service instances. Storage: Total amount of block storage in GBs allocated across all Oracle SOA Cloud Service instances. Public IPs: Total number of IP reservations allocated across all Oracle SOA Cloud Service instances.
Instances	All Oracle SOA Cloud Service instances in the identity domain, with search fields to filter the list of instances.

Element	Description
Create Instance	Create a new Oracle SOA Cloud Service instance. See Provision an Oracle SOA Cloud Service Instance .

Element	Description
<i>instance name</i>	<p>Name of an Oracle SOA Cloud Service instance with the following summary details:</p> <ul style="list-style-type: none"> • An icon indicating current instance status: <ul style="list-style-type: none"> –  The instance is up and running. –  The instance is being created. –  The instance is undergoing maintenance or terminating. –  The instance has failed to be created. This icon can also mean that the service instance has stopped. See the Activity page. • The instance name. Click the instance name to access more details about the instance and administration tasks, such as backup and restore. • Status: Current status of the instance. • Version: Version of Oracle WebLogic Server configured for the instance. Valid values are: 12.2.1.4.0, 12.2.1.3.0, 12.2.1.2.0 (deprecated), and 12.1.3.0 (deprecated). • Edition: Edition configured for the instance, which is always Suite Edition. For more information about this edition, see Explore WebLogic Server and click WebLogic Suite. • Nodes: Number of nodes allocated for the instance. • Created On: When provisioning is complete, date and time in UTC that the instance was created. • OCPUs: Number of OCPUs allocated for the instance. • Memory: Amount of memory in GBs allocated for the instance. • Storage: Amount of storage in GBs allocated for the instance. • Click  to select the following actions (the actions shown are dependent on the instance configuration): <ul style="list-style-type: none"> – Open WebLogic Server Administration Console to open the Oracle WebLogic Server Administration Console. – Open Service Bus Console to open the Oracle Service Bus Console. – Open SOA Composer to open Oracle SOA Composer. – Open B2B Console to open the Oracle B2B Console. – Open Load Balancer Console to open the console to administer the load balancer, if a load balancer has been configured for the instance. See Administer the Load Balancer for an Oracle SOA Cloud Service Instance. – Open MFT Console to open the Oracle Managed File Transfer Console. – Open Fusion Middleware Control Console to open the Oracle Fusion Middleware Control Console to administer your application environment. – Open Worklist Application to open the Oracle Worklist Application. – Open BAM Composer to open the Oracle BAM Composer. – Start Stop Restart. See Stop, Start, or Restart an Oracle SOA Cloud Service Instance. – Access Rules (for Oracle Cloud Infrastructure Classic only). See Manage Access Rules for an Oracle SOA Cloud Service Instance. – Add SSH Access to add a new SSH public key to the instance if needed. See Add an SSH Public Key. – Add Tags or Manage Tags to create or manage tags for the instance. See Create, Assign, and Unassign Tags.

Element	Description
	<ul style="list-style-type: none"> – Change License Type to change the license type of the instance (BYOL or Cloud License). See Change the License Type for an Oracle SOA Cloud Service Instance. – Delete to delete the service instance. In the Delete Instance dialog, set the following options and click Delete: <ul style="list-style-type: none"> * Force service deletion: (Optional) Select this check box if you want the service instance to be deleted even if the database deployment cannot be reached to delete the database schemas. If enabled, you may need to delete the associated database schemas manually on the database deployment if they are not deleted as part of the service instance delete operation. * Administration User Name: Enter the name of the database administrator user that was specified when the database deployment was created. This user owns the instance’s repository and schemas. If you have specified two databases, specify the name of the administrator for the database deployment for the Oracle required schema. * Password: Enter the Database Administrator user password for the database deployment that contains the Oracle required schema <p style="text-align: center;">See Delete an Oracle SOA Cloud Service Instance.</p>
Instance Create and Delete History	<p>Shows details about created or deleted instances.</p> <ul style="list-style-type: none"> • Select the time period for which you are interested in viewing created and failed service instances. • Show only failed attempts: Select this check box if you want to see failed attempts only. • Details: Displays system messages logged during the creation or deletion process. Messages include information about auto-retry attempts.

Explore the Oracle SOA Cloud Service Administration Page for Backups

You can use the Backups tab on the Administration page to back up and restore an Oracle SOA Cloud Service instance.

The screenshot shows the Oracle SOA Cloud Service user interface for instance 'sobl2soacs'. The interface is divided into several sections:

- Navigation Menu:** Includes 'Overview' (3 Nodes) and 'Administration' (0 Patches Available).
- Backup Summary Table:**

Backup Type	Frequency	Storage / Volume Used
Daily at 8:10:00 AM UTC Incremental Backups	0 MB Backups on Cloud Storage	
Wednesday at 8:10:00 AM UTC Full Backups	0 Backup Volume Used (MB)	
N/A Last Successful Backup	0.00 Backup Volume Used (%)	
- Most Recent Backup:** Failed on Apr 14, 2021 8:10:07 AM UTC.
- Available Backups:** No backups available.
- Restore History:** No backups restored.

Element	Description
---------	-------------






Click to view the following information about the instance:






- **Service Level**
- **Region**
- **Created By**
- **Created On**
- **Description**
- **License**
- **Identity Domain**
- **Metering Frequency**
- **Subscription id**

This image shows a close-up of the 'Overview' tile, which displays the number of nodes in the instance, currently '3 Nodes'.

Click the **Overview** tile to access the [Oracle SOA Cloud Service Instance Overview page](#) at any time.

Element	Description
Summary Table	<p data-bbox="678 275 1333 327">The blue summary table at the top of the tab lists the following information:</p> <ul data-bbox="678 338 1377 873" style="list-style-type: none"><li data-bbox="678 338 1377 604">• Status of incremental backups, including:<ul data-bbox="727 373 1377 604" style="list-style-type: none"><li data-bbox="727 373 1240 401">– The scheduled time for incremental backups<li data-bbox="727 411 1377 604">– The total amount of space, in MB or GB, that backups occupy in the Oracle Cloud Infrastructure Object Storage Classic container for storing backups. This amount includes space that is occupied by backups that have been manually uploaded to the container, if any, in addition to the space occupied by backups that Oracle SOA Cloud Service has moved there.<li data-bbox="678 615 1377 751">• Status of full backups, including how much data has been used. The total amount of space, in MB or GB, that local copies of backups occupy in the backup volume on the block storage of the virtual machine where the Administration Server is running.<li data-bbox="678 762 1377 873">• The size of the last successful backup as a percentage of the available space that backups occupy in the backup volume on the block storage of the virtual machine where the Administration Server is running.

Element	Description
Available Backups	<p>List of available backups. By default, only backups for the last 7 days are listed.</p> <p>Use the search fields to specify a range of dates for which you want backups returned, then click .</p> <p>Click  to select the following actions:</p> <ul style="list-style-type: none"> • Backup Now to create an on-demand backup of the instance. See Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance. • Configure Backups to set when scheduled backups occur and to specify how backups are stored. See: <ul style="list-style-type: none"> – Update Backup and Recovery Credentials – Configure Automated Backups for an Oracle SOA Cloud Service Instance • Disable Backups to disable backups for the instance. This includes both automated and on-demand backups. • Enable Backups to reenables backups for the instance. <p>In the list of backups, the icons for each backup indicate status, with a timestamp indicating when the backup was started. Click the icon for additional information:</p> <ul style="list-style-type: none"> •  The backup is in progress. It will not be available for use in restoring the service instance until it is completed. •  The backup completed. It is available for use in restoring the instance if needed. •  <p>The scheduled backup completed, after which Oracle SOA Cloud Service tried but failed to move or delete one or more older backups. For information about when and why Oracle SOA Cloud Service moves or deletes older backups, see Where Backups Are Stored. The backup is still available for use in restoring the service instance.</p> <p>To find out why Oracle SOA Cloud Service could not move or remove the older backup, place the cursor over the icon.</p> <p>The presence of the older backup may cause future backups to fail because of insufficient space. For information about how to prevent future backups from failing in this way see Problems with Backup and Restoration.</p> <p>Each backup includes the following information:</p> <ul style="list-style-type: none"> • Type: A comma-separated pair of words that describes the type of the backup. The first word in the pair describes the extent of the backup: <ul style="list-style-type: none"> – Incremental—The backup contains only the runtime artifacts of each managed virtual machine in the service instance. – Full—The backup contains runtime artifacts and files that change infrequently or do not change. <p>The second word in the pair indicates how the backup was initiated:</p> <ul style="list-style-type: none"> – If the backup was initiated automatically at the scheduled time, Scheduled is displayed.

Element	Description
	<ul style="list-style-type: none"> – If the backup was initiated by a user, the name of the user is displayed. – If the backup was initiated in response to another management operation by a user, the name of the user is displayed. <p>See How Backups Are Initiated.</p> <ul style="list-style-type: none"> • Available Until: The date and time until which the backup will be retained. • Click Notes to display the notes that were provided when the backup was created or the restoration was performed. • Click  to select the following actions: <ul style="list-style-type: none"> – Restore to restore the instance from the backup. See Restore an Oracle SOA Cloud Service Instance from a Backup. – Delete to delete the backup. See Delete a Backup.
Restore History	<p>Expand to display a list of all the restoration operations on this service instance. By default, only restoration operations for the last 7 days are listed. Use the search fields to specify a range of</p> <p>dates for which you want restore history, then click .</p> <p>Select Include unsuccessful restore attempts to include the unsuccessful restoration operations in the list.</p> <p>In the list of restoration operations, the icons for each restoration indicate status, with a timestamp indicating when the restoration was started. Click the icon for additional information:</p> <ul style="list-style-type: none"> •  The restoration operation completed. •  The restoration operation is in progress. •  The restoration attempt was unsuccessful. <p>Each restoration operation includes the following information:</p> <ul style="list-style-type: none"> • From Backup: The date and time when the backup from which the service instance was restored was created. • Status: The status of the restoration operation (Completed, In Progress, or Failed). Click the status to see detailed status messages for the operation. • Click Notes to display the notes that were provided when the backup was created or the restoration was performed.

Explore the Oracle SOA Cloud Service Administration Page for Patching

The Patching tab on the Administration page of the Oracle SOA Cloud Service Console is not supported by Oracle SOA Cloud Service.

This page is not used for patching Oracle SOA Cloud Service instances. Instead, refer to [About Managing Patches for Instances Provisioned With Earlier Releases](#).


The screenshot shows the Oracle SOA Cloud Service console for a service named 'sob12soacs'. The 'Patching' tab is active, showing a warning: 'Last activity BACKUP Apr 14, 2021 8:10:04 AM UTC failed. See the activity log for Details'. Below this, the 'Available Patches' section shows 'No patches available.' and the 'Patch and Rollback History' section shows 'No patches applied.' A left-hand navigation pane includes 'Overview' (3 Nodes) and 'Administration' (0 Patches Available, Most recent backup failed).

Explore the Oracle SOA Cloud Service Activity Page

You can use the Activity page to search for and review Oracle SOA Cloud Service activities that have occurred in your identity domain. To access this page, click the Activity tab in the Oracle SOA Cloud Service Console.

The screenshot shows the 'Activity' page in the Oracle SOA Cloud Service console. It includes a search filter for 'SOA Cloud Service' and a table of activity logs. The table has columns for Operation, Instance Name, Service Type, Operation Status, Start Time, End Time, and Initiated By. The results show a list of operations performed on various instances, including a failed 'Back Up' operation on the 'sob12soacs' instance.

Operation	Instance Name	Service Type	Operation Status	Start Time	End Time	Initiated By
Delete Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 5:42:28 PM UTC	Apr 14, 2021 5:59:12 PM UTC	O CLOUD9...
Scale Application	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 5:19:22 PM UTC	Apr 14, 2021 5:24:04 PM UTC	O CLOUD9...
Scale Application	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 4:56:17 PM UTC	Apr 14, 2021 5:01:37 PM UTC	O CLOUD9...
Scale In	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 4:07:58 PM UTC	Apr 14, 2021 4:42:43 PM UTC	O CLOUD9...
Start Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 3:28:59 PM UTC	Apr 14, 2021 3:47:29 PM UTC	O CLOUD9...
Stop Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 3:25:57 PM UTC	Apr 14, 2021 3:28:18 PM UTC	O CLOUD9...
Scale Out	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 2:13:41 PM UTC	Apr 14, 2021 3:25:44 PM UTC	O CLOUD9...
Create Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 10:39:53 AM UTC	Apr 14, 2021 1:53:38 PM UTC	O CLOUD9...
Back Up	sob12soacs	SOA Cloud Service	Failed	Apr 14, 2021 8:10:04 AM UTC	Apr 14, 2021 8:24:29 AM UTC	System

Element	Description
Search Activity Log	<p>Details about search activity:</p> <ul style="list-style-type: none"> • Start Time Range: Set date values to list only operations started within a specified time range. The range defaults to the previous 24 hours. • Operation Status: Select one or more status types to list operations of only the selected status types: <ul style="list-style-type: none"> – All (default) – Scheduled – Running – Succeeded – Failed • Instance Name: Enter an instance name to list operations only for that instance. You can enter a full or partial service instance name. • Service Type: Select a service type to list operations only for instances of that service type. The default value is the current cloud service type. • Operation: Select one or more to list only those operations. You can select any subset of the given operations. Default: All.
Search	Searches for activities by applying the filters specified by the fields above, and displays matching operations in the list.
Reset	Clears the Start Time Range and Instance Name fields, and returns the Operation Status and Operation fields to their default values.
Results per page	Select the number of results you want to view per page. The default value is 10.
	Click next to an operation to show and hide status messages for the operation.

Explore the Oracle SOA Cloud Service IP Reservations Page



This topic applies only to Oracle Cloud Infrastructure Classic.

You can use the IP Reservations page to search for and view the existing IP reservations. To access this page, click the IP Reservations tab in the Oracle SOA Cloud Service Console.

Element	Description
Search IP Reservations by name or region	Enter a full or partial IP reservation name or region name and click the search icon to search for a particular IP reservation.
Create	Create a new IP reservation. See Create an IP Reservation .

About the Oracle SOA Cloud Service User Interface

Explore the Oracle SOA Cloud Service user interface pages.

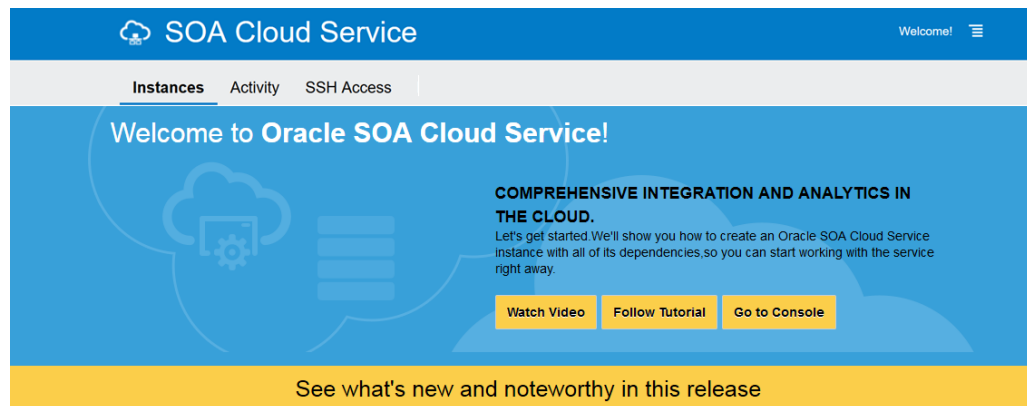
Topics:

- [Explore the Oracle SOA Cloud Service Welcome Page](#)
- [Explore the Oracle SOA Cloud Service Console](#)
- [About the Oracle SOA Cloud Service User Interface](#)
- [Explore the Oracle SOA Cloud Service Administration Page for Backups](#)
- [Explore the Oracle SOA Cloud Service Administration Page for Patching](#)
- [Explore the Oracle SOA Cloud Service Activity Page](#)
- (Oracle Cloud Infrastructure Classic only) [Explore the Oracle SOA Cloud Service IP Reservations Page](#)




Explore the Oracle SOA Cloud Service Welcome Page

You can use the Oracle SOA Cloud Service Welcome page to get started using Oracle SOA Cloud Service.

When you access Oracle SOA Cloud Service the first time for an account, you will see the Welcome page, where you can explore videos and tutorials about Oracle SOA Cloud Service.




Discover

-  **Overview of Oracle SOA Cloud Service**
Overview of features and capabilities of Oracle SOA Cloud Service
2:38
-  **Provisioning Oracle SOA Cloud Service**
Detailed walkthrough of steps to provision Oracle SOA Cloud Service
2:46
-  **Deploying a Service Bus Application to Oracle SOA Cloud Service**
Learn how to deploy a Service Bus application from your local machine to the Oracle SOA Suite Cloud Service
1:54

Learn

Select the role that best describes you, and we'll suggest the best way to learn about Oracle SOACS Cloud Service

 **Service Administrator**
"I create service instances and keep them updated."

Use the Oracle SOA Cloud Service Welcome page to perform the following tasks:

- Get started by stepping through the tutorials.
- Discover Oracle SOA Cloud Service by watching video demonstrations of key tasks.
- Learn what's new and noteworthy in the current release of Oracle SOA Cloud Service.
- Learn about Oracle SOA Cloud Service by selecting your role to customize your learning path.
- Navigate to the Oracle SOA Cloud Service Console.

The following table describes the key information shown on the Oracle SOA Cloud Service Welcome page.

Element	Description
Instances	Click to navigate to the Oracle SOA Cloud Service Console. See Explore the Oracle SOA Cloud Service Console .
Welcome!	Click to redisplay this page.
Watch Video	Click to see a video about how to get started with Oracle SOA Cloud Service.
Follow Tutorial	Click to complete tutorials about how to get started with Oracle SOA Cloud Service.
Go to Console	Click to navigate to the Oracle SOA Cloud Service Console. See Explore the Oracle SOA Cloud Service Console .
See what's new and noteworthy in this release	Click to read What's New for Oracle SOA Cloud Service.
Discover	Watch videos that demonstrate how to perform key tasks.
Learn	Click your role to customize your learning path.

Explore the Oracle SOA Cloud Service Console






You can use the Oracle SOA Cloud Service Console to view all existing Oracle SOA Cloud Service instances and to create new instances.

The screenshot shows the Oracle SOA Cloud Service console interface. At the top, there's a navigation bar with 'ORACLE Cloud' and 'Infrastructure' tabs. Below that, the main header reads 'SOA Cloud Service' with 'QuickStarts' and 'Welcome!' buttons. The main content area is divided into 'Instances' and 'Activity' tabs, with 'Instances' selected. A summary card displays: 2 Instances, 2 OCPUs, 30 GB Memory, 888 GB Storage, and 4 Public IPs. Below the summary, there's a search bar for instance names and a 'Create Instance' button. Two instances are listed:

Instance Name	Version	Edition	Nodes	Created On	OCPUs	Memory	Storage
soacsyn	12.2.1.4.1941	Suite Edition	2	Jun 27, 2020 4:00:41 AM UTC	2	30 GB	444 GB
SOACSOTD	12.2.1.3.1841	Suite Edition	2	Apr 16, 2020 4:46:25 PM UTC	5*	75 GB*	444 GB

The following table describes the key information shown on the Oracle SOA Cloud Service Console.

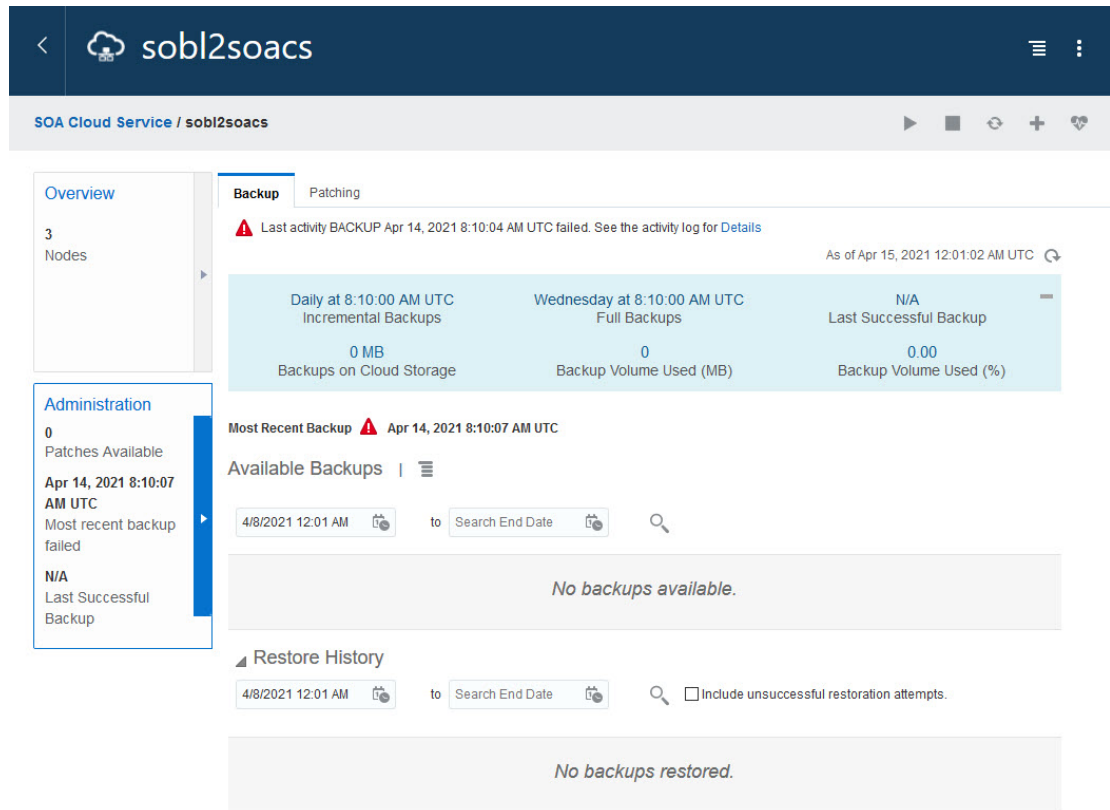
Element	Description
Instances tab	Click to navigate to the Oracle SOA Cloud Service Console (this page).
Activity tab	Click to navigate to the Oracle SOA Cloud Service Console Activity page .
QuickStarts	(Oracle Cloud Infrastructure Classic only) Click to create a QuickStart instance. See Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic .
Welcome!	Click to display the Welcome page.
Summary panel	Shows the following information: <ul style="list-style-type: none"> • Instances: Number of Oracle SOA Cloud Service instances in the identity domain. • OCPUs: Total number of Oracle Compute Units (OCPUs) allocated across all Oracle SOA Cloud Service instances. • Memory: Total amount of memory in GBs allocated across all Oracle SOA Cloud Service instances. • Storage: Total amount of block storage in GBs allocated across all Oracle SOA Cloud Service instances. • Public IPs: Total number of IP reservations allocated across all Oracle SOA Cloud Service instances.
Instances	All Oracle SOA Cloud Service instances in the identity domain, with search fields to filter the list of instances.
Create Instance	Create a new Oracle SOA Cloud Service instance. See Provision an Oracle SOA Cloud Service Instance .

Element	Description
<i>instance name</i>	<p>Name of an Oracle SOA Cloud Service instance with the following summary details:</p> <ul style="list-style-type: none"> • An icon indicating current instance status: <ul style="list-style-type: none"> –  The instance is up and running. –  The instance is being created. –  The instance is undergoing maintenance or terminating. –  The instance has failed to be created. This icon can also mean that the service instance has stopped. See the Activity page. • The instance name. Click the instance name to access more details about the instance and administration tasks, such as backup and restore. • Status: Current status of the instance. • Version: Version of Oracle WebLogic Server configured for the instance. Valid values are: 12.2.1.4.0, 12.2.1.3.0, 12.2.1.2.0 (deprecated), and 12.1.3.0 (deprecated). • Edition: Edition configured for the instance, which is always Suite Edition. For more information about this edition, see Explore WebLogic Server and click WebLogic Suite. • Nodes: Number of nodes allocated for the instance. • Created On: When provisioning is complete, date and time in UTC that the instance was created. • OCPUs: Number of OCPUs allocated for the instance. • Memory: Amount of memory in GBs allocated for the instance. • Storage: Amount of storage in GBs allocated for the instance. • Click  to select the following actions (the actions shown are dependent on the instance configuration): <ul style="list-style-type: none"> – Open WebLogic Server Administration Console to open the Oracle WebLogic Server Administration Console. – Open Service Bus Console to open the Oracle Service Bus Console. – Open SOA Composer to open Oracle SOA Composer. – Open B2B Console to open the Oracle B2B Console. – Open Load Balancer Console to open the console to administer the load balancer, if a load balancer has been configured for the instance. See Administer the Load Balancer for an Oracle SOA Cloud Service Instance. – Open MFT Console to open the Oracle Managed File Transfer Console. – Open Fusion Middleware Control Console to open the Oracle Fusion Middleware Control Console to administer your application environment. – Open Worklist Application to open the Oracle Worklist Application. – Open BAM Composer to open the Oracle BAM Composer. – Start Stop Restart. See Stop, Start, or Restart an Oracle SOA Cloud Service Instance. – Access Rules (for Oracle Cloud Infrastructure Classic only). See Manage Access Rules for an Oracle SOA Cloud Service Instance. – Add SSH Access to add a new SSH public key to the instance if needed. See Add an SSH Public Key. – Add Tags or Manage Tags to create or manage tags for the instance. See Create, Assign, and Unassign Tags.

Element	Description
	<ul style="list-style-type: none"> – Change License Type to change the license type of the instance (BYOL or Cloud License). See Change the License Type for an Oracle SOA Cloud Service Instance. – Delete to delete the service instance. In the Delete Instance dialog, set the following options and click Delete: <ul style="list-style-type: none"> * Force service deletion: (Optional) Select this check box if you want the service instance to be deleted even if the database deployment cannot be reached to delete the database schemas. If enabled, you may need to delete the associated database schemas manually on the database deployment if they are not deleted as part of the service instance delete operation. * Administration User Name: Enter the name of the database administrator user that was specified when the database deployment was created. This user owns the instance’s repository and schemas. If you have specified two databases, specify the name of the administrator for the database deployment for the Oracle required schema. * Password: Enter the Database Administrator user password for the database deployment that contains the Oracle required schema <p style="text-align: center;">See Delete an Oracle SOA Cloud Service Instance.</p>
Instance Create and Delete History	<p>Shows details about created or deleted instances.</p> <ul style="list-style-type: none"> • Select the time period for which you are interested in viewing created and failed service instances. • Show only failed attempts: Select this check box if you want to see failed attempts only. • Details: Displays system messages logged during the creation or deletion process. Messages include information about auto-retry attempts.

Explore the Oracle SOA Cloud Service Administration Page for Backups

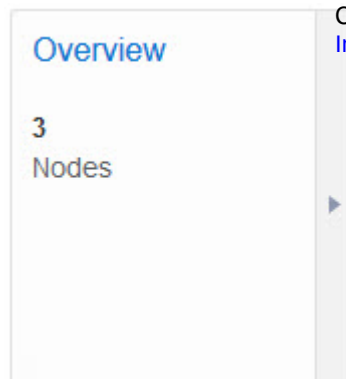
You can use the Backups tab on the Administration page to back up and restore an Oracle SOA Cloud Service instance.



Element	Description
---------	-------------






Click to view the following information about the instance:







- **Service Level**
- **Region**
- **Created By**
- **Created On**
- **Description**
- **License**
- **Identity Domain**
- **Metering Frequency**
- **Subscription id**



Click the **Overview** tile to access the [Oracle SOA Cloud Service Instance Overview page](#) at any time.

Element	Description
Summary Table	<p>The blue summary table at the top of the tab lists the following information:</p> <ul style="list-style-type: none">• Status of incremental backups, including:<ul style="list-style-type: none">– The scheduled time for incremental backups– The total amount of space, in MB or GB, that backups occupy in the Oracle Cloud Infrastructure Object Storage Classic container for storing backups. This amount includes space that is occupied by backups that have been manually uploaded to the container, if any, in addition to the space occupied by backups that Oracle SOA Cloud Service has moved there.• Status of full backups, including how much data has been used. The total amount of space, in MB or GB, that local copies of backups occupy in the backup volume on the block storage of the virtual machine where the Administration Server is running.• The size of the last successful backup as a percentage of the available space that backups occupy in the backup volume on the block storage of the virtual machine where the Administration Server is running.

Element	Description
Available Backups	<p>List of available backups. By default, only backups for the last 7 days are listed.</p> <p>Use the search fields to specify a range of dates for which you want backups returned, then click  .</p> <p>Click  to select the following actions:</p> <ul style="list-style-type: none"> • Backup Now to create an on-demand backup of the instance. See Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance. • Configure Backups to set when scheduled backups occur and to specify how backups are stored. See: <ul style="list-style-type: none"> – Update Backup and Recovery Credentials – Configure Automated Backups for an Oracle SOA Cloud Service Instance • Disable Backups to disable backups for the instance. This includes both automated and on-demand backups. • Enable Backups to reenables backups for the instance. <p>In the list of backups, the icons for each backup indicate status, with a timestamp indicating when the backup was started. Click the icon for additional information:</p> <ul style="list-style-type: none"> •  The backup is in progress. It will not be available for use in restoring the service instance until it is completed. •  The backup completed. It is available for use in restoring the instance if needed. •  The scheduled backup completed, after which Oracle SOA Cloud Service tried but failed to move or delete one or more older backups. For information about when and why Oracle SOA Cloud Service moves or deletes older backups, see Where Backups Are Stored. The backup is still available for use in restoring the service instance. <p>To find out why Oracle SOA Cloud Service could not move or remove the older backup, place the cursor over the icon.</p> <p>The presence of the older backup may cause future backups to fail because of insufficient space. For information about how to prevent future backups from failing in this way see Problems with Backup and Restoration.</p> <p>Each backup includes the following information:</p> <ul style="list-style-type: none"> • Type: A comma-separated pair of words that describes the type of the backup. The first word in the pair describes the extent of the backup: <ul style="list-style-type: none"> – Incremental—The backup contains only the runtime artifacts of each managed virtual machine in the service instance. – Full—The backup contains runtime artifacts and files that change infrequently or do not change. <p>The second word in the pair indicates how the backup was initiated:</p> <ul style="list-style-type: none"> – If the backup was initiated automatically at the scheduled time, Scheduled is displayed. – If the backup was initiated by a user, the name of the user is displayed.

Element	Description
	<ul style="list-style-type: none"> – If the backup was initiated in response to another management operation by a user, the name of the user is displayed. <p>See How Backups Are Initiated.</p> <ul style="list-style-type: none"> • Available Until: The date and time until which the backup will be retained. • Click Notes to display the notes that were provided when the backup was created or the restoration was performed. • Click  to select the following actions: <ul style="list-style-type: none"> – Restore to restore the instance from the backup. See Restore an Oracle SOA Cloud Service Instance from a Backup. – Delete to delete the backup. See Delete a Backup.
Restore History	<p>Expand to display a list of all the restoration operations on this service instance. By default, only restoration operations for the last 7 days are listed. Use the search fields to specify a range of dates for which you</p> <p style="text-align: right;"></p> <p>want restore history, then click  .</p> <p>Select Include unsuccessful restore attempts to include the unsuccessful restoration operations in the list.</p> <p>In the list of restoration operations, the icons for each restoration indicate status, with a timestamp indicating when the restoration was started. Click the icon for additional information:</p> <ul style="list-style-type: none"> •  The restoration operation completed. •  The restoration operation is in progress. •  The restoration attempt was unsuccessful. <p>Each restoration operation includes the following information:</p> <ul style="list-style-type: none"> • From Backup: The date and time when the backup from which the service instance was restored was created. • Status: The status of the restoration operation (Completed, In Progress, or Failed). Click the status to see detailed status messages for the operation. • Click Notes to display the notes that were provided when the backup was created or the restoration was performed.

Explore the Oracle SOA Cloud Service Administration Page for Patching

The Patching tab on the Administration page of the Oracle SOA Cloud Service Console is not supported by Oracle SOA Cloud Service.

This page is not used for patching Oracle SOA Cloud Service instances. Instead, refer to [About Managing Patches for Instances Provisioned With Earlier Releases](#).


The screenshot shows the Oracle SOA Cloud Service console for instance `sobl2soacs`. The **Patching** tab is active, displaying a warning: "Last activity BACKUP Apr 14, 2021 8:10:04 AM UTC failed. See the activity log for Details". Below this, the **Available Patches** section shows "No patches available." and the **Patch and Rollback History** section shows "No patches applied." The left sidebar includes an **Administration** section with 0 patches available and a note that the most recent backup on Apr 14, 2021 8:10:07 AM UTC failed.

Explore the Oracle SOA Cloud Service Activity Page

You can use the Activity page to search for and review Oracle SOA Cloud Service activities that have occurred in your identity domain. To access this page, click the Activity tab in the Oracle SOA Cloud Service Console.

The screenshot displays the **SOA Cloud Service Activity** page. It includes a search filter for "Search Activity Log" with the following parameters: Start Time Range (4/14/2021 12:18 AM), Search to Time, Service Type (SOA Cloud Service), Operation Status (All), and Instance Name. The results table shows 9 results as of Apr 15, 2021 12:18:29 AM UTC.

Operation	Instance Name	Service Type	Operation Status	Start Time	End Time	Initiated By
Delete Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 5:42:28 PM UTC	Apr 14, 2021 5:59:12 PM UTC	O.CLOUD9...
Scale Application	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 5:19:22 PM UTC	Apr 14, 2021 5:24:04 PM UTC	O.CLOUD9...
Scale Application	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 4:56:17 PM UTC	Apr 14, 2021 5:01:37 PM UTC	O.CLOUD9...
Scale In	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 4:07:58 PM UTC	Apr 14, 2021 4:42:43 PM UTC	O.CLOUD9...
Start Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 3:28:59 PM UTC	Apr 14, 2021 3:47:29 PM UTC	O.CLOUD9...
Stop Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 3:25:57 PM UTC	Apr 14, 2021 3:28:18 PM UTC	O.CLOUD9...
Scale Out	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 2:13:41 PM UTC	Apr 14, 2021 3:25:44 PM UTC	O.CLOUD9...
Create Service	sob1221311test	SOA Cloud Service	Succeeded	Apr 14, 2021 10:39:53 AM UTC	Apr 14, 2021 1:53:38 PM UTC	O.CLOUD9...
Back Up	sobl2soacs	SOA Cloud Service	Failed	Apr 14, 2021 8:10:04 AM UTC	Apr 14, 2021 8:24:29 AM UTC	System

Element	Description
Search Activity Log	<p>Details about search activity:</p> <ul style="list-style-type: none"> • Start Time Range: Set date values to list only operations started within a specified time range. The range defaults to the previous 24 hours. • Operation Status: Select one or more status types to list operations of only the selected status types: <ul style="list-style-type: none"> – All (default) – Scheduled – Running – Succeeded – Failed • Instance Name: Enter an instance name to list operations only for that instance. You can enter a full or partial service instance name. • Service Type: Select a service type to list operations only for instances of that service type. The default value is the current cloud service type. • Operation: Select one or more to list only those operations. You can select any subset of the given operations. Default: All.
Search	Searches for activities by applying the filters specified by the fields above, and displays matching operations in the list.
Reset	Clears the Start Time Range and Instance Name fields, and returns the Operation Status and Operation fields to their default values.
Results per page	Select the number of results you want to view per page. The default value is 10.
	Click next to an operation to show and hide status messages for the operation.

Explore the Oracle SOA Cloud Service IP Reservations Page



This topic applies only to Oracle Cloud Infrastructure Classic.

You can use the IP Reservations page to search for and view the existing IP reservations. To access this page, click the IP Reservations tab in the Oracle SOA Cloud Service Console.

Element	Description
Search IP Reservations by name or region	Enter a full or partial IP reservation name or region name and click the search icon to search for a particular IP reservation.
Create	Create a new IP reservation. See Create an IP Reservation .

About Oracle SOA Cloud Service Instances in Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic

You can create Oracle SOA Cloud Service instances in Oracle Cloud Infrastructure and in Oracle Cloud Infrastructure Classic.

Topics:

- [Oracle Cloud Infrastructure](#)
- [Oracle Cloud Infrastructure Classic](#)
- [Differences Between Instances in Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic](#)
- [Differences Between Instances in Oracle Cloud at Customer and Oracle Cloud Infrastructure](#)
- [Workflow for Creating an Instance in Oracle Cloud Infrastructure](#)

Oracle Cloud Infrastructure

Oracle Cloud Infrastructure combines the elasticity and utility of public cloud with the granular control, security, and predictability of on-premises infrastructure to deliver high-performance, high availability, and cost-effective infrastructure services.

Depending on the shape you select for the Oracle SOA Cloud Service region during instance provisioning, Oracle Cloud Infrastructure provides you with dedicated physical server access for the highest performance and strongest isolation.

Oracle Cloud Infrastructure Classic

Oracle Cloud Infrastructure Classic is an enterprise-grade service that provides a rapidly provisioned virtual compute environment to easily migrate Oracle workloads and run them at scale with deployment options and predictable performance.

The underlying compute environment is a *virtual machine* (VM). A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other. VMs are ideal for running applications that do not require the performance and resources (CPU, memory, network bandwidth, storage) of an entire physical machine.

Differences Between Instances in Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic

The Oracle WebLogic Server environment that your Oracle SOA Cloud Service instance provides in either type of infrastructure is substantially the same. A few differences exist in the underlying infrastructure components and in the supported capabilities. Awareness of these differences will help you choose an appropriate region while creating the instance.

Feature	Oracle Cloud Infrastructure	Oracle Cloud Infrastructure Classic
Availability domains	Each region has multiple isolated availability domains, with separate power and cooling. The availability domains within a region are interconnected using a low-latency network. When creating an instance, you can select the availability domain in which the instance should be placed.	Not applicable.
Compute shapes	VM.Standard.* and BM.Standard.* shapes. Note: The list of available shapes may vary by region.	Standard and high memory shapes. Note: The list of available shapes may vary by region.
Networking	You <i>must</i> attach each instance to a subnet, in a virtual cloud network created in Oracle Cloud Infrastructure.	You <i>can</i> attach instances to IP networks defined in Oracle Cloud Infrastructure Compute Classic.
Reserving public IP addresses	Not supported.	Supported.
Scaling the shape of a node	Not supported.	Supported.
Adding block storage	The minimum size and scaling increment of block storage volumes is in multiples of 50 GB.	The minimum size and scaling increment for block storage volumes is 1 GB.
Managing access rules	Configure security rules in the Oracle Cloud Infrastructure interfaces.	Use the Oracle SOA Cloud Service Console to configure access rules.
Object storage for backups	You must create the object storage bucket in Oracle Cloud Infrastructure before creating the instance.	You can create the object storage container either before or during instance creation.
Billing	Oracle Cloud Infrastructure services can only be billed through Universal Credit Service accounts. Existing Universal Credit Service accounts can be used.	You can buy Oracle SOA Cloud Service on a metered or non-metered basis.

Differences Between Instances in Oracle Cloud at Customer and Oracle Cloud Infrastructure

- **External database:** External database support is not available on Oracle Cloud at Customer.
- **Public access network and database network:** Option to specify the public access network and database network while provisioning is not available on Oracle Cloud at Customer.
- **NFS remote backup:** Option to specify NFS remote backup is not available on Oracle Cloud at Customer.
- **Domain and database backup:** Both domain and database backup are supported on Oracle Cloud at Customer.

Workflow for Creating an Instance in Oracle Cloud Infrastructure

Task	More Information
Create the required network, storage, and security resources in Oracle Cloud Infrastructure.	<ul style="list-style-type: none"> To learn about these resources, see Prerequisites for Oracle Platform Services in the Oracle Cloud Infrastructure documentation. For step-by-step instructions to create these resources, see Creating the Infrastructure Resources Required for Oracle Platform Services.
Create the Oracle SOA Cloud Service instance.	See Provision an Oracle SOA Cloud Service Instance

About Managing Oracle SOA Cloud Service Instances

Following best practices ensures that your Oracle SOA Cloud Service instances are manageable.

Reliable management of Oracle SOA Cloud Service instances requires a specific software environment that includes service instances of Oracle Database Classic Cloud Service and Oracle Cloud Infrastructure Object Storage Classic, and a secure shell (SSH) public key. For details on these features, see [Prerequisites](#).

To keep your service instances manageable by Oracle SOA Cloud Service, follow these guidelines:

- To ensure that you can restore the database for an Oracle SOA Cloud Service instance without risking data loss for other service instances, do **not** use the same Oracle Database Classic Cloud Service as a Service instance with multiple Oracle SOA Cloud Service instances. Backups of an Oracle Database Cloud Service instance that are used with multiple Oracle SOA Cloud Service instances contain data for all the Oracle SOA Cloud Service instances. If you restore the database while restoring an Oracle SOA Cloud Service instance, data for all the Oracle SOA Cloud Service instances is restored.
- Do not use an Oracle Cloud Infrastructure Object Storage Classic container that you use for backups of Oracle SOA Cloud Service instances for any other purpose. For example, do not use it to back up Oracle Database Classic Cloud Service instances. Using the container for multiple purposes can result in billing errors.
- Apply only patches that are applicable for Oracle SOA Cloud Service. This includes Patch Set Updates (PSUs) and Oracle SOA Cloud Service bundle patches.
- Use only the default domain that was provisioned when a service instance was created. Do not add any Oracle WebLogic Server domains to the service instance.
- If you plan to integrate multi-domain environments, ensure that the first eight characters of your Oracle SOA Cloud Service 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 Cloud Service instance are generated from the first eight characters of the Oracle SOA Cloud Service instance name, and will use the following formats, respectively:

- `first8charsOfServiceInstanceName_domain`
- `first8charsOfServiceInstanceName_cluster`

See *Administering JMS Resources for Oracle WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

- Add Managed Servers to a service instance only by scaling out the Oracle WebLogic Server cluster in the service instance. Do not use Oracle WebLogic Server administrative interfaces for this purpose.

For information about how to scale out the cluster in a service instance, see [Scale Out an Oracle SOA Cloud Service Cluster](#).

- Add Oracle WebLogic Server clusters to a service instance only by using the Oracle SOA Cloud Service REST API for scaling out a service instance. Do not use Oracle WebLogic Server administrative interfaces for this purpose.

For information about the REST API for scaling out a service instance, see REST API for Oracle SOA Cloud Service.

- Do not attach custom storage volumes to a service instance's VMs.

Any custom storage volumes that you attach are detached if the service instance is restarted.

If a service instance requires additional storage, add storage by scaling the service instance's cluster as explained in [Scale Out an Oracle SOA Cloud Service Cluster](#).

- For any disk volume that Oracle SOA Cloud Service attaches to an service instance VMs during creation of the service 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 service 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 a service instance.

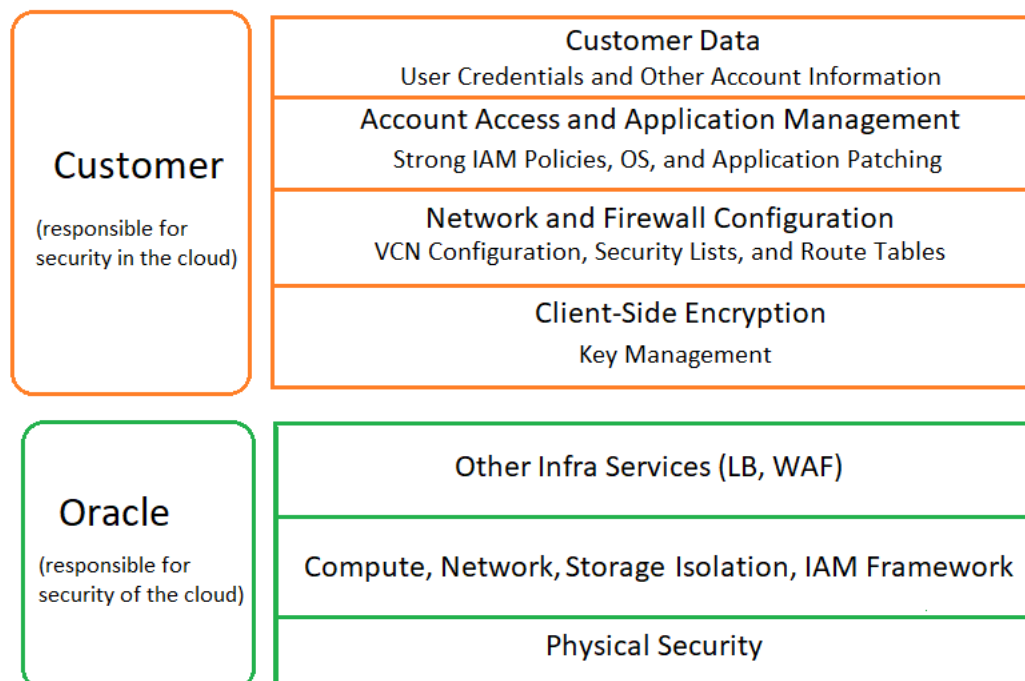
See [About the Default Access Ports](#).

- Do not detach NAT IP addresses from any of a service instance's VMs.
- Do not change the Oracle Fusion Middleware component schemas with which a service instance was provisioned.
- Do not change the ports for the Oracle WebLogic Server administration server and the Oracle Traffic Director administration server.
- Do not change OS users and SSH key settings that Oracle SOA Cloud Service configured during creation of a service instance.

About Security

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 and Oracle Cloud Infrastructure Classic 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. Instances within a security list can inter-communicate freely over any protocol.
- For Oracle Cloud Infrastructure Classic instances:
 - To allow incoming traffic to all the instances in a security list, set up a security rule with the security list as the destination and with the required source and protocol settings.
 - Use security rules carefully and open only a minimal and essential set of ports. Keep in mind your business needs and the IT security policies of your organization.
 - When you add an instance to a security list, all the security rules that use that security list—as either the source or destination—are applicable to the instance. Consider a security list that is the destination in two security rules, one rule that allows SSH access from the public Internet and another rule permitting HTTPS traffic from the public Internet. When you add an instance to this security list, the instance is accessible from the public Internet over both SSH and HTTPS. Keep this in mind when you decide the security lists that you want to add an instance to.
- 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 Cloud Service instances up-to-date with the latest software bundle patches.

The following types of patches apply to your Oracle SOA Cloud Service instances:

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

SOA Bundle Patches

When you provision a new Oracle SOA Cloud Service 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.

Apply only patches that are applicable for Oracle SOA Cloud Service. This includes Patch Set Updates (PSUs) and Oracle SOA Cloud Service bundle patches.

To retrieve a list of SOA bundle patches that have been applied to your Oracle SOA Cloud Service instance:

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

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

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Enter the following command:

```
cat /u01/app/oracle/tools/downloadBinaries/soacs/  
toponame_version_patches.txt
```

For example:

```
cat /u01/app/oracle/tools/downloadBinaries/soacs/  
20.3.1.0.0_soaosbb2b_12.2.1.4_patches.txt
```

Example Output:

```
["p30549478_122140_Generic.zip", "p31396632_122140_Generic.zip"]
```

Applying bundle patches to existing instances may involve multiple Oracle SOA Cloud Service instances that were provisioned at different times that may include different bundle patches. Contact [Oracle Support](#) for information about the latest Oracle SOA Cloud Service certified patches and instructions on how to apply the patches.



Note:

You can find the current list of Oracle SOA Cloud Service 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 [Step 1: Apply the Latest Patch Set Update for WebLogic Server](#).

Operating System Patches

Oracle SOA Cloud Service does not provide cloud tooling to patch the operating system for the nodes in a service instance. You are responsible for installing any operating system patches. Refer to your operating system patching documentation for information.

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.
- 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 Cloud Service Roles and Responsibilities between Oracle and Customer

This table summarizes the division of roles and responsibilities for Oracle SOA Cloud Service.

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"> • Instance provisioning and deprovisioning • Backup and restore • Scale out, scale in, scale up, scale down • Start and stop • Patching 	A	R, A	Customer provisions the Oracle SOA Cloud Service instance and is responsible for all lifecycle operations. Customer manually applies operating system, Oracle SOA Cloud Service, 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.

Task	Oracle's Role	Customer's Role	Comments
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	

About the Infrastructure Resources Used by Oracle SOA Cloud Service

When you create an Oracle SOA Cloud Service instance, the required virtual machines (VMs), block storage volumes, and most of the network settings are provisioned and configured for you.

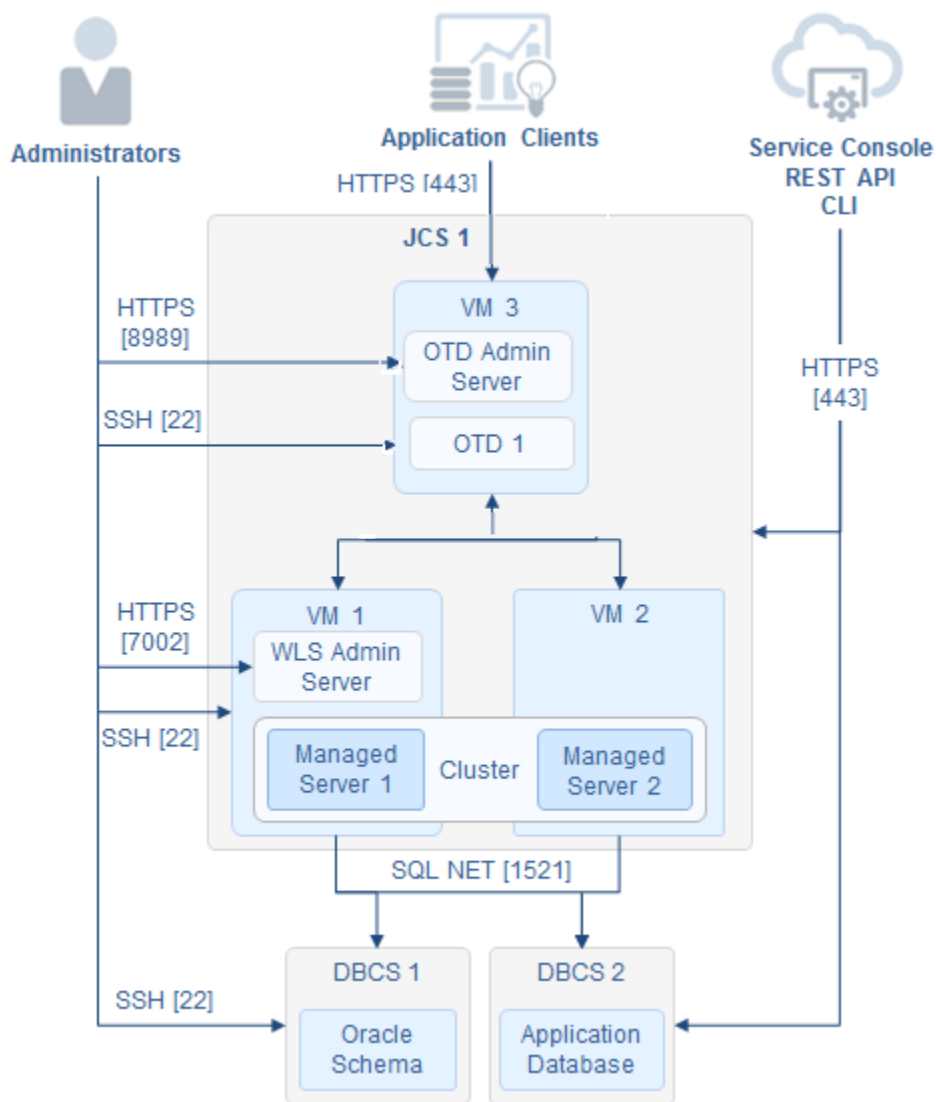
Topics:

- [About the Deployment Topology of Virtual Machines](#)
- [About the Compute Nodes](#)
- [About the Disk Volumes](#)

About the Deployment Topology of Virtual Machines

Using Oracle SOA Cloud Service simplifies the work you've to do in order to provision and configure an Oracle WebLogic Server domain and cluster, and Oracle Traffic Director as the software load balancer.

The following illustration shows an example of the Oracle SOA Cloud Service virtual machine (VM) deployment topology that is set up and configured for you when you provision an Oracle SOA Cloud Service instance with two Managed Servers and also enable a load balancer:



 **Note:**

For information about the network protocols and default ports that can be used from within Oracle Cloud and from outside Oracle Cloud, see [About the Default Access Ports](#). Note that the HTTP port is disabled if you created the Oracle SOA Cloud Service instance by using the service instance creation wizard available through the Oracle SOA Cloud Service Console.

As shown in the illustration, an Oracle SOA Cloud Service instance is a single Oracle WebLogic Server domain that consists of one WebLogic Administration Server and one WebLogic Server cluster of Managed Servers for hosting applications. The example in the topology illustration shows a cluster of two Managed Servers.

About the Compute Nodes

The compute nodes in an Oracle SOA Cloud Service instance run Oracle Linux 6. These virtual machines are highly available and the underlying infrastructure contains built-in capabilities to migrate an unhealthy node to a separate hardware cluster.

Each Oracle SOA Cloud Service instance that you create can contain one or more nodes. The first node always contains the WebLogic Administration Server and the first Managed Server. Each remaining Managed Server runs in its own node. When the service instance is scaled out, each additional Managed Server is also on its own node.

If a local load balancer is enabled for a service instance, the Oracle Traffic Director administration server is in a separate node.

When using the Oracle SOA Cloud Service web console to create an instance, you can create up to four Managed Servers in the cluster. The following table summarizes the number of Managed Servers you can have in the WebLogic Server cluster, and the corresponding nodes:

Compute Node	1–Node Cluster	2–Node Cluster	4–Node Cluster
1st node	Contains WebLogic Administration Server and Managed Server 1	Contains WebLogic Administration Server and Managed Server 1	Contains WebLogic Administration Server and Managed Server 1
2nd node		Contains Managed Server 2	Contains Managed Server 2
3rd node			Contains Managed Server 3
4th node			Contains Managed Server 4
5th node	If present, this node contains the load balancer's administration server	If present, this node contains the load balancer's administration server	If present, this node contains the load balancer's administration server

Note:

By default a load balancer is not enabled for a service instance that has a single-node cluster in the WebLogic Server domain, so the Oracle Traffic Director node won't be present. When you create a service instance that consists of a multinode cluster in the domain, Oracle recommends that you enable a load balancer for the service instance. If enabled, the Oracle Traffic Director node would be present.

Appropriate security rules are configured on the Oracle SOA Cloud Service nodes to enable communication among the different nodes hosting the WebLogic managed servers, and also with the Oracle Traffic Director nodes and the Oracle Database Classic Cloud Service nodes.

You have access to all the compute nodes, including the node on which the WebLogic Administration Server is running. You can use a Secure Shell (SSH) client to log into a node, as described in [Access a VM Through a Secure Shell \(SSH\)](#).

About the Disk Volumes

You have access to all the virtual machine instances created for Oracle SOA Cloud Service, including the virtual machine on which the WebLogic Administration Server is running.

The following table lists the disk volumes that are attached to Oracle SOA Cloud Service virtual machines and the mount points:

Disk Volume	Purpose	Mount Point
Boot/OS volume	The boot volume as provided by the machine image. Contains the OS binaries.	Local disk, no mount point
Backup volume	Contains a copy of backups up to seven days old.	/u01/data/backup
DOMAIN_HOME	Contains data for the domain corresponding to the Oracle SOA Cloud Service instance.	/u01/data/domains
APPLICATION_HOME	Contains deployed applications and application configuration files.	/u01/data/domains
MW_HOME	Contains Oracle WebLogic Server binaries and Oracle Traffic Director binaries.	/u01/app/oracle/ middleware
JCS_RESERVED	Contains files required by Oracle SOA Cloud Service, that is, any binaries and related metadata that are required by the Oracle SOA Cloud Service management layer.	/u01/app/oracle/tools Caution: Do not modify any scripts in the /u01/app/oracle/tools directory.
JDK_HOME	Contains JDK binaries.	/u01/jdk

 **Note:**

- All volumes under /u01, except `DOMAIN_HOME` and `APPLICATION_HOME`, should be treated as read-only volumes.
- The Backup volume is writable by the `oracle` user; the `opc` user has read-only access.
- The Boot/OS volume of any service instance provisioned before the mid-August 2015 update to Oracle SOA Cloud Service is an ephemeral disk volume. Content added to an ephemeral Boot/OS volume does not persist if the service instance is restarted. If the Boot/OS volume is ephemeral, the entire Boot/OS volume, including the `home` directory of the `opc` user, might be recreated from the machine image (for example, when an infrastructure patch is applied or the service instance is restarted).
- The Boot/OS volume of any service instance provisioned before the mid-August 2015 update to Oracle SOA Cloud Service is persistent. Content added to a persistent Boot/OS volume is retained if the service instance is restarted.

3

Before You Begin

Before provisioning an Oracle SOA Cloud Service instance, learn about the Oracle SOA Cloud Service architecture, understand the prerequisites, sign in to the Oracle SOA Cloud Service Console, and generate an SSH key pair.

Topics:

- [About Oracle SOA Cloud Service Architecture](#)
- [Prerequisites](#)
- [Access the Oracle SOA Cloud Service Console](#)
- [Generate a Secure Shell \(SSH\) Public/Private Key Pair](#)

About Oracle SOA Cloud Service Architecture

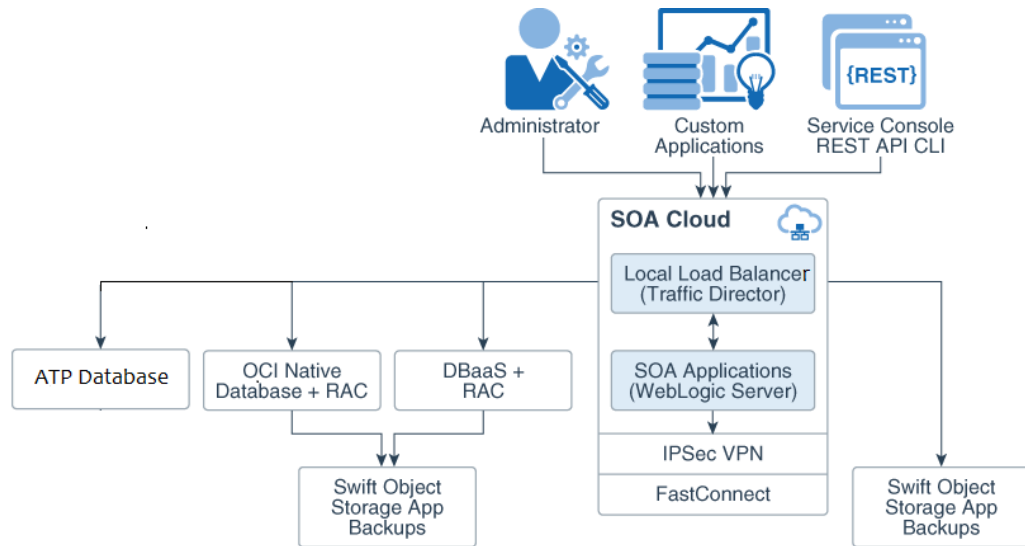
Before creating an Oracle SOA Cloud Service instance, there are architecture details you should consider in order to create the service instance that best meets your requirements.

Topics:

- [About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure](#)
- [About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure Classic](#)

About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure

The following figure illustrates the components that make up a typical Oracle SOA Cloud Service service instance on Oracle Cloud Infrastructure.



Topics:

- [Region](#)
- [Availability Domain](#)
- [Subnet](#)
- [Software Release](#)
- [Database](#)
- [Backup Location](#)
- [Load Balancer](#)

Region

If your identity domain is enabled for regions, you can select a region in which your Oracle SOA Cloud Service instance will reside.

For a list of available regions, see [Data Regions for Platform and Infrastructure Services](#).

When you select an Oracle Cloud Infrastructure region for a service instance, you must also select an Availability Domain. See [Regions and Availability Domains](#) in the Oracle Cloud Infrastructure documentation.

Availability Domain

An availability domain consists of a set of data centers within an Oracle Cloud Infrastructure region.

A region can have multiple isolated availability domains with separate power and cooling, for example. The availability domains within a region are interconnected via a low-latency network. See [Regions and Availability Domains](#) in the Oracle Cloud Infrastructure documentation.

Subnet

A subnet is a subdivision of a cloud network. Each subnet exists in a single availability domain and consists of a contiguous range of IP addresses that do not overlap with other subnets in the cloud network.

You can create your own subnet before you provision an Oracle SOA Cloud Service instance. See *VCNs and Subnets* in the Oracle Cloud Infrastructure documentation.

For convenience, if you do not explicitly select a subnet (**No Preference**), then the service instance is assigned to a subnet in the predefined Virtual Cloud Network (VCN) named `svc-vcn`, which is found in the compartment named `ManagedCompartmentForPaaS`. You cannot modify these predefined subnets, such as assigning a custom security list. If you prefer more control over the network configuration for your service instance, then create a custom subnet.

You must satisfy certain subnet and policy prerequisites when you create a subnet for use with Oracle SOA Cloud Service instances. See *Prerequisites for Oracle Platform Services* in the Oracle Cloud Infrastructure documentation.

Software Release

You can select the following Oracle WebLogic Server releases.

- Oracle WebLogic Server 12c (12.2.1.4.0)
See [Understanding Oracle WebLogic Server](#) and [Documentation Update History](#) in *What's New in Oracle WebLogic Server* for 12c (12.2.1.4.0).
- Oracle WebLogic Server 12c (12.2.1.3.0)
See [Understanding Oracle WebLogic Server](#) and [Documentation Update History](#) in *What's New in Oracle WebLogic Server* for 12c (12.2.1.3.0).

With Oracle SOA Cloud Service, you can easily apply patches to an existing service instance.

Oracle has simplified the cloud provisioning policy to align with the WebLogic Server error correction support policy. Service instance provisioning will now end on the same day as the error correction end date for the corresponding WebLogic release.

This is specific to the provisioning of WebLogic instances through Oracle SOA Cloud Service and that this change has no impact on the use of these WebLogic releases within on-premises environments or within Oracle Cloud IaaS environments.

More information about this change can be found in the [Oracle Fusion Middleware Lifetime Support Policy](#) document and [Error Correction Support Dates for Oracle WebLogic Server](#) Support Note.

Database

Every service instance must be associated with an existing relational database in Oracle Cloud. Oracle SOA Cloud Service provisions the required infrastructure schema on the selected database.

The supported database services in Oracle Cloud vary by region. For an Oracle Cloud Infrastructure region, the infrastructure schema database options are shown in the following table.



Note:

If you specify **No Preference** for your region, or if you have an older Oracle Cloud account that doesn't include regions, then you can choose from the same database options as [Oracle Cloud Infrastructure Classic](#).

Database	Supported Versions	Additional Information
<p>Oracle Cloud Infrastructure database, with or without Oracle Real Application Clusters (RAC) If you want to use RAC, you will need to create an Oracle Cloud Infrastructure database instance using the standard service level and Enterprise Edition Extreme Performance for the Oracle Database software edition.</p> <p>Note: Exadata Cloud Service on Oracle Cloud Infrastructure is not supported.</p>	<ul style="list-style-type: none"> • Oracle Database 19c • Oracle Database 18c • Oracle Database 12c release 2 (12.2.0.1) and release 1 (12.1.0.2) • Oracle Database 11g Release 2 	<p>See Oracle Cloud Infrastructure Database Limitations and Usage Notes, below.</p>
<p>Oracle Autonomous Transaction Processing (ATP) database</p>	<ul style="list-style-type: none"> • Oracle Database 19c • Oracle Database 18c 	<p>See Oracle Autonomous Transaction Processing (ATP) Database Limitations and Usage Notes, below.</p> <p>More Information:</p> <ul style="list-style-type: none"> • Provision Autonomous Database in <i>Using Oracle Autonomous Database on Shared Exadata Infrastructure</i>

General Usage Notes

- All databases must be in an active state and not currently in the process of being provisioned. The WebLogic Server domain in a service instance uses Java Database Connectivity (JDBC) to access the databases.
- To ensure that you can restore the database for an Oracle SOA Cloud Service instance without risking data loss for other service instances, Oracle recommends that you do not associate the same infrastructure schema database (or the same pluggable database) with multiple service instances. Backups of a database that is used with multiple Oracle SOA Cloud Service instances contain data for all the instances. Therefore, if you restore the database from a backup, data for all the service instances is restored, which might not be the intended result.

General Limitations

- Database instances in Oracle Database Classic Cloud Service and Oracle Cloud Infrastructure database must be in the same region and virtual cloud network (VCN) as the Oracle SOA Cloud Service instance. The database and service instance do not need to be in the same subnet or availability domain, but it might be necessary to create and assign security rules to the subnets in order to enable communication between them. The database and service instance can be on different VCNs only if you configure VCN peering. See VCNs and Subnets in the Oracle Cloud Infrastructure Documentation.

- When creating a service instance with the Oracle SOA Cloud Service Console, database instances in Oracle Cloud Infrastructure database and Oracle Autonomous Transaction Processing (ATP) database must be in a compartment that is directly under the root compartment. This restriction does not apply to service instances created with the REST API or CLI.

Oracle Cloud Infrastructure Database Limitations and Usage Notes

- Oracle SOA Cloud Service uses an Oracle Cloud Infrastructure database to host the Oracle Fusion Middleware component schemas required by Oracle Java Required Files (JRF). Make sure you have quota to create an Oracle Cloud Infrastructure database.
- Oracle SOA Cloud Service provisioned with the Oracle Cloud Infrastructure database supports only **Oracle Grid Infrastructure** storage management software. Oracle SOA Cloud Service is not supported with an Oracle Cloud Infrastructure database using **Logical Volume Manager (LVM)** storage management software.
- To use Oracle Cloud Infrastructure database, you must assign a custom subnet to your service instance. The default subnet is not supported.
- 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 Cloud Service 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

Name	Type	JNDI Name	Targets
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
SOADDataSource	GridLink	jdbc/SOADDataSource	soaRACNo_cluster

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

- To use an Oracle Autonomous Transaction Processing (ATP) database, the service instance must be running WebLogic Server 12.2.1.3 or later.
- Oracle SOA Cloud Service supports the Database Adapter for the ATP database. See "Oracle JCA Adapter for Database" in *Understanding Technology Adapters* (12.2.1.4 | 12.2.1.3).
- A minimum of two OCPU ATP databases is recommended.
- Oracle SOA Cloud Service supports only *serverless deployments* of the ATP database. It does not support *dedicated deployments*.
- DBFS is not configured when using ATP-D.
- The Oracle Autonomous Transaction Processing database is *not* supported with the **MFT Cluster** or **Business Activity Monitoring** service types.
- Oracle Enterprise Scheduler (ESS) is not included in the provisioned Oracle SOA Cloud Service instance with the Oracle Autonomous Transaction Processing database.
- DBFS mount points are not created during provisioning for large Oracle B2B payloads.
- Coordinated database backups with the Oracle SOA Cloud Service instance are not supported.

Backup Location

Backups are recorded to a specified object storage location in Oracle Cloud.

For a service instance in an Oracle Cloud Infrastructure region, you must create this storage bucket manually.

See [Create an Object Storage Container](#).

Load Balancer

A load balancer routes requests it receives from clients to the WebLogic Servers configured in a service instance.

Using a load balancer within your service instance is recommended if you are configuring more than one Managed Server or more than one cluster. A load balancer

also gives you the ability to suspend access to a service instance temporarily to perform routine maintenance.

Oracle SOA Cloud Service in Oracle Cloud Infrastructure supports two load balancer options:

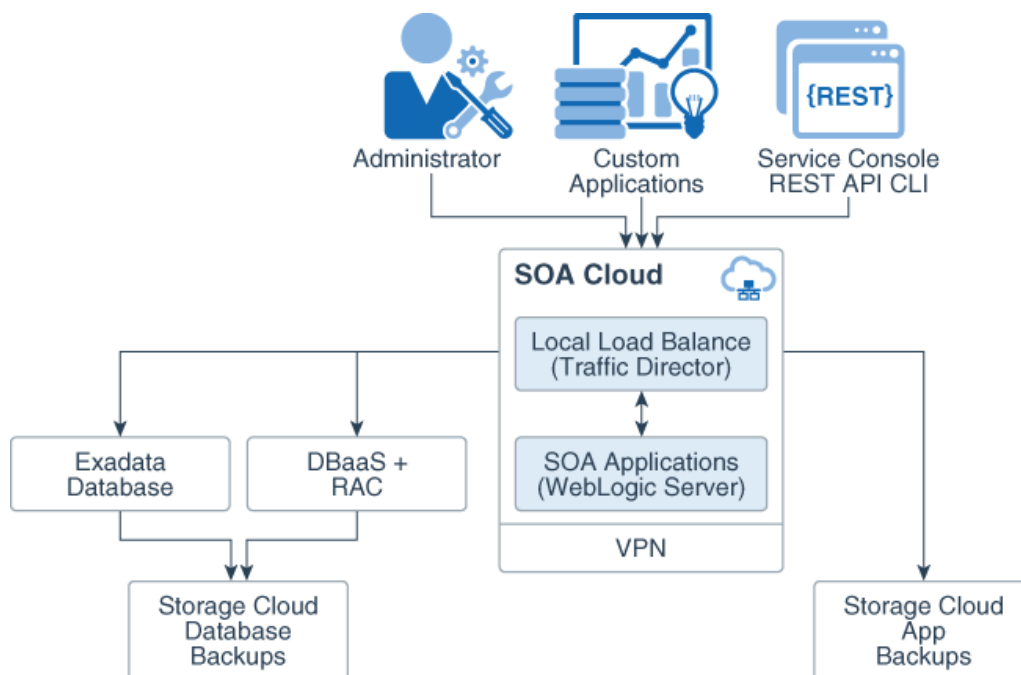
- A user-managed load balancer that runs within your service instance. You can access, patch, and administer this type of load balancer like other nodes in your service instance. This load balancer is an instance of Oracle Traffic Director (OTD) and is administered through the Load Balancer Console. A service instance can include zero or one nodes running OTD. Each load balancer node is assigned a separate public IP address.
- An Oracle-managed load balancer that is automatically patched and maintained by Oracle. This load balancer can be configured after provisioning your Oracle SOA Cloud Service instance in the region where the service instance is created. See [Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning](#).

The Oracle-managed Oracle Cloud Infrastructure load balancer is automatically deployed on multiple nodes to provide high availability and is accessed by clients using a single public IP address. The configuration options vary by region:

- You can assign a subnet to each load balancer node. For high availability, Oracle recommends that each subnet be associated with a different availability domain in the selected region. If the selected region has one availability domain, you can specify only one subnet, which is assigned to both load balancer nodes.
- You can choose to create a public or private Oracle-managed load balancer. A private load balancer cannot be accessed from the public Internet. It is for use cases where you only intend to access your service instance from within your private cloud network or from your on-premises data center over a VPN network.

About Oracle SOA Cloud Service Architecture in Oracle Cloud Infrastructure Classic

The following figure illustrates an Oracle SOA Cloud Service instance on Oracle Cloud Infrastructure Classic.



Topics:

- [Region](#)
- [IP Network](#)
- [Software Release](#)
- [User Authentication](#)
- [Database](#)
- [Backup Location](#)
- [Load Balancer](#)

Region

If your identity domain is enabled for regions, you can select a region in which your Oracle SOA Cloud Service instance will reside.

For a list of available regions, see [Data Regions for Platform and Infrastructure Services](#).

When you select an Oracle Cloud Infrastructure Classic region for a service instance, you can also select an IP Network and assign reserved IP addresses to your nodes. If you don't explicitly select a region (**No Preference**), you cannot select an IP network or use reserved IPs.

IP Network

If you select a specific Oracle Cloud Infrastructure Classic region for your service instance, then you can also select an IP network in that region. Using an IP network gives you more control over the configuration of the network in which your service instance is placed.

By default, if you select an IP network, each underlying node is auto-assigned a public and private IP address. As a result, the IP address might change each time a service instance is started. To assign fixed public IP addresses to instances attached to the IP network, you can create and use IP reservations.

When you select an IP network during provisioning, you must also select a Oracle Database Classic Cloud Service instance that is on an IP network. If the Oracle SOA Cloud Service and Oracle Database Classic Cloud Service are attached to different IP networks, then the two IP networks must be connected to the same IP network exchange. The required access rules for the Oracle SOA Cloud Service instance and Oracle Database Classic Cloud Service database deployment to communicate are created automatically.

If you want to create a service instance that uses an IP network and also includes an Oracle-managed load balancer running on Oracle Cloud Infrastructure Load Balancing Classic, you must first attach an Internet-facing load balancer to the IP network. A service instance uses an Oracle-managed load balancer when you enable authentication with Oracle Identity Cloud Service.

See [Creating an IP Network](#) in *Using Oracle Cloud Infrastructure Compute Classic* (ignore information in this topic about the Compute API and orchestrations).

Software Release

You can select the following Oracle WebLogic Server releases.

- Oracle WebLogic Server 12c (12.2.1.4.0)
See [Understanding Oracle WebLogic Server](#) and [Documentation Update History](#) in *What's New in Oracle WebLogic Server* for 12c (12.2.1.4.0).
- Oracle WebLogic Server 12c (12.2.1.3.0)
See [Understanding Oracle WebLogic Server](#) and [Documentation Update History](#) in *What's New in Oracle WebLogic Server* for 12c (12.2.1.3.0).

With Oracle SOA Cloud Service, you can easily apply patches to an existing service instance.

Oracle has simplified the cloud provisioning policy to align with the WebLogic Server error correction support policy. Service instance provisioning will now end on the same day as the error correction end date for the corresponding WebLogic release.

This is specific to the provisioning of WebLogic instances through Oracle SOA Cloud Service and that this change has no impact on the use of these WebLogic releases within on-premises environments or within Oracle Cloud IaaS environments.

More information about this change can be found in the [Oracle Fusion Middleware Lifetime Support Policy](#) document and [Error Correction Support Dates for Oracle WebLogic Server](#) Support Note.

User Authentication

By default, the WebLogic Server domain in a service instance is configured to use the local WebLogic identity store to maintain administrators, application users, groups, and roles. These security elements are used to authenticate users and also to authorize access to tools like the WebLogic Server Administration Console.

Database

Every service instance must be associated with an existing relational database in Oracle Cloud. Oracle SOA Cloud Service provisions the required infrastructure schema on the selected database.

The supported database services in Oracle Cloud vary by region. For an Oracle Cloud Infrastructure Classic region, the infrastructure schema database options are shown in the following table.



Note:

If you specify **No Preference** for region, or if you have an older Oracle Cloud account that doesn't include regions, then you can also choose these same database options.

Database	Supported Versions	Additional Information
<p>Oracle Database Classic Cloud Service, with or without Oracle Real Application Clusters (RAC)</p> <p>Note: If you want to use RAC, you will need to create an Oracle Database Classic Cloud Service instance using the standard service level and Enterprise Edition Extreme Performance for the Oracle Database software edition.</p>	<ul style="list-style-type: none"> Oracle Database 12c release 1 (12.1.0.2) Oracle Database 12c release 2 (12.2.0.1) 	<p>See Oracle Database Classic Cloud Service Limitations and Usage Notes, below.</p> <p>More Information:</p> <ul style="list-style-type: none"> <i>Administering Oracle Database Classic Cloud Service</i> for information about subscribing to Oracle Database Classic Cloud Service, provisioning Oracle Database Classic Cloud Service instances, and using Oracle RAC in Database as a Service.
<p>Oracle Database Exadata Cloud Service</p>	<ul style="list-style-type: none"> Oracle Database 12c Release 2 Oracle Database 12c Release 1 Oracle Database 11g Release 2 	<p>See Oracle Database Exadata Cloud Service Limitations and Usage Notes, below.</p> <p>More Information:</p> <ul style="list-style-type: none"> Managing Exadata DB Systems in the Oracle Cloud Infrastructure documentation Creating a Customized Database Deployment in <i>Administering Oracle Database Exadata Cloud Service</i>

General Usage Notes

- All databases must be in an active state and not currently in the process of being provisioned. The WebLogic Server domain in a service instance uses Java Database Connectivity (JDBC) to access the databases.
- To ensure that you can restore the database for an Oracle SOA Cloud Service instance without risking data loss for other service instances, Oracle recommends that you do not associate the same infrastructure schema database (or the same pluggable database) with multiple service instances. Backups of a database that is used with multiple Oracle SOA Cloud Service instances contain data for all the

instances. Therefore, if you restore the database from a backup, data for all the service instances is restored, which might not be the intended result.

General Limitations

- If you specify an IP network for a service instance, the infrastructure schema database for the Oracle SOA Cloud Service instance must also be attached to an IP network. If the service instance and the database are attached to different IP Networks, the two IP networks must be connected to the same IP network exchange. See [Create an IP Network](#) in *Using Oracle Cloud Infrastructure Compute Classic*.

Oracle Database Classic Cloud Service Limitations and Usage Notes

- Oracle SOA Cloud Service uses Oracle Database Classic Cloud Service to host the Oracle Fusion Middleware component schemas required by Oracle Java Required Files (JRF). Make sure you have a subscription to Oracle Database Classic Cloud Service (Database as a Service).
- You cannot use an Oracle Database Classic Cloud Service deployment running Oracle Database 18c.
- You can use an Oracle Database Classic Cloud Service deployment running Oracle Database 12.2, but only for service instances running Oracle WebLogic Server 12.2.1 or later.
- For information about subscribing to Oracle Database Classic Cloud Service and provisioning an Oracle Database Classic Cloud Service instance (standard service level), see *Administering Oracle Database Classic Cloud Service*.
- When provisioning an Oracle Database with the Oracle Database Classic Cloud Service provisioning wizard, you *must* select an object storage container in Oracle Cloud Infrastructure Object Storage Classic even though this field is optional. If you do not select a storage container in Oracle Cloud Infrastructure Object Storage Classic, when you run the Oracle SOA Cloud Service provisioning wizard and select this Oracle Database Classic Cloud Service, instance provisioning fails. Always select an Oracle Database Classic Cloud Service that has a storage container in Oracle Cloud Infrastructure Object Storage Classic associated with it.
- Create Oracle Database Classic Cloud Service deployments with a backup option other than `NONE`. This configuration enables Oracle SOA Cloud Service to coordinate backups across your service instance and the database. Coordinated backups are not supported for other database services.
- Do *not* use the Virtual Image service level for Oracle Database Classic Cloud Service as it does not work correctly during backup and restore.
- When creating an Oracle Database Classic Cloud Service instance (standard service level) to use with Oracle SOA Cloud Service, make sure you select either **Cloud Storage Only** or **Both Cloud Storage and Local Storage** as the backup option for the database. If you select **None**, the Oracle SOA Cloud Service provisioning wizard will not present that Oracle Database Classic Cloud Service instance as an available database in the Oracle SOA Cloud Service provisioning wizard.
- If you are using Oracle Real Application Clusters (RAC) with Oracle Database Classic Cloud Service Enterprise Edition - Extreme Performance:
 - 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 Cloud Service 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
EDNLocalTxDataSo urce	GridLink	jdbc/ EDNLocalTxDataSo urce	soaRACNo_cluster
LocalSvcTblDataS ource	GridLink	jdbc/ LocalSvcTblDataS ource	soaRACNo_adminse rver
mds-owsm	GridLink	jdbc/mds/owsm	soaRACNo_cluster, soaRACNo_adminse rver
mds-soa	GridLink	jdbc/mds/ MDS_LocalTxDataS ource	soaRACNo_cluster, soaRACNo_adminse rver
opss-audit-DBDS	GridLink	jdbc/ AuditAppendDataS ource	soaRACNo_cluster, soaRACNo_adminse rver
opss-audit- viewDS	GridLink	jdbc/ AuditViewDataSou rce	soaRACNo_cluster, soaRACNo_adminse rver
opss-data-source	GridLink	jdbc/ OpssDataSource	soaRACNo_cluster, soaRACNo_adminse rver
OraSDPMDataSourc e	GridLink	jdbc/ OraSDPMDataSourc e	soaRACNo_cluster
SOADataSource	GridLink	jdbc/ SOADataSource	soaRACNo_cluster

Oracle Database Exadata Cloud Service Limitations and Usage Notes

- Oracle SOA Cloud Service supports Exadata database as a backend database to create SOAINFRA schemas. If you are not familiar with Oracle Database Exadata Cloud Service, see *Creating a Database Deployment in Using Oracle Database Exadata Cloud Service*.
- An IP reservation is required for using Oracle Database Exadata Cloud Service as your database with Oracle SOA Cloud Service. See [Create and Manage IP Reservations](#). Oracle Database Exadata Cloud Service requires the selection of an IP network during provisioning. You must then provision Oracle SOA Cloud Service in that same IP network. See [Managing IP Networks in Using Oracle Cloud Infrastructure Compute Classic](#).

- If you are provisioning the service instance in an identity domain that does not have regions enabled, a manual IP reservation procedure is required before you can create an Oracle SOA Cloud Service instance that uses an Oracle Database Exadata Cloud Service database deployment. See [Reserve IP Addresses for Oracle Database Exadata Cloud Service When Region Not Enabled](#).
- Your Oracle SOA Cloud Service instance can use an Oracle Database Exadata Cloud Service database deployment for either the Oracle Required Schema or Application Schema databases.

Backup Location

Backups are recorded to a specified object storage location in Oracle Cloud.

For a service instance in an Oracle Cloud Infrastructure Classic region, you can create this storage container manually, or Oracle SOA Cloud Service can create one automatically while you are provisioning the service instance.

See [Create an Object Storage Container](#).

Load Balancer

A load balancer routes requests it receives from clients to the WebLogic Servers configured in a service instance.

Using a load balancer within your service instance is recommended if you are configuring more than one Managed Server or more than one cluster. A load balancer also gives you the ability to suspend access to a service instance temporarily to perform routine maintenance.

Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic supports a user-managed load balancer that runs within your service instance. This load balancer is an instance of Oracle Traffic Director (OTD) and is administered through the Load Balancer Console. A service instance can include zero or one nodes running OTD. Each load balancer node is assigned a separate public IP address.

Prerequisites

Before creating an Oracle SOA Cloud Service instance, there are several prerequisites that must be completed.

Topics:

- [Prerequisites for Oracle Cloud Infrastructure](#)
- [Prerequisites for Oracle Cloud Infrastructure Classic](#)

Prerequisites for Oracle Cloud Infrastructure

Before creating an Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure, you must complete several prerequisites.

Topics:

- [Create Infrastructure Resources](#)
- [Configure Security Lists](#)

- [Generate a Secure Shell \(SSH\) Public/Private Key Pair](#)
- [Create an Oracle Database for Oracle SOA Cloud Service in Oracle Cloud Infrastructure](#)

Additional Resources

Prior to using Oracle SOA Cloud Service, ensure also you're familiar with the following:

- Oracle Cloud
Create and configure your account on Oracle Cloud. See [About Oracle SOA Cloud Service Subscriptions and Licenses](#).
- Oracle Compute VMs
Oracle SOA Cloud Service runs on Oracle Compute VMs. See [Using Oracle Compute Cloud Service](#) for information about disk images, compute shapes, storage volumes, public IP addresses, network groups, access rules, and SSH public/private key pairs.
- Oracle WebLogic Server
Applications are deployed to Oracle WebLogic Server. Oracle SOA Cloud Service supports Oracle WebLogic Server 12c.
- Oracle Traffic Director
To provide load balancing for applications, Oracle SOA Cloud Service uses Oracle Traffic Director Release 12c. Starting with Release 12c, Oracle Traffic Director administration tasks are performed from Oracle Enterprise Manager Fusion Middleware Control. When accessing Oracle Traffic Director from the Oracle SOA Cloud Service Console, you are directed to Oracle Enterprise Manager Fusion Middleware Control:


```
https://hostname/em
```


To use and configure Oracle Traffic Director, see [Administering Oracle Traffic Director](#).
- JDeveloper
Oracle SOA Cloud Service works with the corresponding release of Oracle JDeveloper (for example, 12.2.1.4.0). You can download Oracle JDeveloper from the [Oracle JDeveloper Software](#) page.

Create Infrastructure Resources

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

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

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

 **Note:**

Make a note of the region, tenancy, and storage bucket from the Oracle Cloud Infrastructure Console. Construct the backup storage URL in the following format:

```
https://swiftobjectstorage.region.oraclecloud.com/v1/namespace/
containerName
```

where:

namespace is the namespace of the storage bucket. You find this name in the Oracle Cloud Infrastructure Console under **Object Storage**. Click the name of the bucket on the Bucket Details Page.

containerName is the storage bucket name. Enter the URL above in the **Storage Container Name** field during provisioning of the Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure.

Configure Security Lists

If you plan to provision your Oracle SOA Cloud Service 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.

Open required ports as shown in the following table:

	Private Subnet (OCI only)		Public Subnet (OCI or OCI Classic)	
	with LB	without LB	with LB	without LB
Bastion instance subnet	Port 22 to public	Port 22 to public	N/A	N/A
Oracle SOA Cloud Service instance subnet	Port 22 to Bastion subnet CIDR Port 9073 to load balancer subnet's CIDR All ports to within the same subnet CIDR	Port 22 to Bastion subnet CIDR All ports to within the same subnet CIDR	Port 22 to public Port 9073 to load balancer subnet's CIDR All ports to within the same subnet CIDR	Port 22 to public Port 9074 to public All ports to within the same subnet CIDR
Load balancer subnet	Port 443 to public	N/A	Port 443 to public	N/A
DB connectivity	Port 1521 to public	N/A	Port 1521 to public	N/A
OTD Console access	Port 8989 to known CIDR	N/A	Port 8989 to known CIDR	N/A
WebLogic Admin Server Console access	Port 7002 to known CIDR	Port 7002 to known CIDR	Port 7002 to known CIDR	Port 7002 to known CIDR

The following screen shows an example security list for a public subnet:

Resources

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Status	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allow	Description
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22			TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4		ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3		ICMP traffic for: 3 Destination Unreachable
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	1521			TCP traffic for ports: 1521
<input type="checkbox"/>	No	10.0.3.0/24	All Protocols					All traffic for all ports
<input type="checkbox"/>	No	10.0.0.0/32	TCP	All	8889			TCP traffic for ports: 8889
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	443			TCP traffic for ports: 443 HTTPS
<input type="checkbox"/>	No	10.0.0.0/32	TCP	All	80			TCP traffic for ports: 80
<input type="checkbox"/>	No	10.0.0.0/32	TCP	All	7002			TCP traffic for ports: 7002

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

Generate a Secure Shell (SSH) Public/Private Key Pair

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

After generating an SSH key pair, you can use it to add a new key to an instance if needed. See [Add an SSH Public Key](#)

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 Cloud Service 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 Cloud Service instance, you are prompted to supply the public key. To connect to a VM in an Oracle SOA Cloud Service 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 Cloud Service 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 Database Classic Cloud Service database deployment.

Note:

Do not change the key that is added by Oracle SOA Cloud Service instance. If you change the key that is added by Oracle SOA Cloud Service instance, you might run into backup related issues. If you modify keys, run an on-demand full backup including DBaaS backup and ensure that it completes fine.

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 **You can download PuTTY here** link.

2. Run the PuTTYgen program.

The PuTTY Key Generator window is displayed.

3. Set the **Type of key to generate** option to **SSH-2 RSA**.
4. In the **Number of bits in a generated key** box, enter **2048**.

5. Click **Generate** to generate a public/private key pair.
As the key is being generated, move the mouse around the blank area as directed.
6. (Optional) Enter a passphrase for the private key in the **Key passphrase** box and reenter it in the **Confirm passphrase** box.

 **Note:**

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

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

 **Note:**

The `.ppk` file extension indicates that the private key is in PuTTY's proprietary format. You must use a key of this format when using PuTTY as your SSH client. It cannot be used with other SSH client tools. Refer to the PuTTY documentation to convert a private key in this format to a different format.

8. Select all of the characters in the **Public key for pasting into OpenSSH authorized_keys file** box.
Make sure you select all the characters, not just the ones you can see in the narrow window. If a scroll bar is next to the characters, you aren't seeing all the characters.
9. Right-click somewhere in the selected text and select **Copy** from the menu.
10. Open a text editor and paste the characters, just as you copied them. Start at the first character in the text editor, and do not insert any line breaks.
11. Save the text file in the same folder where you saved the private key, using the `.pub` extension to indicate that the file contains a public key.
12. If you or others are going to use an SSH client that requires the OpenSSH format for private keys (such as the `ssh` utility on Linux), export the private key:
 - a. On the **Conversions** menu, choose **Export OpenSSH key**.
 - b. Save the private key in OpenSSH format in the same folder where you saved the private key in `.ppk` format, using an extension such as `.openssh` to indicate the file's content.

Create an Oracle Database for Oracle SOA Cloud Service in Oracle Cloud Infrastructure

! Important:

For details about the databases supported by Oracle SOA Cloud Service in Oracle Cloud Infrastructure, see [Database](#).

Topics:

- [Create an Oracle Cloud Infrastructure Database for Oracle SOA Cloud Service](#)
- [Create a Policy for the Oracle Cloud Infrastructure Database](#)
- [Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Cloud Service](#)
- [Create a Policy for the Oracle Autonomous Transaction Processing Database](#)

Create an Oracle Cloud Infrastructure Database for Oracle SOA Cloud Service


You can create an Oracle Cloud Infrastructure database for use with Oracle SOA Cloud Service.

For information about the databases supported by Oracle SOA Cloud Service in Oracle Cloud Infrastructure, see [Database](#).

To create an Oracle Cloud Infrastructure database:

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
2. Open the navigation menu, click **Oracle Database**, and then click **Bare Metal, VM, and Exadata**.
3. Choose your **Compartment**, and then click **Launch DB System**.
4. In the Launch DB System dialog, enter the following:

Field	Description
Compartment	By default, the DB system launches in your current compartment and you can use the network resources in that compartment. Click the click here link in the dialog box if you want to enable compartment selection for the DB system, network, and subnet resources.
Display Name	A friendly, display name for the DB system. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB system.
Availability Domain	The availability domain in which the DB system resides.

Field	Description
Shape Type	Select the Virtual Machine option.
Shape	The shape type to use to launch the DB system. The shape type determines the type of DB system and the resources allocated to the system. Select <code>VM:Standard 2.1</code> .
Oracle Database Software Edition	The database edition supported by the DB system. You can mix supported database versions on the DB system, but not editions. (The database edition cannot be changed and applies to all the databases in this DB system.) Select <code>Standard Edition</code> .
	<div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>To provision an RAC database select <code>Enterprise Extreme Edition</code>. This will create a two node database.</p> </div>
Available Storage Size	Select the storage size in GB.
License Type	The type of license you want to use for the DB system. Your choice affects metering for billing. <ul style="list-style-type: none"> • License included means the cost of the cloud service includes a license for the Database service. • Bring Your Own License (BYOL) means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.
SSH Public Key:	The public key portion of the key pair you want to use for SSH access to the DB system. To provide multiple keys, paste each key on a new line. Make sure each key is on a single, continuous line. The length of the combined keys cannot exceed 10,000 characters.
Virtual Cloud Network	The VCN in which to launch the DB system.
Client Subnet	The subnet to which the DB system should attach.
Database Name	The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
Database Version	The version of the initial database created on the DB system when it is launched. After the DB system is active, you can create additional databases on it. You can mix database versions on the DB system, but not editions.

Field	Description
Database Admin Password	A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least 2 uppercase, 2 lowercase, 2 numeric, and 2 special characters. The special characters must be <code>_</code> , <code>#</code> , or <code>-</code> . The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.
Automatic Backup	Check the check box to enable automatic incremental backups for this database.

- Click **Launch 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).
- 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.

 **Note:**

For an RAC database, note the Host Domain Name, Port, and Scan DNS Name. You'll need this information to connect to the RAC DB system.

Create a Policy for the Oracle Cloud Infrastructure Database

For the Oracle Cloud Infrastructure database to show up in the Oracle SOA Cloud Service Console, you need to create a policy in the same compartment on which the database is provisioned by using the Oracle Cloud Infrastructure Console.

- Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
- Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
- Select the **root** compartment for your tenancy, and then click **Create Policy**.
- Enter a name and description for the policy.
- In the **Statement** field, enter the following policy statement:

```
Allow service PSM to inspect database-family in compartment
compartmentName
```

where *compartmentName* name of the compartment on which the Oracle Cloud Infrastructure database is provisioned.

Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Cloud Service

To create an Oracle Autonomous Transaction Processing (ATP) database for Oracle SOA Cloud Service:

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See *Sign In to Your Cloud Account* in *Getting Started with Oracle Cloud*.
2. Open the navigation menu and click **Oracle Database**. Under **Autonomous Database**, click **Autonomous Transaction Processing**.
3. Choose your **Compartment**, and then click **Create Autonomous Database**.

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
 - Display name:** ATPDevDB
 - Database name:** DB202
- Choose a workload type:**
 - Data Warehouse:** Configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
 - Transaction Processing:** Configures the database for a transactional workload, with a bias towards high volumes of random data access. (Selected)
- Choose a deployment type:**
 - Shared Infrastructure:** Run Autonomous Database on shared Exadata infrastructure.
 - Dedicated Infrastructure:** Run Autonomous Database on dedicated Exadata infrastructure. (Selected)
- Choose Autonomous Container Database:**
 - Compartment:** FleetCompartment
 - High Availability Container Database:** InternalACD (pEJ-PHX-AD-3)
- Configure the database:**
 - OCPU Count:** (Field)
 - Storage (TB):** (Field)

At the bottom of the form, there are two buttons: 'Create Autonomous Database' and 'Cancel'.

4. In the Create Autonomous Database wizard, provide the information for the database. See the [Oracle Cloud Infrastructure documentation](#) for field descriptions.

Note:

Choose a deployment type of **Shared Infrastructure**.

5. 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).
6. 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.

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

Create a Policy for the Oracle Autonomous Transaction Processing Database

For the Autonomous Transaction Processing (ATP) database to show up in the Oracle SOA Cloud Service console, you need to create a policy in the same compartment on which the ATP database is provisioned by using the Oracle Cloud Infrastructure console.

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
3. Select the **root** compartment for your tenancy, and then click **Create Policy**.
4. Enter a name and description for the policy.
5. In the **Statement** field, enter the following policy statement:

```
Allow service PSM to inspect autonomous-database in compartment
compartment_name
```

where *compartmentName* is the name of the compartment on which the ATP database is provisioned.

Prerequisites for Oracle Cloud Infrastructure Classic

Before creating an Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure Classic, there are several prerequisites that must be completed.

Before you begin using Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic, you must have:

- A subscription to Oracle Database.
- A subscription to Oracle Cloud Infrastructure Object Storage Classic.
- A secure shell (SSH) public/private key pair.

Oracle Database

Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic supports the following databases:

- **Oracle Database Classic Cloud Service, with or without Oracle Real Application Clusters (RAC)**

Note:

If you use RAC, you will need to create an Oracle Database Classic Cloud Service instance using the standard service level and the database edition called Enterprise Edition - Extreme Performance.

- **Oracle Database Exadata Cloud Service**

For details about the database options supported by Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic, see [Database](#).

Oracle Cloud Infrastructure Object Storage Classic

You need to have subscription to Oracle Cloud Infrastructure Object Storage Classic to store your instance backups.

Additional Resources

Prior to using Oracle SOA Cloud Service, ensure also you're familiar with the following:

- Oracle Cloud
Create and configure your account on Oracle Cloud. See [About Oracle SOA Cloud Service Subscriptions and Licenses](#).
- Oracle Compute VMs
Oracle SOA Cloud Service runs on Oracle Compute VMs. See [Using Oracle Compute Cloud Service](#) for information about disk images, compute shapes, storage volumes, public IP addresses, network groups, access rules, and SSH public/private key pairs.
- Oracle WebLogic Server
Applications are deployed to Oracle WebLogic Server. Oracle SOA Cloud Service supports Oracle WebLogic Server 12c.
- Oracle Traffic Director
To provide load balancing for applications, Oracle SOA Cloud Service uses Oracle Traffic Director Release 12c. Starting with Release 12c, Oracle Traffic Director administration tasks are performed from Oracle Enterprise Manager Fusion Middleware Control. When accessing Oracle Traffic Director from the Oracle SOA Cloud Service Console, you are directed to Oracle Enterprise Manager Fusion Middleware Control:
`https://hostname/em`
To use and configure Oracle Traffic Director, see [Administering Oracle Traffic Director](#).
- JDeveloper
Oracle SOA Cloud Service works with the corresponding release of Oracle JDeveloper (for example, 12.2.1.4.0). You can download Oracle JDeveloper from the [Oracle JDeveloper Software](#) page.

Access the Oracle SOA Cloud Service Console

You access Oracle SOA Cloud Service through a service web console or the REST API.

For information about using the REST API to access Oracle SOA Cloud Service, see [REST API for Oracle SOA Cloud Service](#).

To access Oracle SOA Cloud Service through a web console, you can do one of the following:

- Use the service URL given to you either in an email or by your administrator to access Oracle SOA Cloud Service directly, then provide your user name, password, and identity domain to sign in.
- Sign in to your Oracle Cloud Service account and navigate to the Oracle SOA Cloud Service Console, as described here.

To access the Oracle SOA Cloud Service Console:

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.

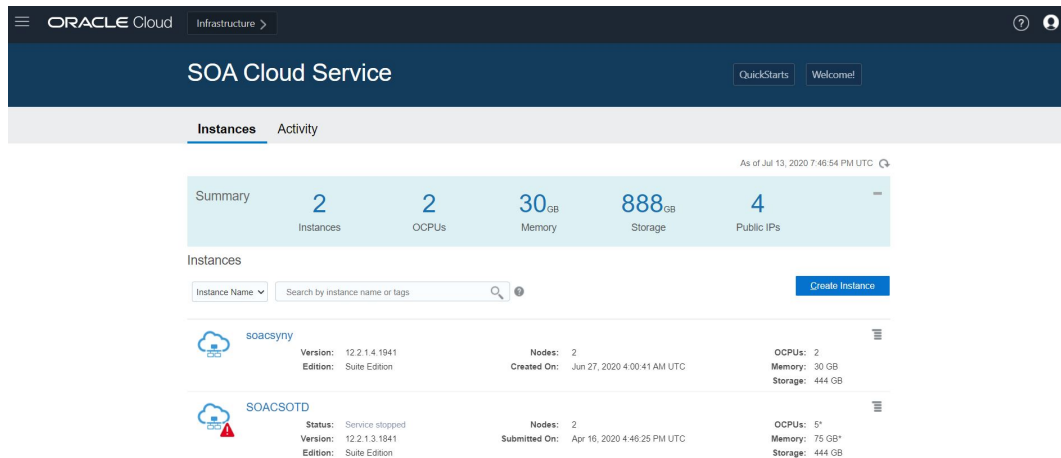
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.

2. Open the navigation menu and click **OCI Classic Services**. Under **Platform Services**, click **SOA**.

When you access Oracle SOA Cloud Service the first time for an account, you will see the [Welcome page](#), where you can explore videos and tutorials about Oracle SOA Cloud Service.

3. On the Welcome page, click **Go to Console** to open the Oracle SOA Cloud Service Console.

For details about the information and actions on this page, see [Explore the Oracle SOA Cloud Service Console](#).



4. To create a new instance, click **Create Instance**.
5. To manage a service instance, click the instance name to open the [Instance Overview page](#).

For information about accessing a VM to run WebLogic Scripting Tool (WLST) commands, see Access a Node with a Secure Shell (SSH) and Using WLST to Administer an Oracle Java Cloud Service Instance in *Administering Oracle Java Cloud Service*.

4

Provision an Oracle SOA Cloud Service Instance

You can provision an Oracle SOA Cloud Service instance on either Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic.



Note:

The information in these topics applies only to *existing* Oracle SOA Cloud Service accounts.

Topics:

- [About Provisioning an Oracle SOA Cloud Service Instance](#)
- [Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure](#)
- [Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure Classic](#)
- [Post-Provisioning Tasks in Oracle Cloud Infrastructure](#)

About Provisioning an Oracle SOA Cloud Service Instance

You can provision an Oracle SOA Cloud Service instance on either Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic.



Note:

The information in this topic applies only to *existing* Oracle SOA Cloud Service accounts.

Using a simple wizard that guides you through the provisioning process, you specify information about your instance including:

- Instance name
- SSH public key
- Cluster size
- Software release
- Service type
- WebLogic Server shape
- Backup and recovery configuration
- Database configuration

- Load balancer configuration

The Oracle SOA Cloud Service environment provides Oracle SOA Suite (12.2.1.4.0 or 12.2.1.3.0) on a single virtual machine, Oracle WebLogic Server default configurations, simplified provisioning for a single node instance, self-management tools, and secure shell (SSH) access to the virtual machine. The environment also provides simplified node cluster provisioning; simplified configuration to preexisting DBaaS and SaaS environments; and cloud self-management tools for automated backup/recovery and scaling, local and central monitoring and management, centralized provisioning, and comprehensive APIs.

Oracle handles all node provisioning, installation, and domain configuration after you make your selections.

Topics:

- [Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure](#)
- [Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure Classic](#)

Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure

You can provision an Oracle SOA Cloud Service instance in a selected compartment in Oracle Cloud Infrastructure.

 **Note:**

The information in this topic applies only to *existing* Oracle SOA Cloud Service accounts.

 **Notes:**

- Before you begin these steps, make sure that you have met the necessary [Prerequisites for Oracle Cloud Infrastructure](#).
- To access the Oracle SOA Cloud Service Console and run the Oracle SOA Cloud Service provisioning wizard, you must have the SOA Administrator role. Users with the SOA Administrator role are created on the My Account/Oracle Cloud Infrastructure Console pages by the tenant administrator. When an account is created, the tenant administrator for that account receives information about how to access these pages through an activation email.

Topics:

- [Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure](#)
- [Provision an Oracle SOA Cloud Service Instance Using the REST API](#)

- [Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet on Oracle Cloud Infrastructure](#)
- [Post-Provisioning Tasks in Oracle Cloud Infrastructure](#)

Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure

You use the Oracle Cloud Infrastructure provisioning wizard to provision a custom Oracle SOA Cloud Service instance.

Topics:

- [Start the Provisioning Wizard](#)
- [Specify Basic Service Instance Information](#)
- [Specify the Service Instance Details](#)

Start the Provisioning Wizard



This topic does not apply to Oracle Cloud Infrastructure Classic.

Start the provisioning process by creating a new service instance:

- In the [Oracle SOA Cloud Service Console](#), click **Create Instance**.

Instance Name	Version	Edition	Nodes	Created On	Submitted On	OCPUs	Memory	Storage
soacsynr	12.2.1.4.1941	Suite Edition	2	Jun 27, 2020 4:00:41 AM UTC		2	30 GB	444 GB
SOACSOTD	12.2.1.3.1841	Suite Edition	2	Apr 16, 2020 4:49:25 PM UTC		5*	75 GB*	444 GB

The **Create Instance** page is displayed.

Specify Basic Service Instance Information



This topic does not apply to Oracle Cloud Infrastructure Classic.

On the Create Instance page of the provisioning wizard, enter basic information for your service instance, including service name, service level, license type, software release, and software edition. Then click **Next**.

Create Instance

Cancel

Instance
Details
Confirm

Next >

Create SOA Cloud Service Instance
Provide basic instance information

* Service Name

Service Description

Notification Email

* Region

* Availability Domain

Subnet

Tags

* SSH Public Key Edit

License Type My organization already owns Oracle middleware software licenses. Bring my existing middleware software license to the SOA Cloud Service.

Subscribe to a new SOA Cloud Service software license and the SOA Cloud Service.

* Software Release

Service Type	Components Installed
Service Name	<p>Specify a name that you will use to identify the new service instance. The name must be unique within the identity domain and must meet the following conditions:</p> <ul style="list-style-type: none"> • Must start with a letter • Cannot be longer than 30 characters • Cannot contain non-alphanumeric characters, including spaces.
Service Description	<p>You may add an optional description that can be used to help identify this new service. The description is only used during service list display and is not used internally.</p>
Notification Email	<p>(Optional) Specify an email address where you would like to receive a notification when the service instance provisioning has succeeded or failed.</p>
Region	<p>Select the region where you want to create your instance. See Data Regions for Platform and Infrastructure Services for regions where Oracle SOA Cloud Service is available.</p> <p>The database deployment that you intend to associate with your Oracle SOA Cloud Service instance must be in the same region that you select in this field.</p>

Service Type	Components Installed
Availability Domain	<p>Select an availability domain. A region can have multiple isolated availability domains, each with separate power and cooling. The availability domains within a region are interconnected using a low-latency network.</p> <p>Note that the database deployment that you intend to associate with your Oracle SOA Cloud Service instance can be in a different availability domain within the region.</p> <p>Note: You cannot distribute an Oracle SOA Cloud Service cluster within a region among multiple availability domains in that region.</p>
Subnet	<p>Select a subnet from a virtual cloud network (VCN) that you had created previously in Oracle Cloud Infrastructure. See Prerequisites for PaaS Services on Oracle Cloud Infrastructure in the Oracle Cloud Infrastructure Documentation.</p> <p>The database deployment that you intend to associate with your Oracle SOA Cloud Service instance can be on a different subnet, but it must be in the same region and VCN.</p>
Tags	<p>(Optional) Select existing tags or add tags to associate with the service instance.</p> <p>To select existing tags, select one or more check boxes from the list of tags that are displayed on the pull-down menu.</p> <p>To create tags, click Click to create a tag to display the Create Tags dialog box. In the New Tags field, enter one or more comma-separated tags that can be a key or a key:value pair.</p> <p>If you do not assign tags during provisioning, you can create and manage tags after the service instance is created. See Create, Assign, and Unassign Tags.</p>

Service Type	Components Installed
SSH Public Key	<p>Specify the value of the VM Public Key, or the name of the file that contains the public key value.</p> <p>Define the public key for the secure shell (SSH). This key is used for authentication when connecting to the Oracle SOA Cloud Service instance using an SSH client.</p> <p>Click Edit to display the public key input for VM access and specify the public key using one of the following methods:</p> <ul style="list-style-type: none"> • Select Key File Name and click Browse to select a file that contains the public key for the secure shell (SSH). • Select Key Value and paste or type a key value in the text box. • Select Create a New Key and click Enter. The Provisioning Wizard generates a key for you. When prompted, save it as a file on your hard drive. Select Key File Name and click Browse to select the file.
License Type	<p>Choose whether you want to leverage the Bring Your Own License (BYOL) option or use your Oracle SOA Cloud Service license.</p> <ul style="list-style-type: none"> • The first option enables you to bring your on-premises Oracle WebLogic Server licenses to Oracle Cloud. Bring Your Own License (BYOL) instances are billed at a lower rate than other instances. See Frequently Asked Questions: Oracle BYOL to PaaS. <p>You must own a Universal Credits subscription or Government subscription in order to use BYOL.</p> <p>Before you scale out a BYOL instance, you must have enough WebLogic Server licenses for the additional OCPUs that will be allocated to the instance after it is scaled.</p> <ul style="list-style-type: none"> • The second option subscribes to a new Oracle SOA Cloud Service license. In this case, your account will be charged for the new service instance according to your Oracle SOA Cloud Service agreement. <p>If you have both BYOL and Oracle SOA Cloud Service entitlements, BYOL is selected by default, but you can change the license type. If you have BYOL entitlements only, BYOL is selected and you cannot change the license type. If you do not have BYOL entitlements, the Oracle SOA Cloud Service license option is selected and you cannot change the license type.</p> <p>See Overview of Oracle Cloud Subscriptions.</p>

Service Type	Components Installed
Software Release	WebLogic Server and Fusion Middleware 12.2.1.4.0 and 12.2.1.3.0 are supported. Note: You cannot upgrade Oracle SOA Cloud Service instances from earlier releases (such as 12.2.1.3.0) to the latest release (12.2.1.4.0). Instead, provision a new 12.2.1.4.0 instance.

Specify the Service Instance Details



This topic does not apply to Oracle Cloud Infrastructure Classic.

In the Instance Details page, you can configure the service type, shape, size, database, and other important details for your instance.

← Previous
Cancel

Instance
Details
Confirm

Next →

Create SOA Cloud Service Instance Details
Some settings are dependent on current region, **eu-frankfurt-1**. Go back to select a different region. ☰ Selection Summary

Select Service Type

* Service Type SOA with SB & B2B Cluster

Enable B2B adapter for EDI

Weblogic

* Compute Shape VM.Standard2.1 - 1.0 OCPU, 1

* Cluster Size 1

* User Name weblogic

* Password

* Confirm Password

Database Configuration

Database Type Oracle Autonomous Transaction Processing
 Oracle Cloud Infrastructure Database
 Oracle Database Cloud Service (Classic)

⚠ SOACS recommends minimum 2 OCPU Oracle Autonomous Transaction Processing Database. Refer to the [documentation](#) for scaling up your ATP instance.

* Compartment Name ManagedCompartmentForPaa

* Database Instance <Select an instance>
No Database instance exists for the selected compartment.

Load Balancer Configuration

* Load Balancer Oracle Traffic Director

Load Balancer Policy Least Connection Count

Compute Shape VM.Standard2.1 - 1.0 OCPU, 1

Backup and Recovery Configuration

* Storage Container Name

* Storage User Name username

* Cloud Storage Password

Topics:

- [Select Service Type](#)
- [Configure WebLogic Server Access](#)

- [Configure the Database](#)
- [Configure the Load Balancer](#)
- [Configure Backup and Recovery](#)
- [Confirm Your Selections](#)

Select Service Type



This topic does not apply to Oracle Cloud Infrastructure Classic.

Select one of the available service types for your Oracle SOA Cloud Service instance.

Item	Description
Business Activity Monitoring	Install and configure Business Activity Monitoring (Oracle BAM). See "Understanding Oracle Business Activity Monitoring" in <i>Monitoring Business Activity with Oracle BAM</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).
MFT Cluster	Install and configure only Oracle Managed File Transfer Cloud Service. See <i>Using Oracle Managed File Transfer Cloud Service</i> .
SOA with SB & B2B Cluster	Install and configure Oracle SOA Suite, Oracle Service Bus, Oracle B2B, Oracle Technology Adapters, and Oracle Cloud Adapters. When you select this service type, the Enable B2B Adapter for EDI checkbox is presented below the dropdown list. You can choose to enable the B2B Adapter for EDI. See B2B Adapter for EDI .

Configure WebLogic Server Access



This topic does not apply to Oracle Cloud Infrastructure Classic.

Specify information about your Oracle WebLogic Server compute shape and administrator details.

Item	Description
Cluster Size	Oracle SOA Cloud Service always creates a domain with one or more servers in a cluster. Choose the cluster size. Choose between 1, 2, 4 or 8 virtual machines (nodes). Note: If you configure more than one node, it is highly recommended that you enable the load balancer on the next page of the Provisioning Wizard.
User Name	The user name of the Oracle WebLogic Server administrator. Note that you can change the user name through the WebLogic Server Administration Console after you have created the instance.

Item	Description
Password	<p>Specify an Oracle WebLogic Server administrator password that meets the following criteria:</p> <ul style="list-style-type: none"> • It must begin with a letter. • It must contain between 8 and 30 characters. • It must contain at least one number. • Optionally, it can contain any number of the following special characters: \$ # _. <p>For example: Ach1z0#d.</p>

Configure the Database



This topic does not apply to Oracle Cloud Infrastructure Classic.

Specify information about your database.

For details about the databases supported by Oracle SOA Cloud Service in Oracle Cloud Infrastructure, see [Database](#).

Item	Description
Database Type	<ul style="list-style-type: none"> • Oracle Autonomous Transaction Processing: Select to provision an Oracle Autonomous Transaction Processing (ATP) database to use with the SOA with SB & B2B Cluster service type. See Create an Oracle Autonomous Transaction Processing Database for Oracle SOA Cloud Service. • Oracle Cloud Infrastructure Database: Select to provision an Oracle Cloud Infrastructure native database with your Oracle SOA Cloud Service instance. See Create an Oracle Cloud Infrastructure Database for Oracle SOA Cloud Service. Note that only native databases belonging to the same region, availability domain, and subnet selected during provisioning of the Oracle SOA Cloud Service instance are available for selection. Therefore, make sure that you choose the same region, availability domain, and subnet in which the native database was provisioned.
Compartment Name	Select the same compartment on which the native database is provisioned from the drop-down list.

Item	Description
Database Instance or Name	<p>Select an existing Oracle Cloud Infrastructure database or Oracle Autonomous Transaction Processing database instance name.</p> <p>Note: Oracle SOA Cloud Service supports only <i>serverless deployments</i> of the Oracle Autonomous Transaction Processing database. It does not support <i>dedicated deployments</i>.</p> <p>If you selected the Oracle Cloud Infrastructure database, select a native database from the drop-down list. Note that only native databases belonging to the same region, availability domain, and subnet selected during provisioning of the Oracle SOA Cloud Service instance are available for selection.</p>
PDB Name	<p>Enter an optional pluggable database (PDB) name.</p> <p>Note: Oracle SOA Cloud Service supports the use of only a single pluggable database.</p>
Administrator User Name	<p>Your database user name. This value must be set to a database user with SYSDBA system privileges. You can use the default user SYS or any user that has been granted the SYSDBA privilege.</p>
Password	<p>The database administrator password specified when the database instance was created.</p>

Configure the Load Balancer



This topic does not apply to Oracle Cloud Infrastructure Classic.

Specify whether or not you want to use the Oracle Traffic Director (OTD) load balancer.

Notes:

- If you do not select a load balancer, then the Managed Server URLs (b2bconsole, worklistapp) are not accessible using the load balancer IP address.
- To provision the Oracle-managed load balancer, do not provision OTD. Instead, manually set up and configure the Oracle Cloud Infrastructure load balancer as a post-provisioning task (see [Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning](#)).

Item	Description
Load Balancer	<ul style="list-style-type: none"> • None: Select if you do not need a load balancer or want to add an Oracle Cloud Infrastructure load balancer post-provisioning (see Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning). • Oracle Traffic Director: Select if you want to manage the load balancer.
Load Balancer Policy (if Oracle Traffic Director is selected)	<p>Select the load balancer mechanism for routing traffic to servers.</p> <ul style="list-style-type: none"> • Least Connection Count. Passes each new request to the managed server with the least number of connections. This policy is useful for smoothing distribution when managed servers slow down. managed servers with greater processing power receive more connections over time. • Least Response Time. Passes each new request to the managed server with the fastest response time. This policy is useful when managed servers are distributed across networks. • Round Robin. Passes each new request to the next managed server in line, evenly distributing requests across all managed servers regardless of the number of connections or response time.

Item	Description
Compute Shape (if Oracle Traffic Director is selected)	<p>Select the number of Oracle Compute Units (OCPU) and amount of RAM memory that you want to allocate to the VM for the load balancer. The larger the compute shape, the greater the processing power.</p> <p>The valid compute shapes for Oracle Cloud Infrastructure are:</p> <ul style="list-style-type: none"> • VM.Standard2.1 – 1.0 OCPU, 15.0GB RAM • VM.Standard1.2 – 2.0 OCPU, 14.0GB RAM • VM.Standard2.2 – 2.0 OCPU, 30.0GB RAM • VM.Standard1.4 – 4.0 OCPU, 28.0GB RAM • VM.Standard2.4 – 4.0 OCPU, 60.0GB RAM • VM.Standard1.8 – 8.0 OCPU, 56.0GB RAM • VM.Standard2.8 – 8.0 OCPU, 120.0GB RAM • VM.Standard1.16 – 16.0 OCPU, 112.0GB RAM • VM.Standard2.16 – 16.0 OCPU, 240.0GB RAM • VM.Standard2.24 – 24.0 OCPU, 320.0GB RAM

**Note:**

If you select a VM. Standard1.X shape, verify that your account has entitlement for it before proceeding with the provisioning.

Note that you cannot change the compute shape after you have created the Oracle SOA Cloud Service instance.

Configure Backup and Recovery



This topic does not apply to Oracle Cloud Infrastructure Classic.

Specify information about the storage container that will be used to store backups. It's a good idea to create a separate container for each instance you create.



Note:

You must have a current subscription to Oracle Cloud Infrastructure Object Storage.

Item	Description
Storage Container Name	Enter the URL of an existing bucket in Oracle Cloud Infrastructure Object Storage. See Prerequisites for Oracle Platform Services in the Oracle Cloud Infrastructure documentation. Format: <code>https://swiftobjectstorage.region.oraclecloud.com/v1/account/bucket</code> Example: <code>https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/myCompany/myBucket</code>
Storage User Name	The name of the Oracle Cloud Infrastructure administrator. Note: The Oracle Identity Cloud Service (IDCS) Federated user name is not supported.
Cloud Storage Password	Enter the auth token generated in Oracle Cloud Infrastructure for the specified user.

Confirm Your Selections



This topic does not apply to Oracle Cloud Infrastructure Classic.

The confirmation page displays the configuration values you choose in the provisioning wizard.

Review the service details. If you need to change the service details, use the navigation bar or **Previous** button at the top of the wizard to step back through the pages in the wizard. Click **Cancel** to cancel out of the wizard without creating a new service instance. If you are satisfied with your choices on the Confirmation page, click **Create**. Click the download icon provided in the top-right of the page to download the REST API used to provision the pod.



Note:

It takes about an hour and a half to create the instance. You are notified by email when it has been created.

Provision an Oracle SOA Cloud Service Instance Using the REST API

To provision an Oracle SOA Cloud Service instance on Oracle Cloud Infrastructure using the REST API instead of the provisioning wizard, see "Provision a New Instance" in *REST API for Oracle SOA Cloud Service*.

To provision an Oracle SOA Cloud Service instance on Oracle Cloud Infrastructure using the provisioning wizard, see [Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure](#).

Notes:

- Associations do not show up in the Oracle SOA Cloud Service Console. The REST API Response also does not show the associations.
- Coordinated backups are not supported with the Oracle Cloud Infrastructure database or Autonomous Transaction Processing (ATP) database.
- Do not delete a database after creating it. There is no check while deleting an Oracle Cloud Infrastructure database or Autonomous Transaction Processing (ATP) database that is associated with an Oracle SOA Cloud Service instance.
- Make sure that the database is up and running when using it to provision an Oracle SOA Cloud Service instance.
- In REST API, when using a connect string, you must connect to an Oracle Cloud Infrastructure database created under the same region and availability domain. If not, there are performance issues. The connect string is not validated while provisioning the Oracle SOA Cloud Service instance. Provisioning fails if the connect string provided is incorrect.
- Make sure that the database port is open to the SOA subnet before using REST API to provision a new Oracle SOA Cloud Service instance. For an Oracle Cloud Infrastructure database, the port is 1521; for Autonomous Transaction Processing (ATP) database, the port is 1522.
- When updating database password credentials, make sure that the database password adheres to the following standards:
 - Password must contain at least 2 uppercase characters
 - Password length should be greater than 9 characters
 - Password must contain at least 2 special characters

Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet on Oracle Cloud Infrastructure



This topic does not apply to Oracle Cloud Infrastructure Classic.

When you create an Oracle SOA Cloud Service instance in an Oracle Cloud Infrastructure region, you can attach the instance to either a private subnet or a public subnet. If you attach the instance to a private subnet, then the nodes of the instance can't have public IP addresses. They are isolated from the public Internet.

Topics:

- [Create the Required Resources in Oracle Cloud Infrastructure](#)
- [Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet](#)

Create the Required Resources in Oracle Cloud Infrastructure




This topic does not apply to Oracle Cloud Infrastructure Classic.

Before creating an Oracle SOA Cloud Service instance attached to a private subnet, you must fulfill certain prerequisites, including creating the required identity, networking, and storage resources in Oracle Cloud Infrastructure.

1. Generate an SSH key pair.

See [Generate a Secure Shell \(SSH\) Public/Private Key Pair](#).

Note the path and name of the files that contain the private and public keys. You'll need the keys later.

2. Complete the following steps from the tutorial  [Creating the Infrastructure Resources Required for Oracle Platform Services](#):

- a. Create a compartment.

If you want to create the Oracle Cloud Infrastructure resources in an existing compartment, then skip this step.

- b. Create a virtual cloud network (VCN) in the compartment you created or identified.

If you want to use an existing VCN, then skip this step.

- c. Create a policy to allow Oracle Cloud platform services to use the networking resources in the compartment that you created or identified.

If the required policy exists for the compartment that you want to use, then skip this step.

- d. Create a bucket in the Object Storage service to store backup of your Oracle SOA Cloud Service instance.

 **Note:**

The user creating the bucket must be a user in Oracle Cloud Infrastructure Identity and Access Management (IAM), not a federated user.

If you'd like to use a bucket that were created previously, then skip this step.

Note the name of the bucket. You'll need them later while creating the service instance.

- e. Generate authentication tokens for the users who created the bucket.

If you have the required token already, then skip this step.

Note the authentication token value. You'll need it later while creating the service instance.

3. In the VCN that you created or identified earlier, create the required networking resources:

- a. Create a service gateway.

The service gateway is required for the Oracle SOA Cloud Service instance to access the Object Storage service.

See [Setting Up a Service Gateway in the Oracle Cloud Infrastructure documentation](#).

- b. Create an internet gateway.

The internet gateway enables communication between the public Internet and the Bastion node.

See [Working with Internet Gateways in the Oracle Cloud Infrastructure documentation](#).

- c. (Optional) Create a NAT gateway.

The NAT gateway is required for the node of the Oracle SOA Cloud Service instance to access the public Internet. Such access would be useful when (for example) you want to allow the nodes to access the Oracle Yum server to download additional packages or OS patches.

See [Setting Up a NAT Gateway in the Oracle Cloud Infrastructure documentation](#).

- d. Create the following route table:

See [Working with Route Tables in the Oracle Cloud Infrastructure documentation](#).

Route Table `route.private` for the Private Subnet

Route Rule	Destination	Target
To route traffic bound for the Object Storage service through the service gateway	Service: OCI <i>region</i> Object Storage	Service gateway
(Optional) To route traffic bound for the public Internet through the NAT gateway	CIDR: 0.0.0.0/0	NAT gateway

- e. Create the following security lists:

See [Working with Security Lists in the Oracle Cloud Infrastructure documentation](#).

Security List `seclist.bastion` for the Bastion Subnet

Security Rule	Source / Destination	IP Protocol / Port
(Ingress) To allow SSH connections to the Bastion node	Source CIDR: 0.0.0.0/0	SSH / 22
(Egress) To allow all outbound traffic	Destination CIDR: 0.0.0.0/0	All protocols / ports

Security List `seclist.private` for the Private Subnet

Security Rule	Source / Destination	IP Protocol / Port
(Ingress) To allow traffic from the other compute nodes in the VCN	Source CIDR: 10.0.0.0/16	All Protocols
(Egress) To allow all outbound traffic	Destination CIDR: 0.0.0.0/0	All Protocols

- f. Create the following subnets:

See Working with VCNs and Subnets in the Oracle Cloud Infrastructure documentation.

Subnet Purpose (Suggested Name)	Availability Domain	Attributes
For the Bastion host (subnet.bastion)	AD1	Example CIDR ¹ : 10.0.1.0/24 Route table: <code>route.public</code> Subnet access: Public Security list: <code>seclist.bastion</code>
For the service instances (subnet.private)	AD1	Example CIDR: 10.0.4.0/24 Route table: <code>route.private</code> Subnet access: Private Security list: <code>seclist.private</code>

¹ Assuming the VCN's CIDR is 10.0.0.0/16

 **Note:**

Make a note of the OCIDs of the subnets. You'll need them later while creating the Bastion host and the service instance.

4. Create a compute instance and attach it to the public subnet that you created for the Bastion host.

Through this node, administrators can access the administration console of the Oracle SOA Cloud Service instance, and they connect using `ssh` to the compute nodes of the service instance.

See Creating an Instance in the Oracle Cloud Infrastructure documentation.

After creating the Bastion compute instance, note its public IP address.

You've created the required resources in Oracle Cloud Infrastructure. You can now create the Oracle SOA Cloud Service instance.

Create an Oracle SOA Cloud Service Instance Attached to a Private Subnet



This topic does not apply to Oracle Cloud Infrastructure Classic.

Use the REST API to create an Oracle SOA Cloud Service instance attached to a private subnet.

 **Note:**

You cannot create an Oracle SOA Cloud Service instance on a private subnet using the Oracle SOA Cloud Service Console.

Prerequisite: Before creating an Oracle SOA Cloud Service instance, create an Oracle Cloud Infrastructure native database in the same private subnet. See [Create an Oracle Cloud Infrastructure Database for Oracle SOA Cloud Service](#).

To create an Oracle SOA Cloud Service instance attached to a private subnet:

1. Create a request body in JSON format by using the following template, and save it in a plain-text file (for example, `create-soacs-instance-on-oci.json`):

 **Notes:**

- This template includes only the minimum set of parameters required to create an instance of Oracle SOA Cloud Service running Oracle WebLogic Server Enterprise Edition.
- This template creates an Oracle SOA Cloud Service instance with Oracle Traffic Director (OTD). If you do not want OTD to be provisioned along with the Oracle SOA Cloud Service instance, then set:

```
"provisionOTD":"false",
```

and remove the following under "components":

```
"OTD":{
  "loadBalancingPolicy":"LEAST_CONNECTION_COUNT",
  "shape":"VM.Standard2.1"
},
```

```
{
  "region":"us-phoenix-1",
  "edition":"SUITE",
  "purchasePack":"soaosbb2b or mft",
  "vmPublicKeyText":"ssh-rsa vm_public_key_text_value",
  "availabilityDomain":"bcaH:PHX-AD-1",
  "provisionOTD":"true",
  "enableNotification":"false",
  "cloudStorageContainer":"https://swiftobjectstorage.us-ashburn-1.oraclecloud.com/v1/ocitenancey/soabackup",
  "cloudStorageUser":"user@example.com",
  "cloudStoragePassword":"authtoken",
```

```

    "serviceVersion": "12cRelease213 or 12cRelease214",
    "serviceLevel": "PAAS",
    "serviceName": "soacsInstanceName",

"subnet": "ocid1.subnet.oc1.phx.aaaaaaacukvw55crhp2ekd2f36vltcpsccx43igo3d
lezejc3dqwft7dgga",
    "isBYOL": "false",
    "components": {
      "OTD": {
        "loadBalancingPolicy": "LEAST_CONNECTION_COUNT",
        "shape": "VM.Standard2.1"
      },
      "WLS": {
        "adminUserName": "weblogic",
        "adminPassword": "webLogicPassword", (min 8 chars, at least 1
uppercase, 1 number, and special char _ or #)
        "dbName": "sys",
        "dbaPassword": "sysPassword", (min 8 chars, at least 1
uppercase, 1 number, and special char _ or #)
        "managedServerCount": "1",
        "connectString": "dbhost:1521/PDB.subnet.vcn.oraclevcn.com",
        (use the correct PDB name)
        "shape": "VM.Standard2.1"
      }
    },
    "enableAdminConsole": "true",
    "meteringFrequency": "HOURLY"
}

```

where `vm_public_key_text_value` is the SSH key pair value.

For information about the REST API payload, see *REST API for Oracle SOA Cloud Service*.

2. Send the REST API request.

To determine the REST endpoint URL, see "REST API Endpoints for Platform Services" in [Getting Started with Oracle Platform Services](#) in the Oracle Cloud Infrastructure documentation.

The following is an example of a REST API request to create an Oracle SOA Cloud Service instance:

```

curl -X POST https://psm.us.oraclecloud.com/paas/api/v1.1/instancemgmt/
identityServiceID/services/soa/instances \
-u user:password \
-H 'X-ID-TENANT-NAME: identityServiceID' \
-H 'Content-Type: application/
vnd.com.oracle.oracloud.provisioning.Service+json' \
-d @create-soacs-instance-on-oci.json

```

where:

- `identityServiceID`: The identity service ID of your Oracle Cloud account.

You can find this information on the service details page for any service in the Oracle Cloud Infrastructure Console.

- *user*: Your Oracle Cloud user name.
- *password*: Your Oracle Cloud password.

A message similar to the following is displayed, indicating that the request was accepted:

```
{
  "details": {
    "message": "Submitted job to create service [mySOACS] in domain
[identityServiceID].",
    "jobId": "50572730"
  }
}
```

3. Wait for the instance to be created.

Notes:

- If you followed all prerequisites and the instance creation fails, make sure that you don't have firewall settings blocking your request.
- If you want to scale out or scale in the instance, you must use the corresponding [REST API](#). These operations will not succeed using the Oracle SOA Cloud Service Console.
- The compute nodes of Oracle SOA Cloud Service instances that are attached to private subnets in Oracle Cloud Infrastructure have private IP addresses, so you can't `ssh` to the nodes or access the administration consoles of such instances from the public Internet.
- You can access the administration consoles and connect to the nodes of such instances through a Bastion host attached to a public subnet or through your on-premises network by using IPsec VPN connectivity. See [Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure](#).
 1. Connect to the Oracle SOA Cloud Service instance through SSH using the Bastion node. Note that the Bastion VM is in same VCN but in a different public subnet.

```
ssh -i opc_key opc@publicBastionIP
```

2. Inside the Bastion node, run the following command to copy the private key to the Bastion node, and connect to the Oracle SOA Cloud Service instance through SSH:

```
ssh -i /tmp/opc_key opc@privateIP
```

where *privateIP* is the WebLogic Server private IP address or the OTD private IP address.

Post-Provisioning Tasks in Oracle Cloud Infrastructure

Review the following topics to learn about additional post-provisioning tasks you must complete for the service to work correctly in Oracle Cloud Infrastructure.

Topics:

- [Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure](#)
- [Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure](#)
- [Register a Custom Domain Name with a Third-Party Registration Vendor](#)
- [Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory](#)

Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure



This topic does not apply to Oracle Cloud Infrastructure Classic.

If you provision an Oracle SOA Cloud Service instance after 1 August 2020 and you are not able to access the WebLogic Server Administration or OTD 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 or OTD Console URLs:

1. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
2. Select the compartment where you created the new instance.
3. In the list of VCNs, select your VCN.
4. On the Virtual Cloud Network Details page, click **Security Lists** in the left pane.
5. Click the security list that the Administration Server VM is using.
6. 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 Examples: 80, 20-22


DESCRIPTION OPTIONAL

Maximum 255 characters

+ Additional Ingress Rule

Add Ingress Rules Cancel

7. 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 your 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 SOURCE PORT RANGE field, enter All.
 - f. In the DESTINATION PORT RANGE field, enter 7002.
 - g. Click **Add Ingress Rules**.



AVAILABLE

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 Remove

Security List Information Tags

OCID: ocmlp1 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	162.142.142.150/32	TCP	All	7002		TCP traffic for ports: 7002	

0 Selected

8. Repeat the steps above to add another ingress rule to access the OTD Console, specifying a `DESTINATION PORT RANGE` of 8989.

Extend Your On-Premises Network with a VCN on Oracle Cloud Infrastructure



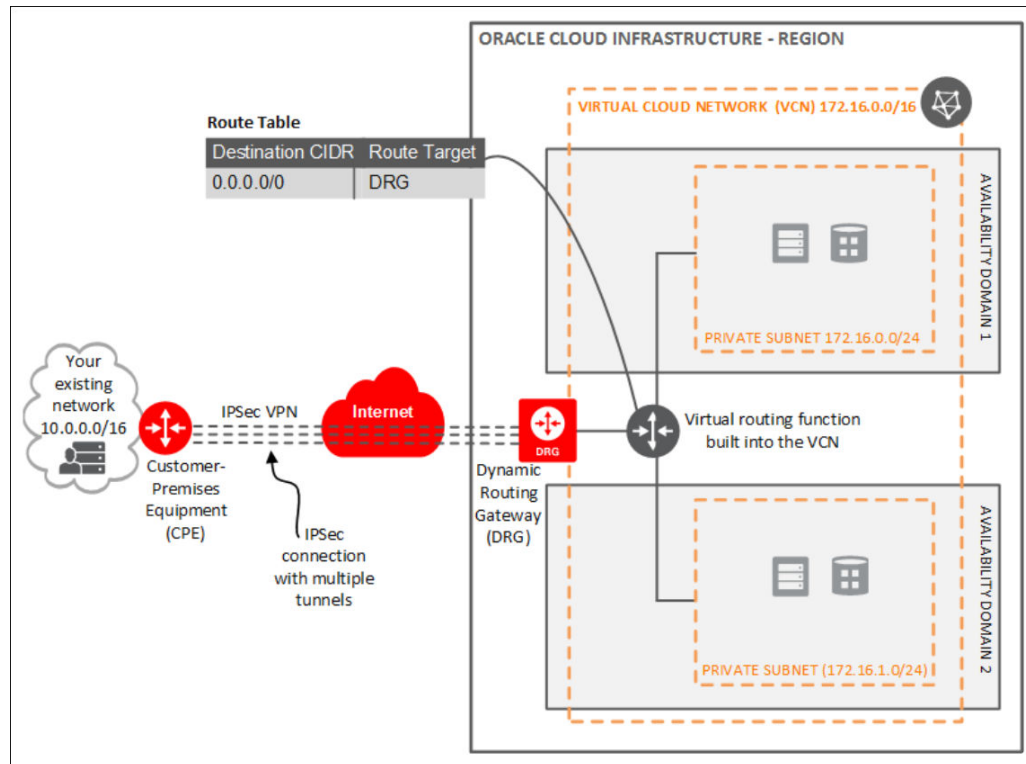
This topic does not apply to Oracle Cloud Infrastructure Classic.

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. This topic provides instructions for setting up and managing an IPSec VPN for your VCN for PaaS services. This topic applies to all PaaS services.

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.
11. Create PaaS Policies.



1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
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
Name	Name of the subnet

Field	Description
Availability Domain	Select an availability domain for your subnet.
CIDR Block	Specify a CIDR block to indicate the network address that can be allocated to the resources.
Route Table	Select a route table to provide mapping for the traffic from the subnet to destinations outside the VCN.
SUBNET ACCESS	PRIVATE SUBNET: Select this option to prohibit public IP addresses for instances in the subnet. PUBLIC SUBNET: Select this option to allow public IP addresses for instances in the subnet.
DNS HOSTNAMES IN THIS SUBNET	Select this option to allow assignment of DNS hostname when launching an instance.
DNS LABEL	Auto-generated if no name is specified.
DNS DOMAIN NAME	Read-only field
DHCP OPTIONS	Select the DHCP option for the VCN.
Security Lists	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 Dynamic Routing Gateway 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**.
 - b. Click **Create Customer-Premises Equipment**.
 - c. Select the compartment, enter a name and IP address for the customer-premises equipment, and click **Create**.

7. Next, create an IPSec connection to the customer-premises equipment.
 - a. Open the navigation menu and click **Networking**. Under **Customer Connectivity**, click **Dynamic Routing Gateway**.
 - b. Click the dynamic routing gateway that you created.
 - c. In the Dynamic Routing Gateway details page, in the navigation pane, under **Resources**, click **IPSec Connections**.
 - d. Enter a name and public (external) IP address of the VPN device to be used to establish IPSec VPN and click **Create**.

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

8. Get the IPSec tunnel information. Select the IPSec Connection and click **Tunnel Information**. The tunnel information contains the IP addresses of the tunnel endpoints and the shared secret to be used to initiate the IPSec connection. It also shows the status of the IPSec connection.
9. Configure the IPSec connection on the remote end. Your network administrator can configure your on-premises VPN device(s) to initiate an IPSec connection to the tunnels created on Oracle Cloud Infrastructure.

 **Note:**

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

10. Configure routing for subnets to go through Dynamic Routing Gateway for on-premises traffic. The default routing table created for a VCN has no rules by default. All instances in VCN have a route to other instances in the VCN only.
 - a. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
 - b. Click the VCN to open its details.
 - c. In the Virtual Cloud Network details page, in the navigation pane, under **Resources**, select **Route Tables** and then click **Edit Route Rules**.
 - d. Modify the default route table to add a default route and set the Dynamic Routing Gateway as the route target. This routes any non-VCN traffic through the Dynamic Routing Gateway into the on-premises network.
11. Configure security rules to allow valid traffic in/out of your subnets.
 - a. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
 - b. In the Virtual Cloud Network details page, in the navigation pane, under **Resources**, select **Security Lists**.
 - c. Select the security list for your VCN and click **Security List Details**.
 - d. The default security list has only three ingress rules and one egress rule to allow all outgoing traffic. Click **Edit All Rules** to modify the rules to allow SSH as required and to open up specific ports for the application running on your compute instances within the subnets.

12. Create a policy the first time you create an Oracle PaaS instance on Oracle Cloud Infrastructure. For subsequent PaaS instances, you can use the same or a new policy.
 - a. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Policies**.
 - b. Click **Create Policy**.
 - c. On the Create Policy page, select the **root** compartment for your tenancy, and then click **Create Policy**.
 - d. In the **Create Policy** dialog box, enter a name and a description for the policy.
 - e. In the **Policy Versioning** field, specify the definitions of the verbs and resources that the policy must use.
 - To specify that the policy must reflect future changes to the definitions of the policy verbs and resources, select **KEEP POLICY CURRENT**.
 - To specify that the policy must use the definitions in effect on a specific date, select **USE VERSION DATE**, and then enter the date in the YYYY-MM-DD format.
 - f. In the **Policy Statements** field, enter the following policy statement.

 **Note:**

Replace `<compartment_name>` with the name of your compartment. Don't change anything else in the policy statement.

```
Allow service PSM to inspect vcns in compartment <compartment_name>
```

- g. Click **plus** to add the next policy.
- h. Add the following policy.

```
Allow service PSM to manage security-lists in compartment
<compartment_name>
```

- i. After you add all the policies, click **Create**.

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 SOA Cloud Service 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 SOA Cloud Service 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 Cloud Service 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.
- See [Import a CA-Issued SSL Certificate to the Load Balancer](#) and [Associate the SSL Certificate With the Load Balancer](#).

Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory

Oracle SOA Cloud Service uses image-based patching, which means that the Oracle Fusion Middleware home installation directory is replaced with a new image when a patch upgrade occurs. Any post-installation configuration changes you make to the `plan.xml` file in the installation subdirectory (`$MW_HOME/soa/soa/plan.xml`) are overridden when upgrade patching occurs:

If you need to customize the `plan.xml` file after installation, ensure that you place this file outside the installation directory. Otherwise, patching overrides your changes.

Provision an Oracle SOA Cloud Service Instance in Oracle Cloud Infrastructure Classic

You can provision an Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure Classic.

 **Note:**

The information in this topic applies only to *existing* Oracle SOA Cloud Service accounts.

 **Notes:**

- Before you begin these steps, make sure that you have met the necessary [Prerequisites for Oracle Cloud Infrastructure Classic](#).
- To access the Oracle SOA Cloud Service Console and run the Oracle SOA Cloud Service provisioning wizard, you must have the SOA Administrator role. Users with the SOA Administrator role are created on the My Account/Oracle Cloud Infrastructure Console pages by the tenant administrator. When an account is created, the tenant administrator for that account receives information about how to access these pages through an activation email.

Topics:

- [Reserve IP Addresses for Oracle Database Exadata Cloud Service When Region Not Enabled](#)
- [Create and Manage IP Reservations](#)
- [Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic](#)
- [Provision Oracle SOA Cloud Service on an IP Network](#)
- [Provision an Oracle SOA Cloud Service Instance with Stack Manager](#)
- [Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure Classic](#)
- [Post-Provisioning Tasks in Oracle Cloud Infrastructure Classic](#)

Reserve IP Addresses for Oracle Database Exadata Cloud Service When Region Not Enabled



This topic applies only to Oracle Cloud Infrastructure Classic.

If regions are enabled for your account and you select a region name in the service instance creation wizard, you can use reserved IP addresses for your VMs without using this procedure. If regions are not enabled, you must follow this procedure to reserve IP addresses:

1. Create an Oracle Database Exadata Cloud Service database deployment if you have not done so already.
2. Determine the initial size for the Oracle WebLogic Server cluster you will define when you create your Oracle SOA Cloud Service instance.
3. Log in to support.oracle.com (My Oracle Support).
4. File a Service Request to obtain authorized IP addresses for your Oracle SOA Cloud Service instance.

Oracle will provide IP addresses and open up the firewall at these addresses on the Oracle Database Exadata Cloud Service.

In the Service Request, specify the following information:

- Your identity domain.

- Oracle Required Schema database name, which must be the name of the Oracle Database Exadata Cloud Service database deployment if you are not specifying a database deployment for the Application Schema.
- (Optional) Application Schema database deployment name.
- Desired number of servers in your WebLogic Server cluster.

Create and Manage IP Reservations



This topic applies only to Oracle Cloud Infrastructure Classic.

IP reservations created using Compute Classic Console are not available for use while provisioning Oracle SOA Cloud Service. Instead, you can pre-allocate IP addresses to be used for Oracle SOA Cloud Service using the IP reservations feature. Note that these reservations are only available for Oracle SOA Cloud Service.

IP reservations are useful when you want to maintain an IP address across the creation and deletion of instances. This may occur because you have web services or endpoints configured to use a specific IP address. When you delete and provision a new instance (for example, move your instance from a test to a production environment), you can continue to use the same IP address.

While reserving IP addresses using this feature, if you select IP reservations from a pool of public IP addresses, then your instance can communicate with external hosts over the public internet. On the other hand, if you select IP reservations from a pool of cloud IP addresses, then your instance can communicate with other Oracle Cloud services, such as the REST endpoint of an Oracle Cloud Infrastructure Object Storage Classic account in the same region, without sending traffic over the public internet.

When provisioning multi-node instances in Oracle SOA Cloud Service, you need to have same number of IP reservations available for use. In order to release IP reservations, delete or scale in a Oracle SOA Cloud Service instance. Note that IP reservations can be used with or without IP networks.

Important:

You cannot attach an IP reservation to an already created Oracle SOA Cloud Service instance. If you choose to detach an IP reservation, you cannot restore from an existing backup.

Note:

A scale out operation either auto-assigns IP reservations or uses reserved IP addresses.

The tasks for creating and managing IP reservations are:

- [Create an IP Reservation](#)
- [Delete an IP Reservation](#)

Create an IP Reservation



This topic applies only to Oracle Cloud Infrastructure Classic.

You can preallocate IP addresses to be used for Oracle SOA Cloud Service using the IP reservations feature.

To create an IP reservation:

1. In the [Oracle SOA Cloud Service Console](#), click **IP Reservations**.

 **Note:**

The IP Reservations tab shows up only if at least one IP reservation has been created.

2. Click **Create**.
The Create IP Reservation window displays.
3. Enter a name for the IP reservation and choose the region where the reservation will be available from.
4. If you intend to use this reservation for an instance that you attach to an IP network, select the **On IP Network** check box. If you leave this check box deselected, the IP reservation can be assigned to only an instance that you attach to the shared network.
5. Click **OK**.

 **Note:**

The IP reservation creation process takes a couple of minutes. The created IP reservation shows in the IP Reservation page list with "UNUSED" status. Once the IP reservation is created successfully, you can go back to **Create a Service** page and use the newly created IP reservation in your service.

Creating the First IP Reservation

To create the first IP Reservation, use the Create Service wizard.

1. In the [Oracle SOA Cloud Service Console](#), click **Create Service**.
2. Enter the text "temp" in the Service Name field, select a region in the Region list, and click **Next**.
3. In the Weblogic section, click the gear icon beside the IP Reservations field.
The Confirmation window displays.
4. Click **OK** to continue.
The Create Service wizard closes and the IP Reservations page displays.
5. Click **Create**.

The Create IP Reservation window displays.

6. Enter a name for the IP reservation and choose the region where the reservation will be available from.
7. If you intend to use this reservation for an instance that you attach to an IP network, select the **On IP Network** check box. If you leave this check box deselected, the IP reservation can be assigned to only an instance that you attach to the shared network.
8. Click **OK**.

Delete an IP Reservation



This topic applies only to Oracle Cloud Infrastructure Classic.

When you no longer require an unused IP reservation, you can delete it.



Note:

You can only delete an unused IP reservation.

To delete an IP reservation:

1. In the [Oracle SOA Cloud Service Console](#), click **IP Reservations**.
2. Locate the unused IP reservation you want to delete and then click the **X** icon in the row for that reservation.
You are prompted to confirm the deletion.
3. Click **OK** to confirm deletion of the IP reservation.

Quickly Try Out an Instance in Oracle Cloud Infrastructure Classic



This topic applies only to Oracle Cloud Infrastructure Classic.

You can create a quick start instance of Oracle SOA Cloud Service with a single click.

Capabilities of a Quick Start Instance

The QuickStarts option automatically provisions Oracle SOA Cloud Service with an Oracle Database Classic Cloud Service instance, but does *not* provision or provide support for an Oracle Cloud Infrastructure Object Storage Classic container instance. Without a container, database backups are not possible. The quick start instance is useful for testing integrations. After testing is complete, you can import integrations into a different Oracle SOA Cloud Service instance.

 **Note:**

Note the following details:

- This instance does *not* include or support the use of an Oracle Cloud Infrastructure Object Storage Classic container.
- No load balancer
- A **Backup** tab on the overview page for the provisioned Oracle SOA Cloud Service instance is not available.

Prerequisites

None.

Creating an Instance

To create a quick start instance:

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
2. Open the navigation menu and click **OCI Classic Services**. Under **Platform Services**, click **SOA**.
3. In the header, click **QuickStarts**.

The QuickStarts page is displayed showing the details of the instance that will be created.

Create Instance
Cancel Custom

QuickStarts

QuickStart instances use Oracle's [Bring Your Own License \(BYOL\)](#) terms. [Click here](#) if you do not want to use an existing license.

* Instance Name

SOA Cloud Service 12.2.1.3 - Single Node

Creates a stack composed of SOA Cloud Service and Database Cloud Service instances. This is a user-managed service, including scaling, starting and stopping.

Create

Includes:

- Service Type: SOA, Service Bus, B2B
- SOA Shape: 1 OCPU
- Oracle Database 12.1, Standard Edition
- DB Shape: 1 OCPU
- Total Block Storage: 395 GB
- No Load Balancer

4. Review the quick start instance details.

Notes:

- Quick start instances use Bring Your Own License (BYOL) terms. Click the link **Click here** if you do not want to use BYOL. For more information, see [About Oracle SOA Cloud Service Subscriptions and Licenses](#).
- Click **Custom** in the upper right corner of the page to launch the provisioning wizard instead of creating a quick start instance.

5. In the **Instance Name** field, enter a name.
6. Click **Create** below the template you want to provision.
7. Download the SSH key when prompted, then click **Create**.
8. When Oracle SOA Cloud Service and Oracle Database Classic Cloud Service instance creation completes, change the password for the `sys` username.

See *Altering User Accounts* in the *Oracle Database Security Guide*.

 **Note:**

If you created a service instance using a QuickStart template, you cannot delete the service instance from the Oracle SOA Cloud Service Console. Using a QuickStart template creates an entire stack for you, so you must delete the entire stack from the Stack console. See [Deleting an Oracle Cloud Stack](#) in *Using Oracle Cloud Stack Manager*.

Provision Oracle SOA Cloud Service on an IP Network



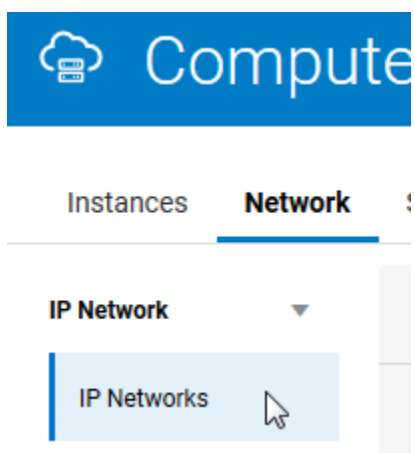
This topic applies only to Oracle Cloud Infrastructure Classic.

If you want to provision Oracle SOA Cloud Service on an IP network, follow the steps described in this section.

Create an IP Network

To complete this task, you must have the `Compute_Operations` role. If you do not have this role, ask your system administrator to assign you this role. See [Modifying User Roles in Managing and Monitoring Oracle Cloud](#).

1. Open the navigation menu and click **OCI Classic Services**. Under **Classic Infrastructure Services**, click **Compute Classic**. The Compute Classic Console is displayed.
2. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
3. Click the **Network** tab.
4. In the **Network** drop-down list, expand **IP Network**, then click **IP Networks**.



5. Click **Create IP Network**.

Update your IP network as required. You can change the IP address prefix, add or remove an IP network exchange, update the description, or enable or disable the network. [Learn more...](#)

*Required

6. Select or enter the required information:

Element	Description
Name	Enter a name for the IP network.
IP Address Prefix	<p>Enter the IP address prefix for this IP network, in CIDR format. When you create instances, you can associate a vNIC on the instance with an IP network. That vNIC on the instance is then allocated an IP address from the specified IP network.</p> <p>Select the IP address prefix for your IP networks carefully. Consider the number of instances that you may want to add to the network. This helps determine the size of the subnet required.</p> <p>If you create multiple IP networks and you may want to add these IP networks to the same IP network exchange, then ensure that you do not allocate overlapping address ranges to these IP networks.</p> <p>Similarly, if you plan to connect to your IP networks using VPN, ensure that the addresses you specify for your IP networks do not overlap with each other or the IP addresses used in your on-premises network.</p> <p>Note: RFC 6598 addresses are not supported.</p>

Element	Description
IP Exchange	Specify the IP network exchange to which you want to add this IP network. An IP network can belong to only one IP network exchange. Before you specify an IP network exchange for an IP network, ensure that the IP addresses in this IP network do not overlap with the IP addresses in any other network in the same IP network exchange. If you do not specify an IP network exchange while creating an IP network, you can do so later by updating an IP network. If you want to connect IP networks using an IP network exchange, do this before creating instances with an interface on those IP networks. This ensures that routes are appropriately configured on instances by the DHCP client during instance initialization.
Description	Enter a meaningful description for your IP network, if required.
Tags	Enter a list of the tags that you want to associate with your IP network, if required.

7. Click **Create**

The IP network is created and added to the specified IP network exchange.

Provision Oracle Cloud Infrastructure Classic

You must provision Oracle Cloud Infrastructure Classic before using the provisioning wizard to create an Oracle SOA Cloud Service instance.



Note:

When you provision Oracle Cloud Infrastructure Classic, specify the same IP network value that you created.

Provision an Instance

1. Follow the steps in [Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure Classic](#) to invoke the Oracle SOA Cloud Service provisioning wizard.
2. In the **IP Network** field, specify the IP network you created.

Provision an Oracle SOA Cloud Service Instance with Stack Manager



This topic applies only to Oracle Cloud Infrastructure Classic.

Use Oracle Cloud Stack to provision instances of both Oracle SOA Cloud Service and Oracle Database Classic Cloud Service as a single operation.

Oracle Cloud Stack is a component of Oracle Cloud that enables you to create multiple cloud resources as a single unit called a stack. You create, delete and manage these resources together as a unit, but you can also access, configure, and manage them through their

service-specific interfaces. Stacks also define the dependencies between your stack resources, so that Oracle Cloud Stack creates and destroys the resources in a logical sequence.

Stacks are created from templates. The Quick Start feature of Oracle SOA Cloud Service uses stack templates so that you can quickly create service instances based on standard configurations.

Oracle Cloud Stack also includes a certified Oracle stack template named `Oracle-SOACS-DBCS-Template`. This template creates a stack that's comprised of these resources:

- A database deployment in Oracle Database Classic Cloud Service
- A service instance in Oracle SOA Cloud Service that is connected to the database deployment
- A storage container in Oracle Cloud Infrastructure Object Storage Classic to support cloud backups for the Oracle SOA Cloud Service instance and the database deployment

Topics:

- [Get Started](#)
- [Template Parameters](#)
- [Create a Stack with the CLI](#)
- [Customize the Template](#)

Get Started

Create a stack using the `Oracle-SOACS-DBCS-Template` template. Refer to these topics in *Using Oracle Cloud Stack Manager*:

- [Accessing Oracle Cloud Stack Manager](#)
- [Creating a Cloud Stack](#)

A video and a tutorial are also available.

 [Video](#)

 [Tutorial](#)

Template Parameters

In the `Oracle-SOACS-DBCS-Template` template, the values of these input parameters can be customized for each stack creation:

- Oracle WebLogic Server and Oracle Database versions
- Oracle WebLogic Server and Oracle Database VM compute shapes (CPU, memory, storage)
- Oracle WebLogic Server user name
- Oracle WebLogic Server and Oracle Database system passwords
- Oracle Database name (SID)
- Oracle Database usable storage in Gigabytes

- SSH public key for all nodes
- Name of the Oracle Cloud Infrastructure Object Storage Classic container to create
- Storage user name and password

The stack name (the predefined parameter `serviceName`) is used to name the new services. This stack name is joined with the text `SOACS` and `DBCS`.

Create a Stack with the CLI

In addition to the web console, Oracle Cloud Stack supports the same command line interface (CLI) that you can use to create and manage an Oracle SOA Cloud Service instance. Execute the `stack create` command and specify the template's name, `Oracle-SOACS-DBCS-Template`. Provide values for the template parameters, and be sure to properly enclose any values that contain white space or other special characters. For example:

```
psm stack create -n MyStack -t Oracle-SOACS-DBCS-Template -p
commonPwd:"password" backupDestination:"BOTH"
backupStorageContainer:"https://acme.storage.oraclecloud.com/v1/MyService-
acme/MyContainer" backupStorageUser:"john@example.com"
backupStoragePassword:"password" publicKeyText:"key_text"
```

To identify the parameter names to use with the CLI, view or export the template. See [Viewing a Template](#) in *Using Oracle Cloud Stack Manager*.

Customize the Template

Use Oracle Cloud Stack to copy and update the `Oracle-SOACS-DBCS-Template` template in order to customize your stack's behavior. Modify the template's name and contents, such as adding a template parameter or changing the parameters used to provision the Oracle SOA Cloud Service instance. Refer to these topics in *Using Oracle Cloud Stack Manager*:

- [Cloning an Oracle Template](#)
- [Creating Resources](#)
- [Creating Template Parameters](#)

Tip:

While editing a resource in a stack template, place your mouse over a parameter name to view its description.

See below for some examples of customizing this stack template.

Enable Access to the Administration Console

By default, network access to the WebLogic Server Administration Console in an Oracle SOA Cloud Service instance is disabled for security reasons. To enable access to the console after creating a stack, see [Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure Classic](#). Alternatively, you can update the template and enable access to the console at the time the service instance is provisioned. Edit the Oracle SOA Cloud Service resource and set `enableAdminConsole` to `true`.

Set the WebLogic Server Cluster Size

By default, the Oracle WebLogic Server domain in an Oracle SOA Cloud Service instance contains a single Managed Server to host your Java Enterprise applications. This is appropriate for a development environment, but test or production systems may require a larger cluster of Managed Servers. Oracle SOA Cloud Service allows users to scale out an existing service instance after creating it, but alternatively you can update the stack template. Edit the Oracle SOA Cloud Service resource, expand `components` and `WLS`, and then set `managedServerCount`.

```
components:
  WLS:
    ...
    managedServerCount: 3
```

Create a Separate Application Database

An Oracle SOA Cloud Service instance requires at least one Oracle Database Classic Cloud Service deployment in order to host the required Oracle schemas. But a new Oracle SOA Cloud Service instance can also connect to a second database deployment (or a second Pluggable Database in the same database deployment) to separate the Oracle schemas from your application schemas. Create a second database resource in your template and associate it with the Oracle SOA Cloud Service instance.

1. Add a second Oracle Database Classic Cloud Service resource to your template named `dbcs2`. See [Creating Resources](#) in *Using Oracle Cloud Stack Manager*.
2. For the database deployment's `serviceName` parameter, use the `Join` function to give the resource a unique name. For example:

```
'Fn::Join':
  - ''
  - - 'Fn::GetParam': serviceName
    - DBCSAPP
```

3. Edit the Oracle SOA Cloud Service resource, expand `components` and `WLS`, and then set `appDBs` to the following value:

```
- dbServiceName:
  'Fn::GetAtt':
    - dbcs2
    - serviceName
  dbName: sys
  dbaPassword:
    'Fn::GetParam': commonPwd
```

Provision a Custom Oracle SOA Cloud Service Instance on Oracle Cloud Infrastructure Classic

You use the Oracle Cloud Infrastructure Classic provisioning wizard to provision a custom Oracle SOA Cloud Service instance.

Topics:

- [Start the Provisioning Wizard](#)
- [Specify Basic Service Instance Information](#)
- [Specify the Service Instance Details](#)
- [Confirm Your Selections](#)

Start the Provisioning Wizard



This topic applies only to Oracle Cloud Infrastructure Classic.

Start the provisioning process by creating a new service instance:

- In the [Oracle SOA Cloud Service Console](#), click **Create Instance**.

SOA Cloud Service						
Welcome!						
Instances Activity SSH Access						
Summary						
5	10	112.5 GB	722 GB	10		
Instances	OCPUs	Memory	Storage	Public IPs		
Instances						
Search by instance name						
Create Instance						
	SOAOSBB2BipResv0103	Version: 12.2.1.2.0	Nodes: 2	Created On: Jan 3, 2018 10:33:26 PM UTC	OCPUs: 2	Memory: 22.5 GB
	SOAOSBB2B1213	Version: 12.1.3.0.6	Nodes: 2	Created On: Jan 3, 2018 10:11:52 PM UTC	OCPUs: 2	Memory: 22.5 GB
					Storage: 146 GB	
					Storage: 138 GB	

The **Create Instance** page is displayed.

Specify Basic Service Instance Information



This topic applies only to Oracle Cloud Infrastructure Classic.

On the Create Instance page, enter basic information for your service instance, including service name, service level, metering frequency, software release, and software edition.

Create Instance

Cancel

Instance
Details
Confirm

Next >

Create SOA Cloud Service Instance
Provide basic instance information

* Service Name

Service Description

Notification Email

* Region

IP Network

Tags

* SSH Public Key Edit

License Type My organization already owns Oracle middleware software licenses. Bring my existing middleware software license to the SOA Cloud Service.

Subscribe to a new SOA Cloud Service software license and the SOA Cloud Service.

* Software Release

Service Type

Components Installed

Service Name

Specify a name that you will use to identify the new service instance. The name must be unique within the identity domain and must meet the following conditions:

- Must start with a letter
- Cannot be longer than 50 characters
- Cannot contain non-alphanumeric characters other than the hyphen character.

Service Description

You may add an optional description that can be used to help identify this new service. The description is only used during service list display and is not used internally.

Notification Email

(Optional) Specify an email address where you would like to receive a notification when the service instance provisioning has succeeded or failed.

Service Type	Components Installed
Region	<p>(Available only if your account has regions) Select a region if you want to create the service instance in a specific region, or if you want to use a custom IP network. You must also select a region if you intend to assign reserved IP addresses to your service instance nodes.</p> <p>Do not select Oracle Cloud Infrastructure regions such as us-phoenix-1, us-ashburn-1, or eu-frankfurt-1. For a complete list of Oracle Cloud Infrastructure regions that should not be selected, see Data Regions for Platform and Infrastructure Services.</p> <p>The Oracle Database Classic Cloud Service deployment that you intend to associate with your Oracle SOA Cloud Service instance must be in the same region that you select in this field.</p> <p>If you select No Preference, Oracle SOA Cloud Service will select one of the available Oracle Cloud Infrastructure Classic regions. However, you will not be able to use an IP network or reserved IP addresses for your service instance.</p>

Service Type	Components Installed
IP Network	<p>If the <i>regions</i> and <i>IP networks</i> features are supported for your account, during provisioning you can attach the service instance to an IP network that is already created in Oracle Compute Cloud Service. A region name must be explicitly specified when you use an IP network. When you specify an IP network during provisioning, you must also specify a database deployment on Oracle Database Classic Cloud Service or Oracle Database Exadata Cloud Service that is on an IP network. If your Oracle SOA Cloud Service and Oracle Database Classic Cloud Service or Oracle Database Exadata Cloud Service are attached to different IP networks, then the two IP networks must be connected to the same IP network exchange. Access rules required for communication between the Oracle SOA Cloud Service instance and Oracle Database Classic Cloud Service or Oracle Database Exadata Cloud Service deployment are created automatically when connected with IP exchange. See <i>Creating an IP Network in Using Oracle Cloud Infrastructure Compute Classic</i>.</p> <p>Creating IP Networks</p> <ul style="list-style-type: none"> • If the IP Network field is not visible in the wizard for your account, IP network functionality is probably not enabled in your data center. Contact Oracle Support if you want to use the IP network feature for your account. • Oracle Database Classic Cloud Service Behavior: <ul style="list-style-type: none"> – When you do <i>not</i> choose a Region/IP Network in the provisioning screens, Oracle SOA Cloud Service provisioning screens allow you to choose Oracle Database Classic Cloud Service not in an IP network. This is equivalent to non-IP network functionality. – When you choose a Region/IP Network in the provisioning screens: <ul style="list-style-type: none"> * The Oracle SOA Cloud Service provisioning screens list all Oracle Database Classic Cloud Service entries from all IP networks. * The Oracle SOA Cloud Service provisioning screens list Oracle Database Classic Cloud Service entries from the same subnet. * The provisioning screens do not list Oracle Database Classic

Service Type	Components Installed
	<p>Cloud Service entries from non-IP networks.</p> <ul style="list-style-type: none"> * You must ensure that you use a Oracle Database Classic Cloud Service from an IP network with which your Oracle SOA Cloud Service instance can exchange packets. In other words, Oracle SOA Cloud Service and Oracle Database Classic Cloud Service should be in the same IP network or in IP networks that are connected with an IP exchange. * Internal IP addresses from the IP network subnet are assigned to VMs when provisioning completes. <p>Updating IP Networks</p> <ul style="list-style-type: none"> • When you update IP networks: <ul style="list-style-type: none"> – Make sure you do not change the IP address of a subnet, only change the IP prefix. – The IP prefix should be changed to expand the current IP network. For example, to change the prefix from /27 to /8 to expand the network. – Restart VMs from the Oracle SOA Cloud Service Console as soon as you update an IP network prefix. Failing to restart the VMs causes Console URLs not to work properly during backup. <p>Deleting IP Networks</p> <ul style="list-style-type: none"> • If you plan to delete the IP network/IP exchange, make sure all VMs and instances are deleted. • Instances are no longer functional when the IP networks are deleted. Therefore, the Enterprise Manager, WebLogic Server, and other Oracle SOA Cloud Service Consoles are not accessible. • To re-enable instances, you can recreate the IP networks/IP exchange with the exact same name and IP subnet (with a similar prefix). • Every time an instance is deleted, the private IP address is reclaimed by the subnet.

Service Type	Components Installed
Tags	<p>(Not available on Oracle Cloud at Customer)</p> <p>(Optional) Select existing tags or add tags to associate with the service instance.</p> <p>To select existing tags, select one or more check boxes from the list of tags that are displayed on the pull-down menu.</p> <p>To create tags, click Click to create a tag to display the Create Tags dialog box. In the New Tags field, enter one or more comma-separated tags that can be a key or a key:value pair.</p> <p>If you do not assign tags during provisioning, you can create and manage tags after the service instance is created. See Create, Assign, and Unassign Tags.</p>
SSH Public Key	<p>Specify the value of the VM Public Key, or the name of the file that contains the public key value.</p> <p>Define the public key for the secure shell (SSH). This key is used for authentication when connecting to the Oracle SOA Cloud Service instance using an SSH client.</p> <p>Click Edit to display the public key input for VM access and specify the public key using one of the following methods:</p> <ul style="list-style-type: none"> • Select Key File Name and click Browse to select a file that contains the public key for the secure shell (SSH). • Select Key Value and paste or type a key value in the text box. • Select Create a New Key and click Enter. The Provisioning Wizard generates a key for you. When prompted, save it as a file on your hard drive. Select Key File Name and click Browse to select the file.

Service Type	Components Installed
License Type	<p>Choose whether you want to leverage the Bring Your Own License (BYOL) option or use your Oracle SOA Cloud Service license.</p> <ul style="list-style-type: none"> The first option enables you to bring your on-premises Oracle WebLogic Server licenses to Oracle Cloud. Bring Your Own License (BYOL) instances are billed at a lower rate than other instances. See Frequently Asked Questions: Oracle BYOL to PaaS. <p>You must own a Universal Credits subscription or Government subscription in order to use BYOL.</p> <p>Before you scale out a BYOL instance, you must have enough WebLogic Server licenses for the additional OCPUs that will be allocated to the instance after it is scaled.</p> <ul style="list-style-type: none"> The second option subscribes to a new Oracle SOA Cloud Service license. In this case, your account will be charged for the new service instance according to your Oracle SOA Cloud Service agreement.
Software Release	<p>WebLogic Server and Fusion Middleware 12.2.1.4.0 and 12.2.1.3.0 are supported.</p> <p>Note: You cannot upgrade Oracle SOA Cloud Service instances from earlier releases (such as 12.2.1.3.0) to the latest release (12.2.1.4.0). Instead, provision a new 12.2.1.4.0 instance.</p>
Metering Frequency	<p>You will see the Metering Frequency field if you are using a <i>metered</i> account. The default metering frequency is Monthly.</p> <p>Note: Hourly metering is not currently supported. If you choose the Hourly option you will receive a validation error stating that the service type and hourly metering frequency combination is not a valid entitlement.</p>

Specify the Service Instance Details



This topic applies only to Oracle Cloud Infrastructure Classic.

In the Instance Details page, you can configure the service type, shape, size, database, and other important details for your instance.

Create SOA Cloud Service Instance Details
Some settings are dependent on current region, **eucom-north-1**. Go back to select a different region. [Selection Summary](#)

Select Service Type

* Service Type: SOA with SB & B2B Cluster

Enable B2B adapter for EDI:

Weblogic

* Compute Shape: OC1m - 1.0 OCPU, 15.0GB RAM

* Cluster Size: 1

Reserved IPs: Assign Automatically

* User Name: weblogic

* Password: [masked]

* Confirm Password: [masked]

Database Configuration

Name: <Select an instance>

Load Balancer Configuration

Provision Load Balancer:

Backup and Recovery Configuration

* Storage Container Name: https://oicpm.eu.storage.oracle

* Storage User Name: username

* Cloud Storage Password: [masked]

Create Cloud Storage Container:

Topics:

- [Select Service Type](#)
- [Configure WebLogic Server Access](#)
- [Configure the Database](#)
- [Configure the Load Balancer](#)
- [Configure Backup and Recovery](#)

Select Service Type

This topic applies only to Oracle Cloud Infrastructure Classic.

Select one of the available service types for your Oracle SOA Cloud Service instance.

Table 4-1 Service Types

Item	Description
Business Activity Monitoring	Install and configure Business Activity Monitoring (Oracle BAM). See "Understanding Oracle Business Activity Monitoring" in <i>Monitoring Business Activity with Oracle BAM</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).
SOA with SB & B2B Cluster	Install and configure Oracle SOA Suite, Oracle Service Bus, Oracle B2B, Oracle Technology Adapters, and Oracle Cloud Adapters. When you select this service type, the Enable B2B Adapter for EDI checkbox is presented below the dropdown list. You can choose to enable the B2B Adapter for EDI. See B2B Adapter for EDI .

Configure WebLogic Server Access



This topic applies only to Oracle Cloud Infrastructure Classic.

Specify information about your Oracle WebLogic Server compute shape and administrator details.

Item	Description
Cluster Size	<p>Oracle SOA Cloud Service always creates a domain with one or more servers in a cluster. Choose the cluster size. Choose between 1, 2, 4 or 8 virtual machines (nodes).</p> <p>Note: If you configure more than one node, it is highly recommended that you enable the load balancer on the next page of the Provisioning Wizard.</p>
Reserved IPs	<p>Select reserved IP addresses for the nodes in your cluster, or leave the default value as Assign Automatically if you want Oracle to automatically assign IP addresses to these nodes. The number of IP addresses that you select must equal the number of nodes in the cluster.</p> <p>If using Oracle Database Exadata Cloud Service, you must deselect Assign Automatically and explicitly select an IP address.</p> <p>This option is displayed only if you selected a specific Region for this service instance.</p> <p>This field is mandatory if you are using Oracle Database Exadata Cloud Service as your database and optional if you are using Oracle Database Classic Cloud Service.</p> <p>You create IP reservations by using the IP Reservations tab in the Oracle SOA Cloud Service Console or by clicking the + sign to the right of this field. If you do not see this tab on the console, click the gear icon next to this field and follow the instructions to create your first IP reservation. After creating IP reservations, you need to restart the instance creation wizard. See Create and Manage IP Reservations.</p>

Item	Description
Assign IP Reservations	<p>If you are provisioning an Oracle SOA Cloud Service instance and you associate your service instance with an Oracle Database Exadata Cloud Service database deployment, you must assign the previously reserved IP addresses for your instance nodes.</p> <p>This task is only required if you plan to use an Oracle Database Exadata Cloud Service database deployment for either the Oracle Required Schema or Application Schema databases.</p> <p>For information on reserving IP addresses, see Reserve IP Addresses for Oracle Database Exadata Cloud Service When Region Not Enabled.</p> <ol style="list-style-type: none"> 1. Click the Assign IP Reservations button to open the IP Reservations for WebLogic dialog. <p>Note that the Assign IP Reservations button is inactive until you specify an Oracle Database Exadata Cloud Service database deployment in the Database Configuration:Name field.</p> 2. On the dialog, move the IP addresses from the Available list to the Selected list. <p>The number of IP addresses you select must be equal to the requested Cluster Size. The first IP address you select is used for the Administration Server node. Subsequent IP addresses are assigned to the remaining Managed Server nodes.</p> 3. Click the checkbox adjacent to the text Check this box to confirm that selected IP are opened up on the Exadata firewall. 4. Click Assign. <p>You will receive an error message if you click Next and have neglected to specify the reserved IP addresses.</p> <p>If you need to scale out your service at a later time, you will first need to request another IP reservation.</p>
User Name	<p>The user name of the Oracle WebLogic Server administrator.</p> <p>Note that you can change the user name through the WebLogic Server Administration Console after you have created the instance.</p>

Item	Description
Password	<p>Specify an Oracle WebLogic Server administrator password that meets the following criteria:</p> <ul style="list-style-type: none"> • It must begin with a letter. • It must contain between 8 and 30 characters. • It must contain at least one number. • Optionally, it can contain any number of the following special characters: <p style="text-align: center;">\$ # _</p> <p style="text-align: center;">. For example: Ach1z0#d.</p>

Configure the Database



This topic applies only to Oracle Cloud Infrastructure Classic.

Specify information about your database.

For details about the databases supported by Oracle SOA Cloud Service in Oracle Cloud Infrastructure Classic, see [Database](#).

In the Provisioning Wizard, specify the following information:

Item	Description
Name	Select an existing Oracle Database Classic Cloud Service or Oracle Database Exadata Cloud Service instance name. Note that only the Oracle Database Classic Cloud Service in the selected region are available for selection.
PDB Name	<p>Enter an optional pluggable database (PDB) name. If a pluggable database name is not specified, the pluggable database name specified during Oracle Database Classic Cloud Service provisioning is used as the default.</p> <p>Note:</p> <ul style="list-style-type: none"> • This field is mandatory if using an Oracle Database Exadata Cloud Service instance. • Oracle SOA Cloud Service supports the use of only a single pluggable database.
Administrator User Name	Your Oracle Database Classic Cloud Service user name. This value must be set to a database user with SYSDBA system privileges. You can use the default user SYS or any user that has been granted the SYSDBA privilege.
Password	The database administrator password specified when the Oracle Database Classic Cloud Service instance was created.

 **Note:**

Oracle SOA Suite automatically creates SOA schemas in this database, such as SOAINFRA and MDS. The SOA schemas take the same password that you specified in the [WebLogic](#) section of this wizard.

Configure the Load Balancer



This topic applies only to Oracle Cloud Infrastructure Classic.

Specify whether or not you want to use the OTD load balancer.

 **Notes:**

- If you do not select a load balancer, then the Managed Server URLs (b2bconsole, worklistapp) are not accessible using the load balancer IP address.
- You can add a load balancer later if you do not configure a load balancer while provisioning your Oracle SOA Cloud Service instance. See [Add an Oracle Traffic Director Load Balancer to an Oracle SOA Cloud Service Instance Post-Provisioning](#).

Item	Description
Provision Load Balancer	<p>Select the check box to provision a load balancer. A load balancer delivers the following benefits:</p> <ul style="list-style-type: none"> • Manages the routing of requests across all Managed Servers. • Enables you to configure the routing policy. • Enables you to suspend an Oracle SOA Cloud Service instance temporarily to perform routine maintenance, as described in Suspending an Oracle SOA Suite Cloud Service Instance. <p>If you have more than one node in your cluster and do not choose a load balancer during provisioning, then only one server receives all of the work requests, while the other server(s) in the cluster are idle. The server that receives all of the HTTP requests might become overloaded, while the other servers are under utilized.</p> <p>To add an OTD load balancer later, see Add an Oracle Traffic Director Load Balancer to an Oracle SOA Cloud Service Instance Post-Provisioning.</p>

Item	Description
Load Balancer Policy	<p>If the Provision Load Balancer check box is selected:</p> <ul style="list-style-type: none"> • Least Connection Count. Passes each new request to the Managed Server with the least number of connections. This policy is useful for smoothing distribution when Managed Servers slow down. Managed Servers with greater processing power receive more connections over time. • Least Response Time. Passes each new request to the Managed Server with the fastest response time. This policy is useful when Managed Servers are distributed across networks. • Round Robin. Passes each new request to the next Managed Server in line, evenly distributing requests across all Managed Servers regardless of the number of connections or response time.
Compute Shape	<p>If the Provision Load Balancer check box is selected: Select the number of Oracle Compute Units (OCPU) and amount of RAM memory that you want to allocate to the VM for the load balancer. The larger the compute shape, the greater the processing power.</p> <p>The valid compute shapes for Oracle Cloud Infrastructure Classic are:</p> <ul style="list-style-type: none"> • OC3M: 1 OCPU, 7.5GB RAM • OC4M: 2 OCPU, 15.0GB RAM • OC5M: 4 OCPU, 30.0GB RAM • OC6M: 8 OCPU, 60.0GB RAM <p>Note that you cannot change the compute shape after you have created the Oracle SOA Cloud Service instance.</p>
Reserved IPs	<p>If the Provision Load Balancer check box is selected: Select a reserved IP address.</p> <p>If using Oracle Database Exadata Cloud Service, you must deselect Assign Automatically and select an IP address. You must select a different IP address from what you selected in the WebLogic section of the wizard. That IP address is disabled from selection in this list.</p>

Configure Backup and Recovery

Specify information about your Oracle WebLogic Server compute shape and administrator details. Specify information about the storage container that will be used to store backups. It's a good idea to create a separate container for each instance you create.



Note:

You must have a current subscription to Oracle Cloud Infrastructure Object Storage Classic.

Item	Description
Storage Container Name	Enter the name of the Oracle Cloud Infrastructure Object Storage Classic container used to provide storage for your service instance backups using the following format: <i>Storage-storage_identitydomain/containername</i> For example: <i>Storage-us4112opcs0a01/InsightBackup</i> Note: If the storage is used to back up the database, the name cannot include more than one “-” character in the name. If the name contains more than one “-” character the backup will fail. By default, all backups that are more than seven days old are moved to the storage service at this URL.
Storage User Name	The name of the Oracle Cloud Infrastructure Classic administrator.
Cloud Storage Password	The password, generated in Oracle Cloud Infrastructure Classic, for the user who created the specified container.
Create Cloud Storage Container	Select this check box to use the information you specified to automatically create the storage container for you.

Confirm Your Selections



This topic applies only to Oracle Cloud Infrastructure Classic.

The confirmation page displays the configuration values you choose in the provisioning wizard.

Review the service details. If you need to change the service details, use the navigation bar or **Previous** button at the top of the wizard to step back through the pages in the wizard. Click **Cancel** to cancel out of the wizard without creating a new

service instance. If you are satisfied with your choices on the Confirmation page, click **Create**.

**Note:**

It takes about an hour and a half to create the instance. You are notified by email when it has been created.

Post-Provisioning Tasks in Oracle Cloud Infrastructure Classic

Review the following topics to learn about additional post-provisioning tasks you must complete for the service to work correctly in Oracle Cloud Infrastructure Classic.

**Note:**

The information in this topic applies only to *existing* Oracle SOA Cloud Service accounts.

Topics:

- [Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure Classic](#)
- [Configure VPN as a Service on Oracle Cloud Infrastructure Classic](#)
- [Register a Custom Domain Name with a Third-Party Registration Vendor](#)
- [Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory](#)

Access WebLogic Server Administration and OTD Consoles in Oracle Cloud Infrastructure Classic




This topic applies only to Oracle Cloud Infrastructure Classic.

If you provision an Oracle SOA Cloud Service instance after 1 August 2020 and you are not able to access the WebLogic Server Administration or OTD 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 a rule to allow access to the WebLogic Server Administration or OTD Console URLs:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Manage Access Rules**.
2. Click **Create Rule** to open the Create Access Rule dialog.

Create Access Rule

* Rule Name: ?


Description: ?

* Source: ?

* Destination: ?

* Destination Port(s): ?

* Protocol: ?





















 This operation may take some time.

3. In the Create Access Rule dialog, create a rule to access the WebLogic Server Administration Console:
 - a. In the **Rule Name** field, enter a name for the access rule.
 - b. In the **Source** list, select **<custom>**, then enter the public IP address of the machine where the Administration Server URL is opened from a browser (for example, if your public IP address is x.x.x.x then enter x.x.x.x/32).
 - c. In the **Destination** list, select **WLS_ADMIN_HOST**.
 - d. In the **Destination Port** field, enter 7002.
 - e. In the **Protocol** list, select **TCP**.
 - f. Click **Create**.

Access Rules

You can use access rules to control network access to service components. On this page, you can manage your access rules.

Results per page: 50 17 result(s) as of Apr 30, 2020 11:10:10 PM UTC

Status	Rule Name	Source	Destination	Ports	Protocol	Description	Rule Type	Actions
	ora_p2otd_ssh	PUBLIC-INTERNET	OTD_OTD_SERVER	22	TCP	Permit SSH access to nodes	DEFAULT	
	ora_p2otd_ahttps	PUBLIC-INTERNET	OTD_OTD_SERVER	8989	TCP	Permit public access to the ...	DEFAULT	
	ora_p2otd_chhttps	PUBLIC-INTERNET	OTD_OTD_SERVER	443	TCP	Permit public access to the ...	DEFAULT	
	ora_p2otd_chhttp	PUBLIC-INTERNET	OTD_OTD_SERVER	80	TCP	Permit public access to the ...	DEFAULT	
	sys_infra2otd_admin_...	PAAS-INFRA	OTD_ADMIN_HOST	22	TCP	DO NOT MODIFY: Permit PS...	SYSTEM	
	ora_admin2otd_ssh	WLS_ADMIN	OTD_OTD_SERVER	22	TCP	SSH connections from the ...	DEFAULT	
	ora_ots2ma_chhttp	OTD_OTD_SERVER	WLS_MS	9073	TCP	Permit HTTP connections fro...	SYSTEM	
	ora_ots2ma_chhttps	OTD_OTD_SERVER	WLS_MS	9074	TCP	Permit HTTPS connections f...	SYSTEM	
	accessToConsole	160.34.88.49/32	WLS_ADMIN	7002	TCP	DO NOT MODIFY: Permit WL...	USER	
	ora_p2admin_ssh	PUBLIC-INTERNET	WLS_ADMIN	22	TCP	Permit SSH access to nodes	DEFAULT	

4. Repeat the steps above to add another access rule to access the OTD Console, specifying a **Destination Port** of 8989 and a **Destination** of **OTD_OTD_SERVER**.

Configure VPN as a Service on Oracle Cloud Infrastructure Classic



This topic applies only to Oracle Cloud Infrastructure Classic.

You can set up a VPN connection between your data center and IP networks using VPN as a Service on Oracle Cloud Infrastructure Classic. This provides a secure communication channel between your data center and Oracle SOA Cloud Service instances that are added to your IP networks. For example, from a Oracle SOA Cloud Service instance configured with VPN as a Service, you can connect through FTP or invoke a database at your data center.

Before configuring VPN as a Service with Oracle SOA Cloud Service, you must satisfy the following prerequisites.

- Create an IP network. See [Provision Oracle SOA Cloud Service on an IP Network](#).
- Provision a database to use the same IP network.

After satisfying these prerequisites, VPN as a Service configuration is a several step process:

- You create a virtual network interface card set (VNICset) in which to group all virtual network interface cards (vNICs) that you want to access over the VPN connection. This task is a prerequisite for creating a VPN as a Service instance.
- You create a VPN as a Service instance. This action creates a new VM host on which the VPN as a Service software is installed and an instance is started.
- You configure a tunnel between the VPN as a Service instance and your company's data center. This establishes a secure channel for accessing the data center as if it were inside your Oracle SOA Cloud Service environment.

Topics:

- [Create a Virtual NIC Set](#)
- [Create a VPN Connection Using VPN as a Service](#)

Create a Virtual NIC Set

You must create a virtual network interface card set (vNICset) in which to group all virtual network interface cards (vNICs) that you want to access over the VPN connection. Each instance (Oracle SOA Cloud Service and Oracle Database Cloud Service) has an associated vNIC. This task is a prerequisite for creating a VPN connection using VPN as a Service.

1. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.
See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
2. Open the navigation menu and click **OCI Classic Services**. Under **Classic Infrastructure Services**, click **Compute Classic**.
3. Click the **Network** tab.
4. In the left navigation pane, select **IP Network**, then **Virtual NIC Sets**.
5. Click **Create vNICset**.
6. Select or enter the required information:

Element	Description
Name	Enter a name for the vNICset.
vNICs	Select the required vNICs (for example, Oracle Database Cloud Service and Oracle SOA Cloud Service). Without a vNIC, traffic through your company's gateway is not allowed. vNICs are created automatically when you provision Oracle SOA Cloud Service and Oracle Database Cloud Service.
Applied Access Control Lists	Select the access control lists (ACLs) that you want to apply to this vNICset, including the default ACL. When you apply an ACL to a vNICset, all security rules in that ACL are applied to traffic to or from each of the vNICs in the vNICset. ACLs are created automatically when you provision Oracle SOA Cloud Service and Oracle Database Cloud Service.
Description	Enter a meaningful description for the vNICset.
Tags	Enter a list of the search tags that you want to associate with this vNICset.

7. Click **Create**.

The vNICset is created. You can use this vNICset as the next hop in any routes that you create, or as the source or destination in a security rule. ACLs are also applied to vNICsets.

You can manage your vNICsets. See *Managing vNICsets* in *Using Oracle Cloud Infrastructure Compute Classic*.

Create a VPN Connection Using VPN as a Service

After creating the vNICset, you can create a VPN instance and configure a tunnel between Oracle SOA Cloud Service and your data center using VPN as a Service.

1. In the left navigation pane, select **VPN > VPNaaS > VPN Connections**.

This page shows details about the created VPN as a Service instances.

- **Name:** The name of the VPN as a Service instance.
- **Tunnel/Life Cycle:** The status of the tunnel (up or down) and the instance. If the tunnel is up and the instance is ready, you can use VPN as a Service to connect to your data center.
- **Public IP/Private IP:** The public and private IP addresses. Nothing needs to be manually entered. These are automatically created.
- **IP Network:** The IP network on which the Oracle SOA Cloud Service was created.
- **Customer Gateway:** The gateway of your company.
- **Customer Reachable Route:** The reachable route of your company.

2. Click **Create VPN Connection**.

3. Select or enter the required information:

Element	Description
Name	Enter a name for the VPN connection.
IP Network	Select the IP network that you want to access over this VPN connection. This is the same IP network you configured for your database and Oracle SOA Cloud Service instance or another IP network that is in the same IP exchange with the IP network you configured for your database.
Connected IP Networks	This field displays the IP networks reachable over this VPN connection. The VPN connection enables you to access all IP networks that are added to the same IP network exchange as the specified IP networks.
vNICsets	Select the vNICsets that contain the vNICs that you want to access over this VPN connection. A vNIC must belong to one of the specified vNICsets and be part of one of the connected IP networks to be reachable over this VPN connection. The vNICsets determine which instances can communicate over the VPN as a Service instance. You must first click Create to display the available vNICsets.
Customer Gateway	Enter the public IP address of the VPN device in your data center to which you want to connect.
Customer Reachable Routes	Enter (in CIDR format) a comma-separated list of subnets in your data center that should be reachable using this VPN connection.
Pre-shared Key	The pre-shared key (PSK), is used while setting up the VPN connection to establish the authenticity of the gateway that is requesting the connection. You must enter the same key here and on the gateway in your data center. The PSK must contain only alphanumeric characters.
IKE ID	<p>The Internet Key Exchange (IKE) ID identifies the cloud gateway on the gateway in your data center. Only IKE v1 in Main Mode is supported. The IKE ID can be the name or IP address of your cloud gateway. If you do not specify the IKE ID, then the IP address of your cloud gateway is used by default. Alternatively, you can specify a text string that to use as the IKE ID. The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period (.), hyphen (-), and underscore (_). The IKE ID cannot contain embedded space characters.</p> <p>Note: If you specify the IKE ID, ensure that you specify the Peer ID type as Domain Name on the gateway in your data center. Other Peer ID types, such as email address, firewall identifier or key identifier, are not supported.</p>

Element	Description
Specify Phase 1 IKE Proposal	<p>Select this option to specify Phase 1 IKE v1 options, if required. You can specify the following values:</p> <ul style="list-style-type: none"> • IKE Encryption: Select the IKE encryption algorithm. • IKE Hash: Select the IKE hash algorithm. • IKE DH group: Select the Diffie Hellman (DH) group. • IKE Lifetime: Specify a value between 600 seconds to 9999999 seconds. The default value is 28800 seconds. <p>If no values are specified, all possible values are permitted.</p>
Specify Phase 2 ESP Proposal:	<p>Select this option to specify Phase 2 Encapsulating Security Payload (ESP) options, if required. You can specify the following values:</p> <ul style="list-style-type: none"> • ESP Encryption: Select the ESP encryption algorithm. • ESP Hash: Select the ESP hash algorithm. • IPSEC Lifetime: Specify a value between 600 seconds to 9999999 seconds. The default value is 3600 seconds. <p>If no values are specified, all possible values are permitted.</p>
Require Perfect Forward Secrecy	<p>Deselect this check box, which is selected by default. If the gateway in your data center supports Perfect Forward Secrecy (PFS), retain this setting to require PFS.</p>
Description	Enter a description.
Tags	Specify one or more tags to help you identify and categorize the VPN connection.

4. Click **Create**.

After the VPN connection is created successfully (the status of the **Life Cycle** is displayed as **Ready**, but the status of **Tunnel** is **Down**), you see the public IP address appear for the VPN connection created. The public IP address is created automatically with the VPN connection creation.

5. Note the public IP address of the created VPN as a Service and add the public IP address in your on-premises data center.

The status of tunnel changes to **Up** after several minutes.

You can manage your VPN as a Service connections. See [Setting Up a VPN Connection Using VPNaaS in *Using Oracle Cloud Infrastructure Compute Classic*](#).

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 SOA Cloud Service 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 SOA Cloud Service 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 Cloud Service 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.
- See [Import a CA-Issued SSL Certificate to the Load Balancer](#) and [Associate the SSL Certificate With the Load Balancer](#).

Move a Customized plan.xml File from the Oracle Fusion Middleware Home Installation Directory

Oracle SOA Cloud Service uses image-based patching, which means that the Oracle Fusion Middleware home installation directory is replaced with a new image when a patch upgrade occurs. Any post-installation configuration changes you make to the `plan.xml` file in the installation subdirectory (`$MW_HOME/soa/soa/plan.xml`) are overridden when upgrade patching occurs:

If you need to customize the `plan.xml` file after installation, ensure that you place this file outside the installation directory. Otherwise, patching overrides your changes.

5

Deploy Applications to an Oracle SOA Cloud Service Instance

Learn about the tasks related to deploying applications to an Oracle SOA Cloud Service instance.

Topics:

- [Deploy and Undeploy Applications to an Oracle SOA Cloud Service Instance](#)
- [Use a Shared File System](#)
- [Use an OTD Host Name with an Oracle Service Bus Business Service](#)
- [Connect to MFT Embedded Servers Using Oracle Traffic Director](#)
- [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 to an Oracle SOA Cloud Service Instance

You can deploy and undeploy applications to an Oracle SOA Cloud Service instance using JDeveloper, Fusion Middleware Control, the WebLogic Server Administration Console, and WLST commands. You cannot deploy and undeploy applications directly through the Oracle SOA Cloud Service Console.

Topics:

- [Use Oracle JDeveloper to Deploy an Application](#)
- [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](#)

Use Oracle JDeveloper to Deploy an Application

You can use Oracle JDeveloper to deploy a SOA composite application or Oracle Service Bus application to an Oracle SOA Cloud Service instance.

Topics:

- [Add an Ingress/Access Rule to Allow the JDeveloper Connection](#)
- [Create an Application Server Connection in JDeveloper](#)
- [Deploy a SOA Composite Application to Oracle SOA Cloud Service from JDeveloper](#)

- [Deploy an Oracle Service Bus Application to Oracle SOA Cloud Service from JDeveloper](#)



Add an Ingress/Access Rule to Allow the JDeveloper Connection


After provisioning the Oracle SOA Cloud Service 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 Cloud Service:

1. On the [Instance Overview page](#) of the provisioned Oracle SOA Cloud Service instance, make a note of the public IP address (or addresses in the case of a multinode cluster) associated with each SOA server.

Resources

	Host Name: sob1221311test-wls-1	OCPUs: 1
	Public IP: 129.146.136.141	Memory: 15 GB
	Shape: VM.Standard2.1	Storage: 247 GB
	Fault Domain: FAULT-DOMAIN-3	
	Instance: Runs sob12213_server_1	
	Availability Domain: trTP:PHX-AD-1	
	Host Name: sob1221311test-wls-3	OCPUs: 1
	Public IP: 158.101.23.141	Memory: 15 GB
	Shape: VM.Standard2.1	Storage: 197 GB
	Fault Domain: FAULT-DOMAIN-2	
	Instance: Runs sob12213_server_3	
	Availability Domain: trTP:PHX-AD-1	

2. In the [Oracle SOA Cloud Service Console](#), click  for the instance and select **Open 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:

Settings for [redacted]_server_1

Configuration Protocols Logging Debug Monitoring Control Deployments Services

General Cluster Services Keystores SSL Federation Services Deployment Migration

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

Name: [redacted]_server_1

Template: [redacted]_cluster_Template [Change](#)

Machine: [redacted]_machine_1

Cluster: [redacted]_cluster

Listen Address: [redacted]wls-1.soac!

Listen Port Enabled

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 sob1221311test-
wls-1.soacsp2pubsubne.soacsp2vcn.oraclevcn.com
158.101.23.141 sob1221311test-
wls-3.soacsp2pubsubne.soacsp2vcn.oraclevcn.com
129.146.136.141 sob1221311test-wls-1
158.101.23.141 sob1221311test-wls-3
```

5. (Does not apply to Oracle Cloud Infrastructure Classic) Add the ingress rule to permit traffic from JDeveloper to the SSL listener port of the Managed Server:
 - a. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.

See Sign In to Your Cloud Account in *Getting Started with Oracle Cloud*.
 - 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:

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.

6. (For Oracle Cloud Infrastructure Classic only) Add the access rule to permit traffic from JDeveloper to the SSL listener port of the Managed Server:
 - a. In the [Oracle SOA Cloud Service Console](#), click for the service instance and select **Access Rules**.
 - b. In the Create Access Rule dialog, create an access rule for port 9074 to access JDeveloper as shown in the following screenshot. The value in the **Destination Port(s)** field is the SSL listener port of the Managed Server.

- c. Add another access rule for port 9072, with the same source as port 9074.

Important:

By adding this access 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

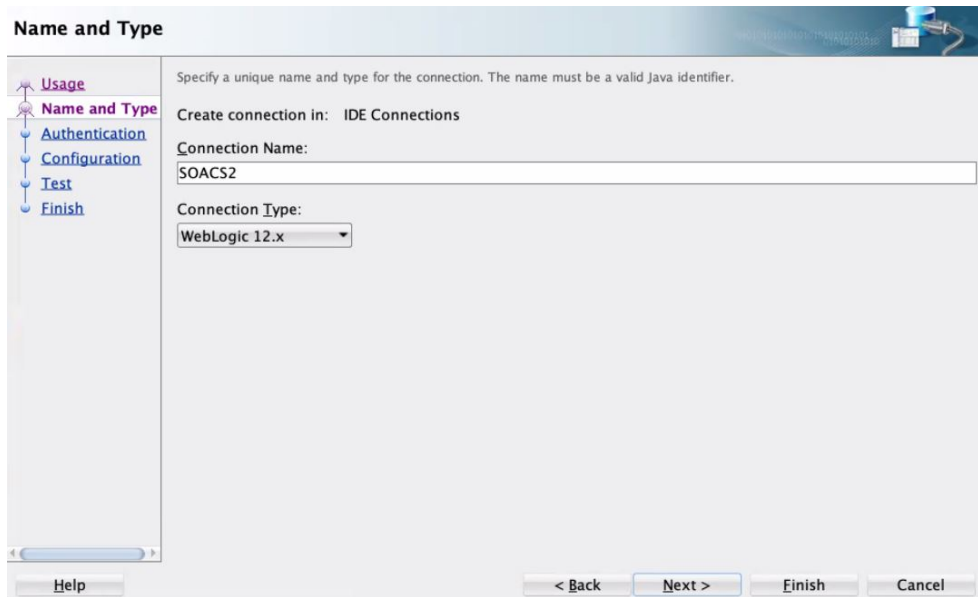
To create a new application server connection in JDeveloper:

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 Cloud Service 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**.

WebLogic Server connections use a host name and port to establish a connection. The Domain of the target will be verified

WebLogic Hostname (Administration Server):
129.146.98.254

Port: 9001 SSL Port: 9072

Always use SSL

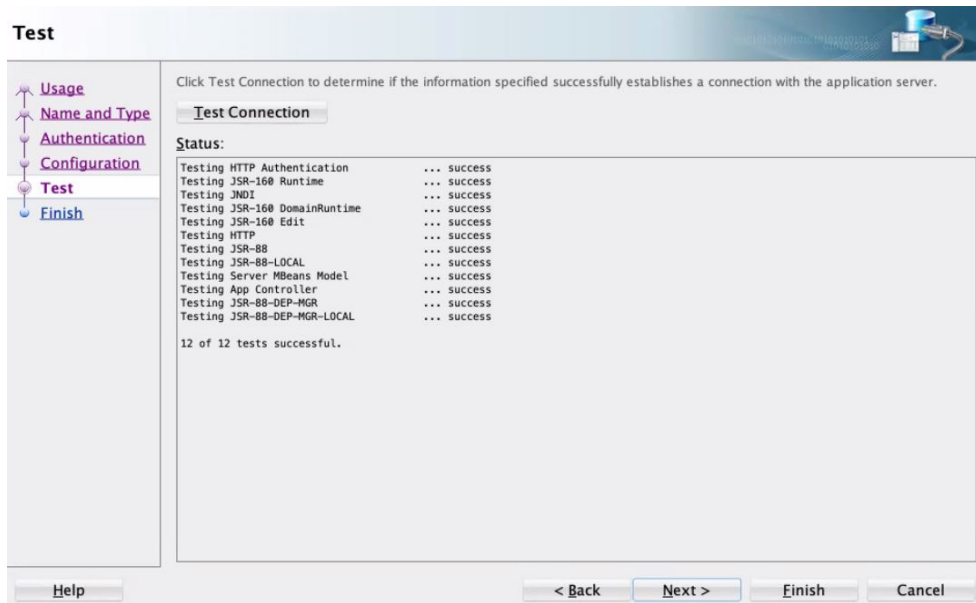
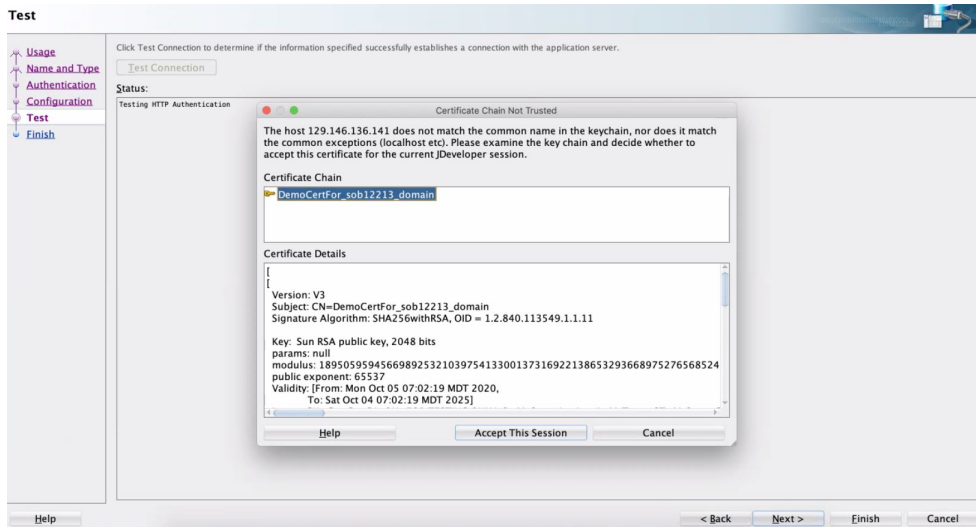
WebLogic Domain:
SOACS122_domain

Help < Back Next > Finish Cancel

- 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.

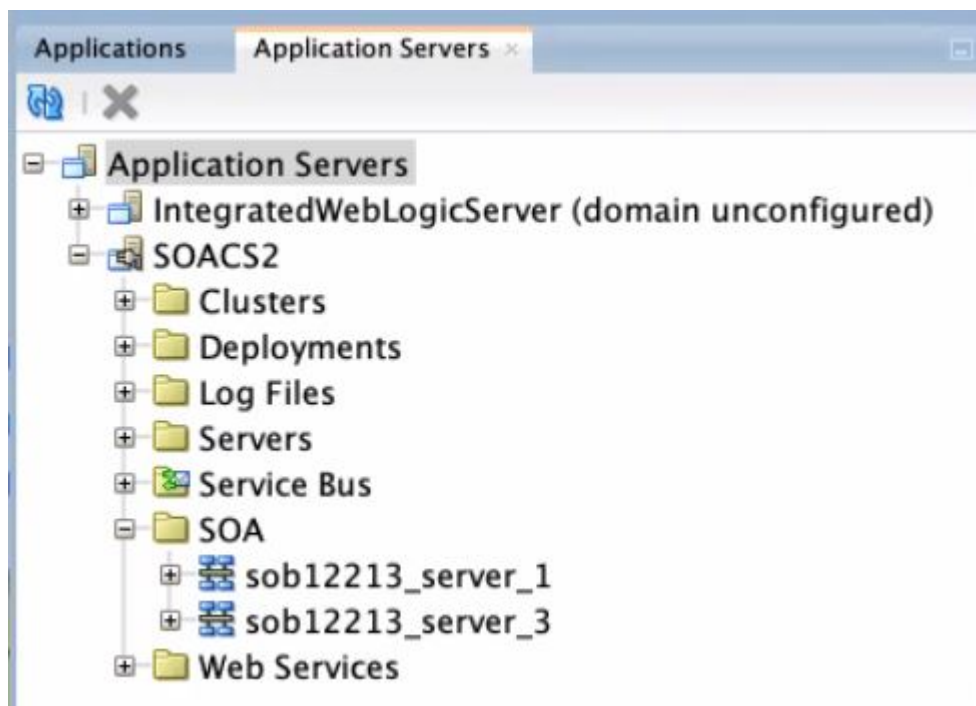


Notes:

- 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.



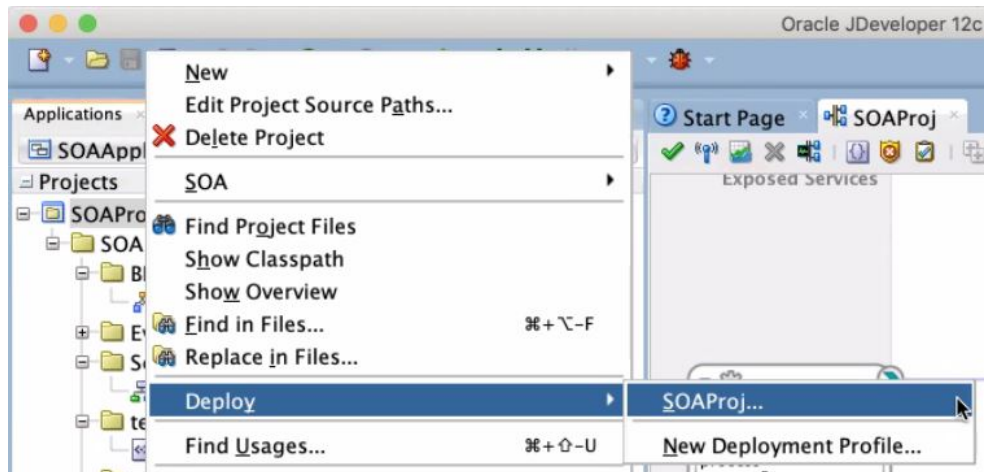
Next step: [Deploy a SOA composite application](#) or [Deploy an Oracle Service Bus application](#).

Deploy a SOA Composite Application to Oracle SOA Cloud Service from JDeveloper

SOA composite applications are deployed to Managed Servers.

To deploy a SOA composite application to Oracle SOA Cloud Service from JDeveloper:

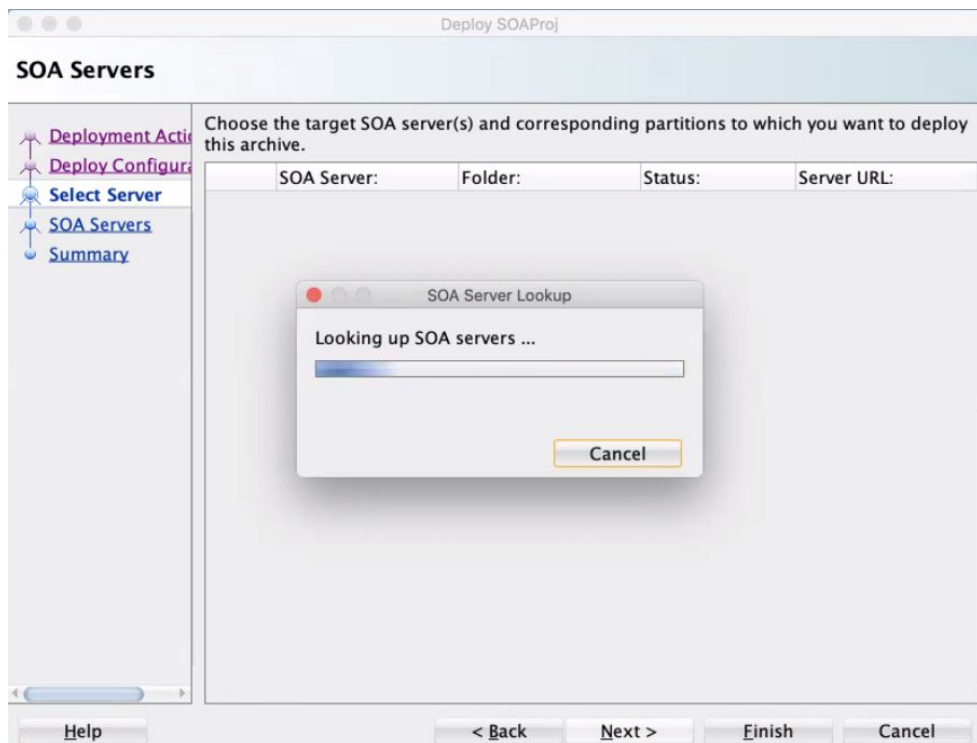
1. In JDeveloper, right-click the SOA project you want to deploy and select **Deploy**, then the name of the project.

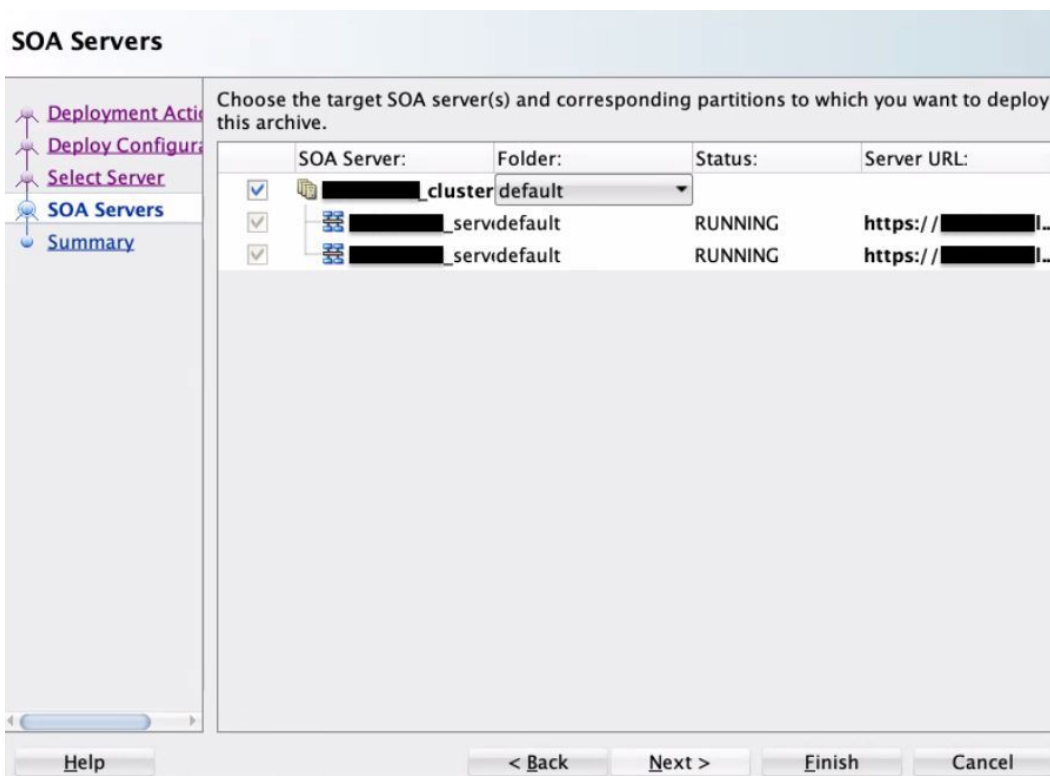


The deployment wizard is displayed.

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.

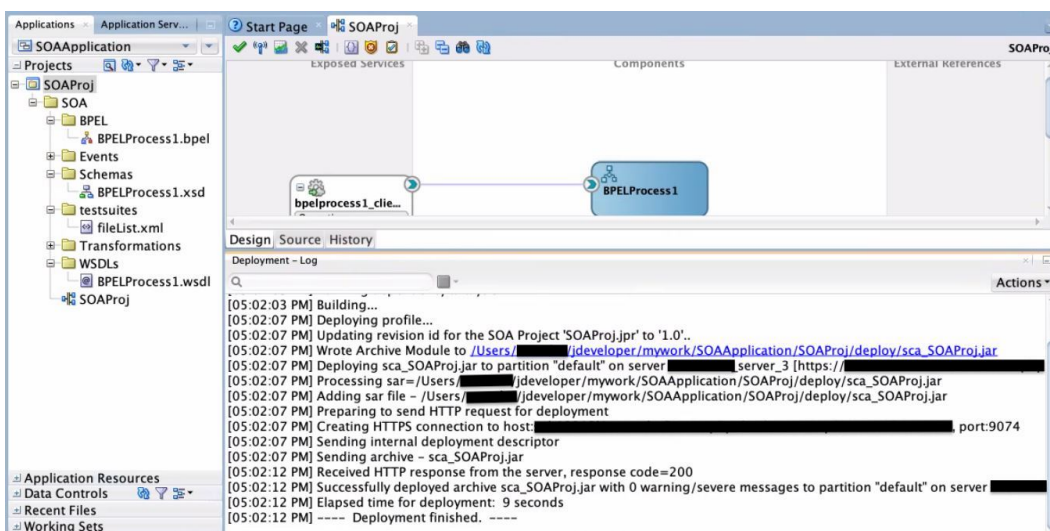




 **Note:**

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.



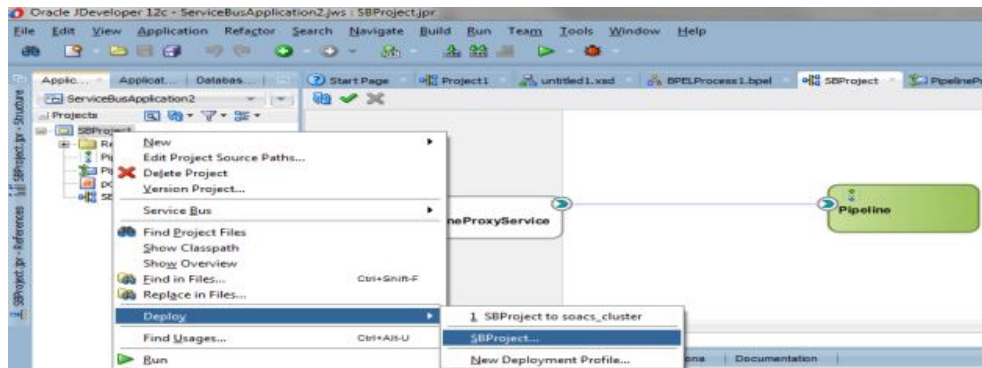
The JDeveloper Console logs indicate that the composite application was deployed successfully.

Deploy an Oracle Service Bus Application to Oracle SOA Cloud Service from JDeveloper

Oracle Service Bus applications are deployed to the Administration Server.

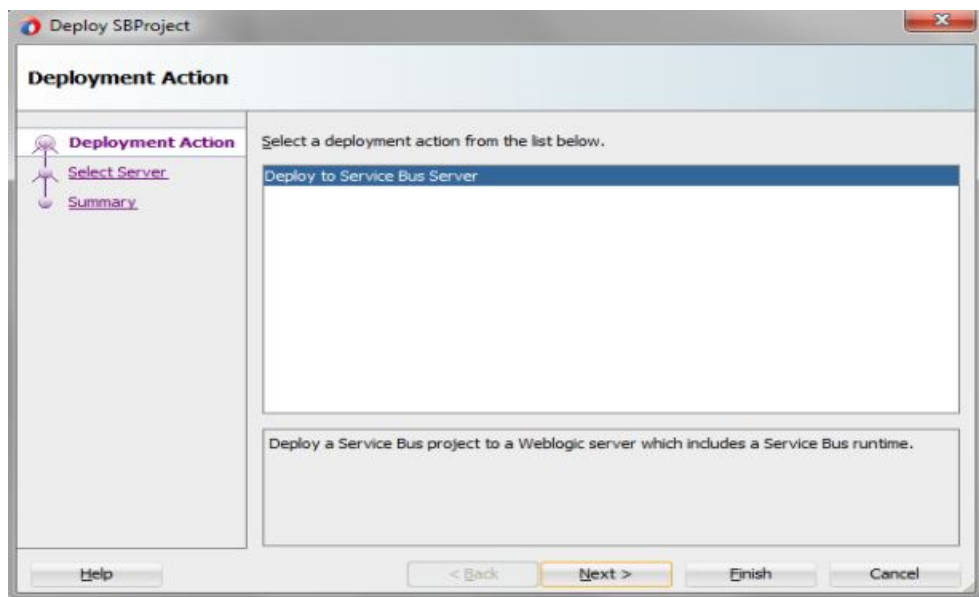
To deploy an Oracle Service Bus application to Oracle SOA Cloud Service from JDeveloper:

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

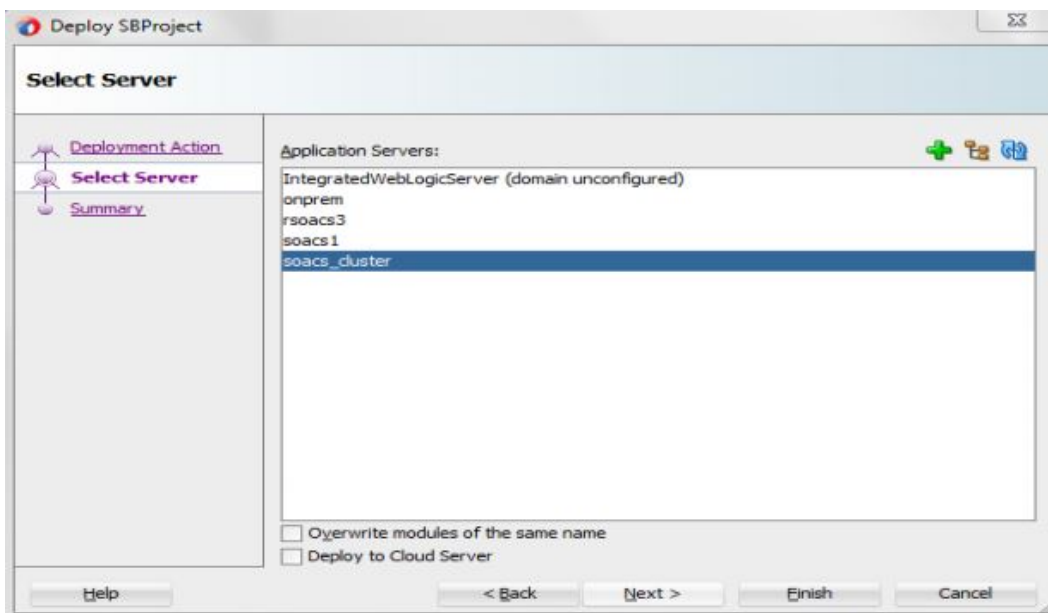


The deployment wizard is displayed.

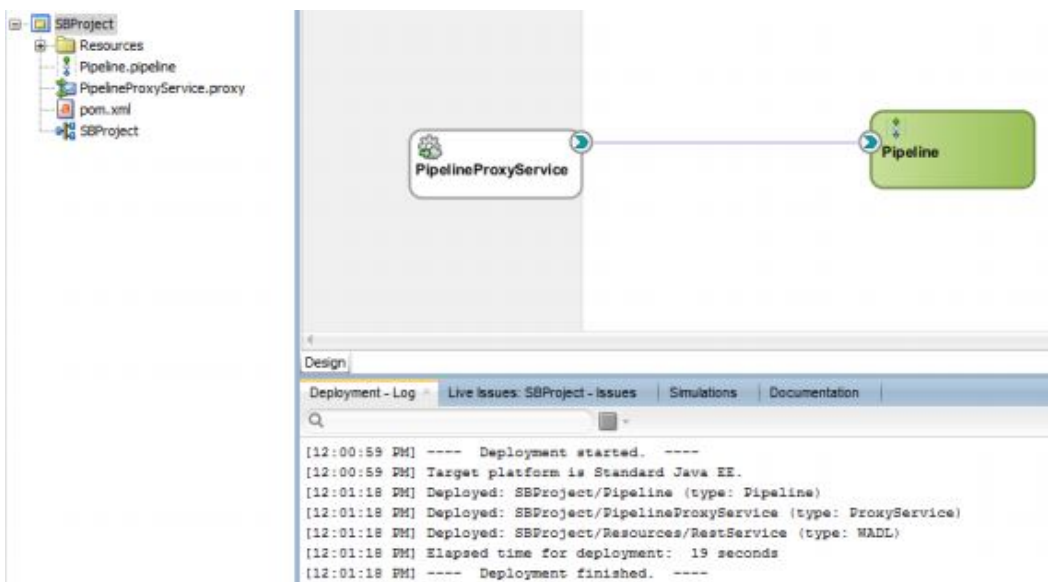
2. On the Deployment Action page, select **Deploy to Service Bus Server**.



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 Cloud Service 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](#).

Oracle Enterprise Manager Fusion Middleware Control is one of the consoles available through the Oracle SOA Cloud Service Console. For information about opening Oracle Enterprise Manager Fusion Middleware Control, see [Access an Administration Console for Software that a Service Instance Is Running](#).

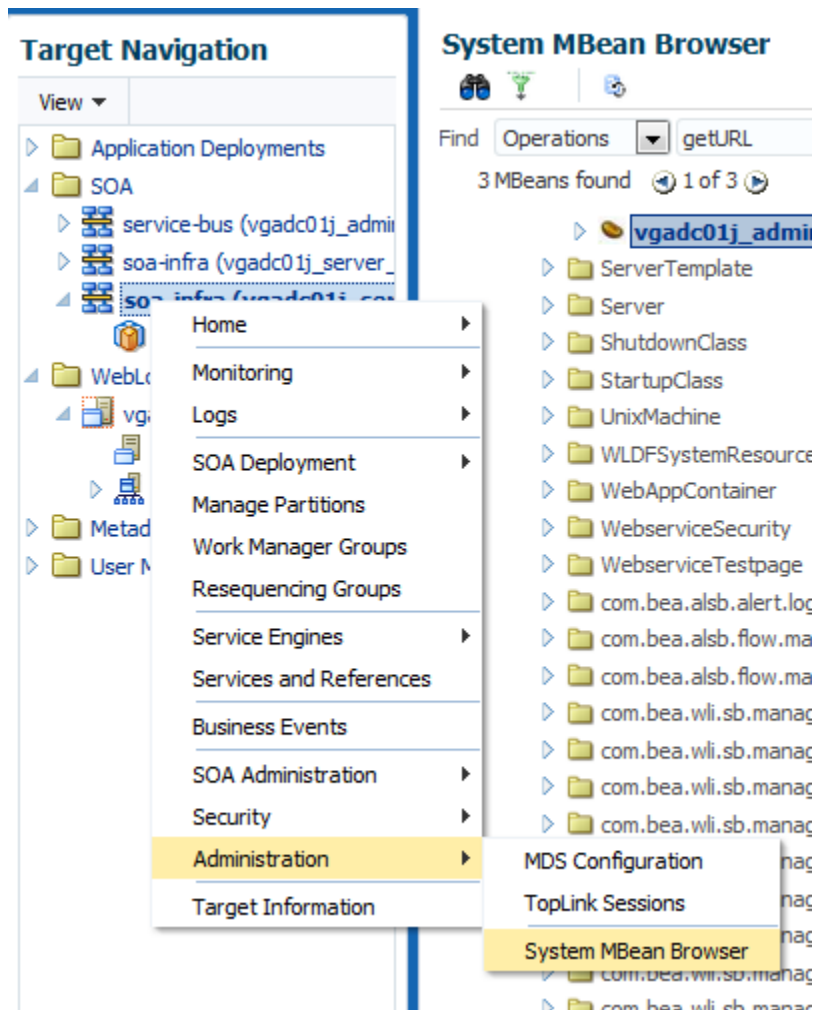
For additional resources, see "Deploying, Undeploying, and Redeploying SOA Composite Applications" in *Administering Oracle Fusion Middleware* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

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

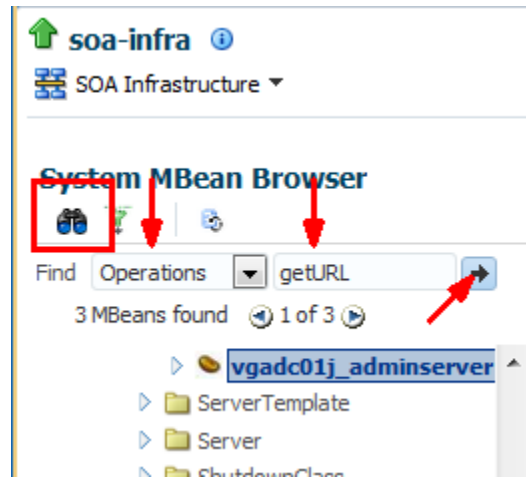
Before you can use Fusion Middleware Control to deploy applications, you must add a Managed Server IP in to a non-proxy host.

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

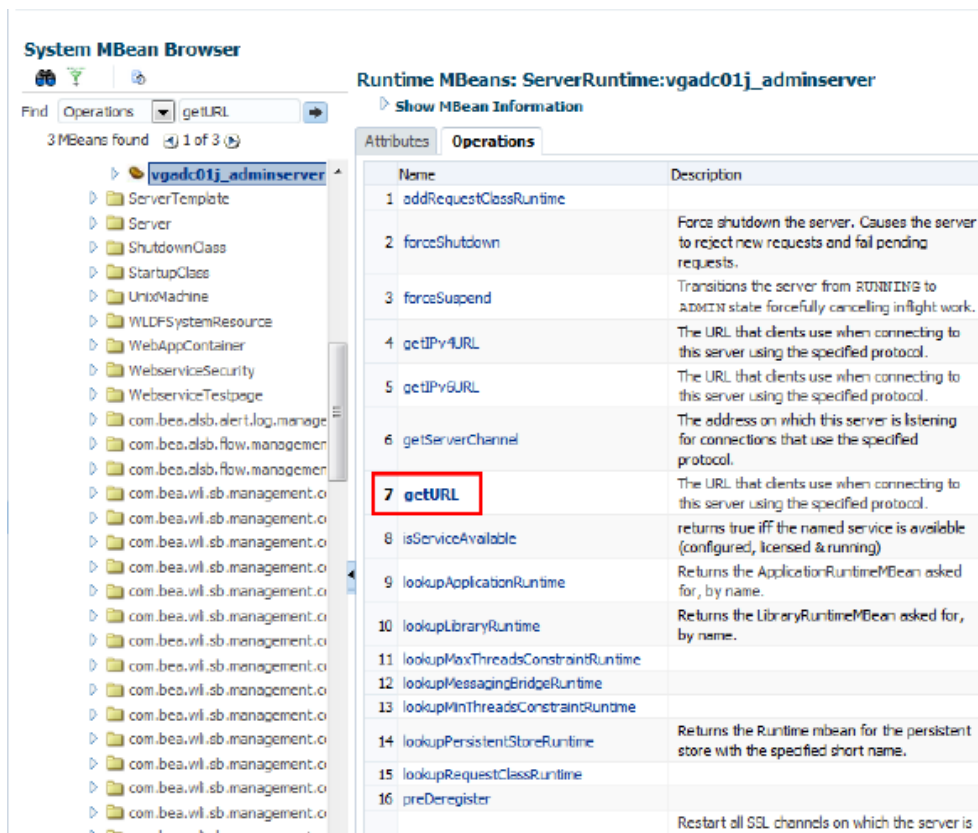
1. Log in to Fusion Middleware Control.
2. Find the server in the **Target Navigation** pane.
3. Right-click the server and select **Administration > System MBean Browser**.



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



5. Click **getURL**.



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

Operation: getURL

Information
The changes made on this screen 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.name-vgad01j_adminserver_Location-vgad01j_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 port 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 getURL 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	http

Return Value
http://vq3601gf8cc00b2n-813-jca-wls-Lopzbaa.oraclecloud.internal:7701

- Follow the instructions in "Configuring the Proxy Server for Runtime" in *Oracle Cloud Adapters Postinstallation Configuration Guide* (12.2.1.4 | 12.2.1.3 | 12.2.1.2 | 12.1.3) 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
```

- Restart the servers (both Administration Server and Managed Servers) for the settings to take effect.

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 Cloud Service instance, just as you would deploy and undeploy the application to an on-premises service instance.


The Oracle WebLogic Server Administration Console is one of the consoles available through the Oracle SOA Cloud Service Console. For information about opening the Oracle WebLogic Server Administration Console, see [Access an Administration Console for Software that a Service Instance Is Running](#).

Topics:

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


Use the WebLogic Server Administration Console to Deploy an Application

To deploy an application using the WebLogic Server Administration Console:

1. In the [Oracle SOA Cloud Service Console](#), click  for the service instance you want to start and select **Open 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, click the application.
5. Click **Start**, then **Servicing all requests**.
6. 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

To undeploy undeploy an application using the WebLogic Server Administration Console:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open 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 applications you want to remove, then click **Delete**.
5. Click **Yes** to confirm the delete request.
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 Cloud Service 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](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))
- *WLST Command Reference for SOA Suite* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#))


Access an Application Deployed to an Oracle SOA Cloud Service Instance

You can access an application deployed to an Oracle SOA Cloud Service instance through a URL in a browser.

To access a deployed application:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Service Bus Console**.
2. Sign in to the Oracle Server Bus Console
3. Copy the Host IP Address of the load balancer or Managed Server, depending on whether your Oracle SOA Cloud Service instance has a load balancer.
4. 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. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open WebLogic Server Administration Console**.
 - b. Sign in to the WebLogic Server Administration Console.
 - c. Select *domain* > **Deployments**, where *domain* is the domain where the application is deployed.
 - d. In the **Deployments** table, click on the name of your service.
The Settings dialog is displayed.
 - e. In the **Overview** tab, locate the context-root.
5. Open a browser and in the address bar, enter 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.

The default ports differ according to whether you created the service instance on which the application by using the service instance creation wizard accessible in the Oracle SOA Cloud Service Console REST API for Oracle SOA Cloud Service. The HTTP port is disabled if you created the service instance by using the service instance creation wizard.

See [About the Default Access Ports](#).

- 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).** Available on both Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic. A standard Oracle SOA Cloud Service or Managed File Transfer (MFT) Cloud Service 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.

- **File Storage Service (FSS).** Available on Oracle Cloud Infrastructure only. It can be used with Oracle SOA Cloud Service only, not with Managed File Transfer (MFT) Cloud Service. To use FSS, you must complete the following manual configuration tasks post-provisioning:

1. (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`
2. 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.

3. 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.

Use an OTD Host Name with an Oracle Service Bus Business Service

When configuring a business service URI in Oracle Service Bus, you must use the Oracle Traffic Director (OTD) host name, rather than the public IP address, if its metadata points to a service deployed on Oracle Weblogic Server in the same Oracle SOA Cloud Service environment.


For example:

- When using a proxy server in the Oracle Service Bus configuration, use the real host name and use port 80.
- Then the OTD host name is `http://xz-osbxy-drop5-1vm-20-jcs-1b-1:8080`

Connect to MFT Embedded Servers Using Oracle Traffic Director

To allow sFTP traffic from the public internet to MFT embedded sFTP servers, open the required port(s) using the PaaS Service Manager (PSM) user interface and configure the TCP proxy and origin-server pool in the load balancer, Oracle Traffic Director (OTD). For details, refer to "Managing TCP Proxies" in *Administering Oracle Traffic Director* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#)).

To connect to MFT embedded servers through OTD:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in to Console using your credentials .
2. On the upper left corner of the page, click the **OTD Domain** configurations button.


3. Click **Traffic Director**, and then select the **opc-config** option.
4. From the **Traffic Director Configuration** drop-down list, click **Administration**, and select **TCP Proxies**.
5. Click **Create** to create new TCP proxy.
6. In the **New TCP Proxy Wizard**, enter the following details:
 - a. **General** — Name: Enter a name for the proxy. Click **Next**.
 - b. **Listener** — Name: Name is entered by default. Enter port number 7522 for the listener. Enter a valid IP address for the listener. Click **Next**.
 - c. **Origin Server Pool** — Select the **Create a new pool of origin servers** radio button and enter the following information:
 - **Name**: Enter a name for the origin-server pool.
 - **Type**: TCP value is entered by default.
 - **Address Family**: Select the address family that the server in the origin-server pool uses to listen for requests.
 - **Add Server**: Click the + icon to add the server.
 - **Host**: Enter the WebLogic server host name in the origin-server pool.
 - **Port**: Enter the port number for the server in the origin-server pool.
7. Click **Next**. Review the information and then click **Create TCP Proxy**.
The TCP Proxy is created and automatically deployed.
8. Click **Close** to close the wizard.
9. Enter the following command to verify that you can connect to MFT embedded servers through OTD: balancer:

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

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. In the [Oracle SOA Cloud Service Console](#), click  for the instance in which the composite is running and select **Open WebLogic Server Console**
2. Get the IP address of the WebLogic Server Console from the browser URL field.
For example: 12.251.267.111
3. 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* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).
4. 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 in 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 Oracle WebLogic Server Administration Console:

```
https://hostname:7002/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.

Field	Value
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 servers to have the values take effect.

6

Administer Oracle SOA Cloud Service

Review the tasks for administering Oracle SOA Cloud Service.

Topics:

- [Administer the Load Balancer for an Oracle SOA Cloud Service Instance](#)
- [Access an Oracle SOA Cloud Service Instance After Provisioning](#)
- [Run WLST Commands on a VM](#)
- [Perform Lifecycle Operations on an Oracle SOA Cloud Service Instance](#)
- [Perform a JNDI Lookup of JMS Resources Deployed on the Administration Server](#)
- [Change JVM Heap Size Settings](#)
- [Perform Database Operations for an Oracle SOA Cloud Service Instance](#)
- [Change JVM Heap Size Settings](#)
- [Unmount and Mount DBFS](#)
- [Configure User Messaging Service on a Cluster](#)
- [Configure Mail Sessions](#)

Administer the Load Balancer for an Oracle SOA Cloud Service Instance

Oracle recommends configuring a load balancer when using a multinode cluster (such as production use cases). You can configure a load balancer during provisioning (see [Load Balancer Configuration](#)) or post-provisioning, as described in these topics.

Topics:

- (Oracle Cloud Infrastructure only) [Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning](#)
- (Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic) [Configure an Oracle Traffic Director Load Balancer During Provisioning or Post-Provisioning](#)

Note:

You can disable the load balancer to suspend the Oracle SOA Cloud Service instance temporarily, to block any new traffic from being delivered to the service instance. This is useful when you want to perform routine maintenance on an Oracle SOA Cloud Service instance, but do not want to stop the service instance. Once the maintenance activities have been completed, you can re-enable the load balancer to allow traffic to be delivered. See [Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance](#)

Configure an Oracle Cloud Infrastructure Load Balancer Post-Provisioning



This topic does not apply to Oracle Cloud Infrastructure Classic.

You can configure an Oracle Cloud Infrastructure load balancer for an Oracle SOA Cloud Service instance after provisioning the instance.

Usage Notes:

- You can configure an Oracle Cloud Infrastructure load balancer post-provisioning for an Oracle SOA Cloud Service instance of service types **SOA with SB & B2B Cluster** and **MFT Cluster**.
- If you are provisioning a new Oracle SOA Cloud Service instance, then select **None** for **Load Balancer** in the Create Instance Wizard.
- You can configure only one Oracle Cloud Infrastructure load balancer for one Oracle SOA Cloud Service instance.
- The Oracle Cloud Infrastructure load balancer should be created in custom compartment, not within `ManagedCompartmentForPaaS`.
- The Oracle Cloud Infrastructure load balancer has high availability (HA) features, spanned across different Availability Domains.
- Unlike OTD, the Oracle SOA Cloud Service Console does not show the Oracle Cloud Infrastructure load balancer on the instance details page.
- For existing Oracle SOA Cloud Service instances that use OTD:
 - If you have manually imported any certificates into Oracle Traffic Director (OTD), you must reimport these certificates into the new load balancer after it is created.
 - If provisioned with OTD, then ensure that OTD is in running state and then remove the OTD instance using REST API.
- After completing the steps to add an 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](#)), and you replaced the OTD load balancer with the Oracle Cloud Infrastructure load balancer, make sure your runtime URLs use the Oracle Cloud Infrastructure load balancer IP address instead of the OTD public 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 Cloud Service instance will not delete the Oracle Cloud Infrastructure load balancer. You must manually delete the load balancer from the Oracle Cloud Infrastructure Console.

- Do not invoke the **Add OTD component** operation from Oracle SOA Cloud Service Console. If you do so, OTD will override the Oracle Cloud Infrastructure load balancer configuration.

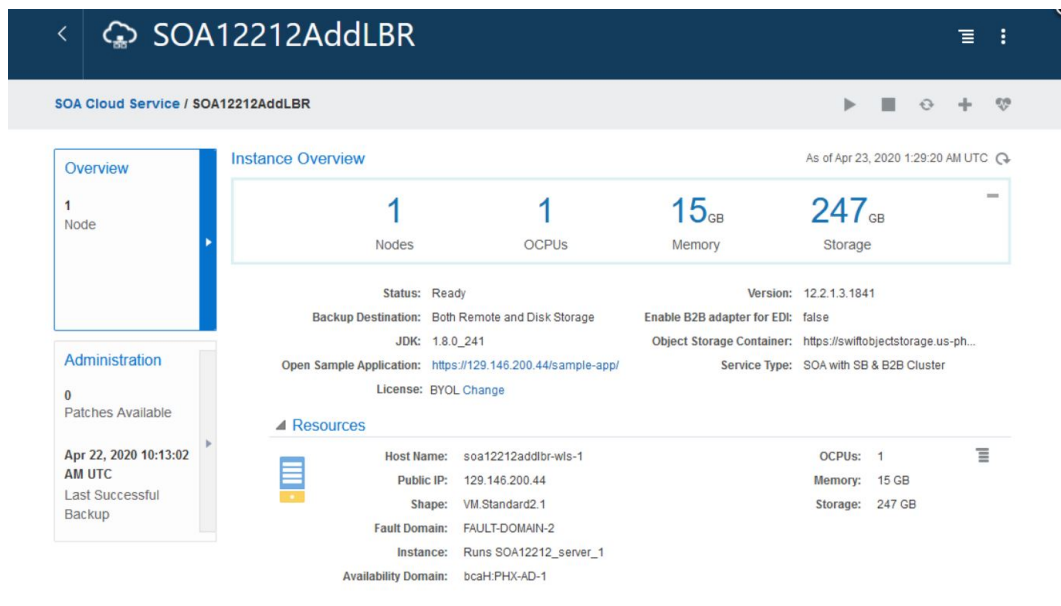
 **Note:**

This procedure uses the following example IP addresses:

- WebLogic Server Public IP: 129.146.200.44
- OTD Public IP if available: 129.213.147.163 (the steps below replace this OTD load balancer with the Oracle Cloud Infrastructure load balancer)
- Oracle Cloud Infrastructure load balancer Public IP: 129.146.91.95

To configure an Oracle Cloud Infrastructure load balancer post-provisioning:

1. As a prerequisite, create a database and create an Oracle SOA Cloud Service instance (without OTD) in Oracle Cloud Infrastructure regions.



The screenshot shows the Oracle SOA Cloud Service console interface. The main heading is "SOA12212AddLBR". Below the heading, there's a navigation bar with "SOA Cloud Service / SOA12212AddLBR". The main content area is titled "Instance Overview" and shows the following details:

- Overview:** 1 Node
- Instance Overview:** 1 Nodes, 1 OCPUs, 15 GB Memory, 247 GB Storage
- Status:** Ready
- Version:** 12.2.1.3.1841
- Backup Destination:** Both Remote and Disk Storage
- Enable B2B adapter for ED:** false
- JDK:** 1.8.0_241
- Object Storage Container:** https://swiftobjectstorage.us-ph...
- Open Sample Application:** https://129.146.200.44/sample-app/
- Service Type:** SOA with SB & B2B Cluster
- License:** BYOL Change
- Resources:**
 - Host Name: soa12212addlbr-wls-1
 - Public IP: 129.146.200.44
 - Shape: VM.Standard2.1
 - Fault Domain: FAULT-DOMAIN-2
 - Instance: Runs SOA12212_server_1
 - Availability Domain: bcaH.PHX-AD-1
 - OCPUs: 1
 - Memory: 15 GB
 - Storage: 247 GB

2. **Remove the OTD load balancer.** See [Remove the Oracle Traffic Director Load Balancer from an Oracle SOA Cloud Service Instance](#).
3. **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) []:SOAC5Dev
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.

```
/cygdrive/d/soacs/linux
vgorugan@vgorugan-lap1 /cygdrive/d/soacs/linux
$ cat mycert.key
-----BEGIN PRIVATE KEY-----
MIIEEwIBADANBgkqhkiG9w0BAQEFAASCBBKkwggS1AgEAAoIBAQL7Tch3kGRQ7cI
oon2zGdNhU+PVBBa28ynUFGp3oF/fNNKL1aXNdhT1T71AqMBjN4gk01Ybb/DYrWs
sxZ2o2Gcz1QcVetZ2WgHUWjbStTiqE3sR8R1nQMvFLBYypa/25no1iJrpsPQoX3h
NnBWA+gu/5c4R5J+Uoyh1HoW2xVu0wS9E3Nn19Sz+L14sCSd11G593VyF+tbwvTF
uDYkPVeIFZ8oiOIQWij0aMoiJnbZ01pKptGgXBN5rS2cFeasoKERd3+nQYhXumiJ
K5BObf1GcXbvvgBw02Uzthv7H5ZQgUrjF1/+XU+ItD31UU4jDU8CwtG5PUKWbydM
NMwc9WnXAgMBAECCggEAAxMEbcJIAsSekcb8hbL3K7gCwxwphZFjr80nPVtw/34gm
N0wXZhgtrXUS0eNRYy2HI+StP6SkYN/cacRg6Ba7F4/711t0uGIK/QYghXSt8gJ
xLIgSBWh4kN51RuHYkURQ01ZF334HcERGL+tWd6dNXgs83BAyR69eAIhBQ8wd4Tt
UwEom+IbEW1j5cULr7d9wpcE2ILs41JD0YFv1j20j61/Iz6VVC5zogTiwK9IFS39
b0vk0jN5JBiKJ9Z0f2uMMma/BbDtze5a7oDd9ghyEScfkOUs9Qu2DYswL.V9UZI61
tv3pBAPsFe19etqDw24qfjWZ3x0okKWcvcC8rVw04QKBgQD/IZeyRV0zK5xtvC9p
fDn5i01DzdpBaLiwZ6fEGqQSVuNrKct0afv0EFpQLPgMBtBegTSjnaf3yXMKCiqw
+40YEB47MRmdXe+TD/GTWm7ekCqFZhmK7GQjVXdfGXnpwMvE6ADUZHBPfHKjzQC
v31Jsq1EXHy1exj59euV47UyOwKBgQDMnvxfCIt8WJDUnjOoLSKy2Xmqgxt9D0U5
i38Fk5BA55d5AcD57hsvImcyikJRvgN11p3Di6UBto77ivmeab7cPiK03KsJmgm
MdgUE5dvSS50C06BGP8ufqt1R+wCpIr+WwFZ1BeYmh89akMR4Zz+/zu70RwF53wq
ZGm/hsExFQKBgQDjHx6SPxm3Ae3h6pMyjrp1okMIR2syq2d1nAFHnIfPI7au/1dE
25jInv4nPcEbw8Lo1ZEszp7HAXj2x1726x9AZ6dxxoMc6FhA+KE0Q695w1TcA8H
d9is3IVCBQoa7RzyfcXQRX9BzNbrQgyFHb8FKp1xE/yY+prDet9csjeOHQKBgQCe
AmeAi7gq3X15tnDNFY097xItLrNdb11VgpMkCz9ptWjIuD1y1o2j6j0aD8KA130V
gbsqFJmDVYdQoCrmXyrDIAnNq1ry9PwYcQwC+14FYcYIqH0E0/i6PrbIajGmGMn8
f6jdM67E+L8G/fes5zwe7b0C5YJ88B2B3uiKLDUhwQKBgQDknRfNn16a5QpDoSet
ytwd4Y3ZAimW7ZZtgwKm2/+N8dwYDxd10vhtFSZz03VYRhL8F7nze9CTtCQpfx7F
UVomfKk43W1nGdQ+FekF9nqaByInR+6s+Mb7pAxxv9aJQ2e/OeffY4qToBNWvE
K708IGoeVQS6IQXnzP2X2kHvdA==
-----END PRIVATE KEY-----
```

- 4. In the Oracle Cloud Infrastructure Console, create a load balancer:
 - a. Sign in to your Oracle Cloud Service account and navigate to the Oracle Cloud Infrastructure Console.

See Signing in to Your Cloud Account in *Getting Started with Oracle Cloud*.

- b. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
- c. In the left pane, click **Load Balancers**.
- d. Scroll down in the left pane and select the same compartment as your Oracle SOA Cloud Service instance uses.
- e. Click **Create Load Balancer**.
- f. In the Select Load Balancer Type dialog, click **Create Load Balancer**.
- g. In the Create Load Balancer wizard, on the **Add Details** page:
 - **Load Balancer Name:** Enter a name for the load balancer.
 - **Virtual Cloud Network in *compartment*:** Select the same VCN used by your Oracle SOA Cloud Service instance.
 - **Subnet in *compartment*:** Select subnet(s).
 - Click **Show Advanced Options**, and on the **Management** tab, select the same compartment used by your Oracle SOA Cloud Service instance.

Create Load Balancer

1 Add Details
2 Choose Backends
3 Configure Listener

A load balancer provides automated traffic distribution from one entry point to multiple servers in a backend set. The load balancer ensures that your services remain available by directing traffic only to healthy servers in the backend set.

LOAD BALANCER NAME
SOACLBEVQ

CHOOSE VISIBILITY TYPE

Public Private
 You can use the assigned public IP address as a front end for incoming traffic. You can use the assigned private IP address as a front end for internal incoming VCN traffic.

CHOOSE THE MAXIMUM TOTAL BANDWIDTH

Small 100 Mbps Medium 400 Mbps Large 8000 Mbps

CHOOSE NETWORKING

VIRTUAL CLOUD NETWORK IN TELECOMPARTMENT [\[choose compartment\]](#)
testvcn

To create a public load balancer, specify a single regional subnet (recommended), or two availability domain-specific subnets in different availability domains.

SUBNET 1 OF 2 IN TELECOMPARTMENT [\[choose compartment\]](#)
Public Subnet boah-PH1-AD-1

SUBNET 2 OF 2 IN TELECOMPARTMENT [\[choose compartment\]](#)
Public Subnet boah-PH1-AD-2

USE NETWORK SECURITY GROUPS TO CONTROL TRAFFIC

[Hide Advanced Options](#)

Management Tagging

CREATE IN COMPARTMENT
TestCompartment
ocsaas1 boah/TestCompartment

- h. Click **Next**.
- i. On the **Choose Backends** page:
 - **Port:** Enter 9073.
 - **Status Code:** Enter 404.
 - Click **Show Advanced Options**, and set **BACKEND SET NAME** to httpBackend.

Create Load Balancer

Add Details
 Choose Backends
 Configure Listener

A load balancer distributes traffic to backend servers within a backend set. A backend set is a logical entity defined by a load balancing policy, a health check policy, and a list of backend servers (Compute instances).

SPECIFY A LOAD-BALANCING POLICY

Weighted Round Robin
 This policy distributes incoming traffic sequentially to each server in a backend set list.

IP Hash
 This policy ensures that requests from a particular client are always directed to the same backend server.

Least Connections
 This policy routes incoming request traffic to the backend server with the fewest active connections.

SELECT BACKEND SERVERS OPTIONAL

No backend servers selected. Click **Add Backends** to select resources from a list of available Compute instances. You can choose instances from one compartment at a time. After you add instances from one compartment, you can choose **Add More Backends** to add instances from another compartment. You can also add backend servers after you create the load balancer.

Add Backends

SPECIFY HEALTH-CHECK POLICY

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers.

PROTOCOL: HTTP

PORT OPTIONAL: 8073

INTERVAL IN MS OPTIONAL: 100000

TIMEOUT IN MS OPTIONAL: 3000

NUMBER OF RETRIES OPTIONAL: 3

STATUS CODE OPTIONAL: 404

URL PATH (URI): /

RESPONSE BODY RESEX OPTIONAL:

[Hide Advanced Options](#)

Backend Set Name: Security List Session Persistence

BACKEND SET NAME: httpBackend

- j. Click **Next**.
- k. On the **Configure Listener** page:
- **Listener Name:** Enter `httpsListener`.
 - **Specify the type of traffic your listener handles:** Select **HTTPS**.
 - **Specify the port your listener monitors for ingress traffic:** Enter `443`.
 - Import the `mycert` certificate and key as follows:
 - Select **Choose SSL Certificate File**, and add `mycert.crt`.
 - Select **Specify Private Key**, and add `mycert.key`.

Create Load Balancer

Add Details
 Choose Backends
 Configure Listener

A listener is a logical entity that checks for incoming traffic on the load balancer's IP address. To handle TCP, HTTP and HTTPS traffic, you must configure at least one listener per traffic type. You can configure additional listeners after you create your load balancer.

LISTENER NAME: httpsListener

SPECIFY THE TYPE OF TRAFFIC YOUR LISTENER HANDLES

HTTPS
 HTTP
 TCP

SPECIFY THE PORT YOUR LISTENER MONITORS FOR INGRESS TRAFFIC

443

CHOOSE SSL CERTIFICATE FILE PASTE SSL CERTIFICATE
SSL CERTIFICATE
 Drop a file or [select one](#)
Certificate must be in PEM format and must be signed. File extension must be .pem, .cer, or .crt.

mycert.crt

SPECIFY CA CERTIFICATE
 CHOOSE CA CERTIFICATE FILE PASTE CA CERTIFICATE
CA CERTIFICATE
 Drop a file or [select one](#)
Certificate must be in PEM format and must be signed. File extension must be .pem, .cer, or .crt.

CertGenCA.pem

SPECIFY PRIVATE KEY
 CHOOSE PRIVATE KEY FILE PASTE PRIVATE KEY
PRIVATE KEY
 Drop a file or [select one](#)
Private Key must be in PEM format. File extension must be .pem or .key.

mycert.key

ENTER PRIVATE KEY PASSPHRASE OPTIONAL:

You can configure path route rules and custom header rule sets after you create the load balancer. For more information, see [Managing Request Routing](#) and [Managing Rule Sets](#).

[Show Advanced Options](#)

5. Once the Oracle Cloud Infrastructure load balancer is created, note that the **Overall Health** and **Backend Sets Health** shows a status of **Unknown**. To resolve this, continue with the steps below.

The screenshot displays the 'Load Balancer Details' page for a resource named 'SOACSVGLB'. On the left, there is a green hexagonal icon with 'LB' and the word 'ACTIVE' below it. The main content area is divided into sections: 'Load Balancer Information' (including OCID, creation time, shape, IP address, and subnets), 'Overall Health' (showing 'Unknown'), and 'Backend Sets Health' (showing 'Unknown'). Below these is a 'Resources' sidebar and a '10 Metrics' section with a graph area that currently shows 'No data for this time range'.

Note:

6. **Add backends:**
 - a. In the left pane of the Load Balancer Details page, click **Backend Sets**, then click the link to the `httpBackend` backend set.
 - b. In the left pane of the Backend Set Details page, click **Backends**, then click **Add Backends**.
 - c. In the Add Backends dialog, click `CHANGE COMPARTMENT` to select the compartment for your Oracle SOA Cloud Service instance if not already displayed, then select the checkbox next to the instance name, and enter a **Port** value of `9073`.

The 'Add Backends' dialog allows users to choose between adding compute instances or IP addresses. It specifies the compartment as 'INSTANCES IN MOCKMANAGEDCOMPARTMENTSOA'. A table lists several instances, with the one 'SOA|SOA12214AddLBRVG|wls|vm-1' selected. The port for this instance is set to 9073.

<input type="checkbox"/>	Name	IP Address	OCID	Availability Domain	Port	Weight
<input type="checkbox"/>	500104469 dbaas dbaasOCIO308 db_1 vm-1	10.0.0.48	...s4ekiq Show Copy	bcaH:PHX-AD-1	80	1
<input checked="" type="checkbox"/>	SOA SOA12214AddLBRVG wls vm-1	10.0.0.150	...7swr2a Show Copy	bcaH:PHX-AD-1	9073	1
<input type="checkbox"/>	SOA SOA12214AddLBRVG wls vm-2	10.0.0.152	...ynmpa Show Copy	bcaH:PHX-AD-1	80	1
<input type="checkbox"/>	SOA SOA12214AtpStress10 l vm-1	10.0.0.147	...s3pdvq Show Copy	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](#)

7. Add a rule set:

- a. In the left pane of the Load Balancer Details page, 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

8. Edit the listener:

- a. In the left pane of the Load Balancer Details page, 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 page, 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 *****.

Edit Backend Set

[Help](#)

USE SSL

Session Persistence

To enable cookie-based session persistence, specify whether the cookie is generated by your application server or by the load balancer. Learn more about [session persistence](#).

DISABLE SESSION PERSISTENCE
 ENABLE APPLICATION COOKIE PERSISTENCE
 ENABLE LOAD BALANCER COOKIE PERSISTENCE

COOKIE NAME

Specify "*" to match any cookie name.

DISABLE FALLBACK
Disable fallback to other servers when the original server is unavailable.

[Update Backend Set](#) [Cancel](#)

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 Cloud Service that require you to import SSL certificates into the Oracle Cloud Infrastructure load balancer, import them now.

11. Update front end hosts:

- a. Sign 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.

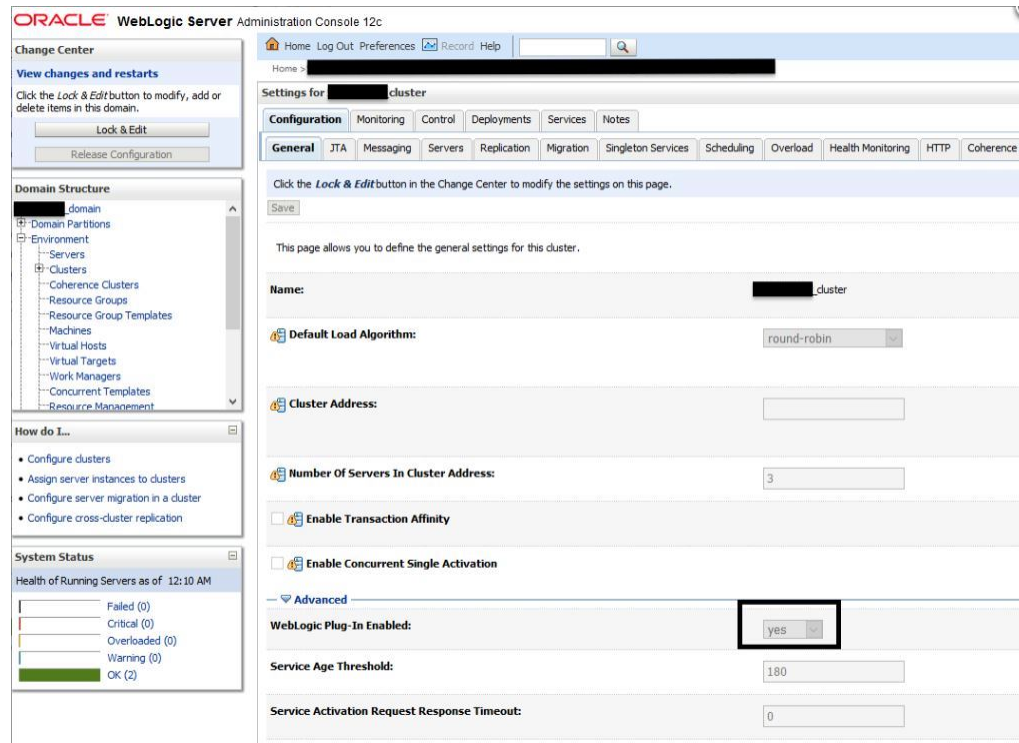
The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for [redacted] cluster" and is under the "Configuration" tab. The "HTTP" sub-tab is selected. The page contains the following configuration fields:

- Frontend Host:** 129.146.91.95
- Frontend HTTP Port:** 0
- Frontend HTTPS Port:** 443

There are "Save" buttons below the configuration fields and a "Lock & Edit" button in the Change Center on the left. A message at the top states: "All changes have been activated. However 1 items must be restarted for the changes to take effect."

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

- a. Sign 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:

From the [Oracle SOA Cloud Service Console](#), restart the Administration Server and Managed Servers. See [Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs](#).

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**.

The screenshot shows the Oracle Cloud Infrastructure console for a Load Balancer named SOACSVGLB. The console is divided into several sections:

- Load Balancer Information:** Shows the load balancer is in an 'ACTIVE' state. It provides details such as OCID, creation time (Sat, May 2, 2020, 24:14:17 UTC), shape (100Mbps), IP address (129.146.91.95), virtual cloud network, and subnets.
- Overall Health:** Indicated as 'OK' with a green checkmark.
- Backend Sets Health:** Shows three backend sets, all with a status of 'OK' (1 OK, 0 Warning, 0 Critical).
- Resources:** Lists various resources associated with the load balancer, including Backend Sets (1), Path Route Sets (0), Rule Sets (0), Listeners (1), Hostnames (0), and Certificates (1).
- 10 Metrics:** A section for monitoring metrics. It shows a table for 'Inbound Requests' with columns for name, count, and status. The table is currently empty, with a note 'No data for this time range'.

- Verify the URLs: you should be able to access the following Managed Server URLs using the Oracle Cloud Infrastructure load balancer IP address (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.
 - 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.

Configure an Oracle Traffic Director Load Balancer During Provisioning or Post-Provisioning

You can add, delete, or modify Oracle Traffic Director (OTD) as a load balancer for an Oracle SOA Cloud Service instance during provisioning or after provisioning the instance.

Topics:

- [About Oracle Traffic Director Load Balancer Virtual Machines](#)
- [Add an Oracle Traffic Director Load Balancer to an Oracle SOA Cloud Service Instance Post-Provisioning](#)
- [Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance](#)
- [Remove the Oracle Traffic Director Load Balancer from an Oracle SOA Cloud Service Instance](#)

About Oracle Traffic Director Load Balancer Virtual Machines

If an Oracle Traffic Director (OTD) load balancer is enabled for an Oracle SOA Cloud Service instance, the OTD Administration Server is hosted on one virtual machine (VM).

The following table lists the file paths found on the OTD load balancer VM:

Name	Path	Description
JAVA_HOME	/u01/jdk	Java installation
ORACLE_HOME	/u01/app/oracle/middleware/otd	Oracle Traffic Director installation
DOMAIN_HOME	/u01/data/otd-instance/otd_domain	Oracle WebLogic Server domain that is used to manage and monitor Oracle Traffic Director

Add an Oracle Traffic Director Load Balancer to an Oracle SOA Cloud Service Instance Post-Provisioning

You can add an Oracle Traffic Director (OTD) load balancer to an Oracle SOA Cloud Service instance during provisioning (see [Provision an Oracle SOA Cloud Service Instance](#)) or after provisioning, as described here.



Note:


You can only add one OTD load balancer. If your instance is already front ended with a load balancer, you cannot add a second load balancer.

For any Oracle SOA Cloud Service instance that contains more than one Managed Server node, a load balancer provides these benefits:

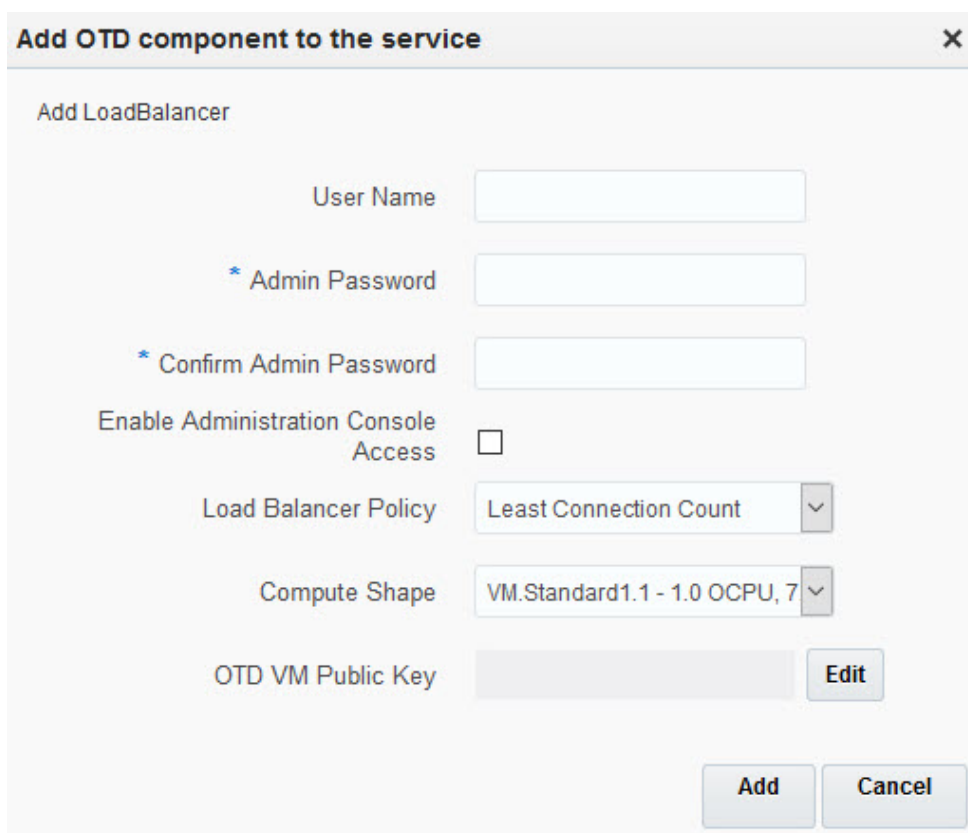
- Manages the routing of requests across all Managed Servers.
- Enables you to configure the routing policy.
- Enables you to suspend a service instance temporarily to perform routine maintenance, as described in [Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance](#).

A service instance can include zero or one load balancer nodes (VMs). Each node is assigned a separate public IP address.

To add a load balancer to an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance with the cluster that you want to scale out.
2. On the Overview page, click  (in the header) and select **Add OTD component to the service**.

The Add OTD component to the service dialog is displayed.



Add OTD component to the service ✕

Add LoadBalancer

User Name

* Admin Password

* Confirm Admin Password

Enable Administration Console Access

Load Balancer Policy ▼

Compute Shape ▼

OTD VM Public Key

3. Provide values for the load balancer.

The user name and password for the Oracle Traffic Director administrator are used to access the Oracle Traffic Director administration console as described in [Access an Administration Console for Software that a Service Instance Is Running](#).

 **Note:**

If you add a load balancer to an Oracle SOA Cloud Service instance after the service instance was created, you must define the user name and password for the Oracle Traffic Director administrator explicitly. The user name and password are **not** set by default to the user name of the WebLogic Server administrator. This behavior differs from the behavior when a load balancer is added to a service instance while the service instance is being created.

Option	Description
User Name	<p>The name must be between 8 and 128 characters long and cannot contain any of the following characters:</p> <ul style="list-style-type: none"> • Tab • Brackets • Parentheses • These special characters: <ul style="list-style-type: none"> – Left angle bracket (<) – Right angle bracket (>) – Ampersand (&) – Pound sign (#) – Pipe symbol () – Question mark (?)
Admin Password	<p>The password must meet these requirements:</p> <ul style="list-style-type: none"> • Starts with a letter • Is between 8 and 30 characters long • Contains letters, at least one number, and, optionally, any number of these special characters: <ul style="list-style-type: none"> – Dollar sign (\$) – Pound sign (#) – Underscore (_) <p>No other special characters are allowed.</p>

Option	Description
Load Balancer Policy	<p>Select the policy to use for routing requests to the load balancer.</p> <p>Valid policies include:</p> <ul style="list-style-type: none"> • Least Connection Count—Passes each new request to the Managed Server with the least number of connections. This policy is useful for smoothing distribution when Managed Servers get bogged down. Managed Servers with greater processing power to handle requests will receive more connections over time. • Least Response Time—Passes each new request to the Managed Server with the fastest response time. This policy is useful when Managed Servers are distributed across networks. • Round Robin—Passes each new request to the next Managed Server in line, evenly distributing requests across all Managed Servers regardless of the number of connections or response time.
Compute Shape	<p>Select the number of Oracle Compute Units (OCPU) and amount of RAM memory that you want to allocate to the VM for the load balancer. The larger the compute shape, the greater the processing power.</p> <p>The valid compute shapes for Oracle Cloud Infrastructure are:</p> <ul style="list-style-type: none"> • VM.Standard1.2 • VM.Standard1.4 • VM.Standard1.8 • VM.Standard1.16 • BM.Standard1.36 <p>The valid compute shapes for Oracle Cloud Infrastructure Classic are:</p> <ul style="list-style-type: none"> • OC1M: 1 OCPU and 15 GB memory • OC2M: 2 OCPUs and 30 GB memory • OC3M: 4 OCPUs and 60 GB memory • OC4M: 8 OCPUs and 120 GB memory <p>Note that you cannot change the compute shape after you have created the Oracle SOA Cloud Service instance.</p>

Option	Description
OTD VM Public Key	<p>Specify the value of the VM Public Key, or the name of the file that contains the public key value to use when connecting to the OTD server.</p> <p>Define the public key for the secure shell (SSH). This key is used for authentication when connecting to the Oracle SOA Cloud Service instance using an SSH client.</p> <p>Click Edit to display the public key input for VM access and specify the public key using one of the following methods:</p> <ul style="list-style-type: none"> • Select Key File Name and click Browse to select a file that contains the public key for the secure shell (SSH). • Select Key Value and paste or type a key value in the text box. • Select Create a New Key and click Enter. The Provisioning Wizard generates a key for you. When prompted, save it as a file on your hard drive. Select Key File Name and click Browse to select the file.

4. Click **Add Load Balancer**.

The Overview page is updated to show that the load balancer is being added. While the load balancer is being added, the service instance is in maintenance status and you cannot start any other management operation on the service instance.


After the load balancer is added, information about the load balancer is also available on the Load Balancer tab on the Administration page.

If you require the WebLogic Plug-in Enabled control to be set in Oracle WebLogic Server, you must set this control manually. If you add a load balancer to an Oracle SOA Cloud Service instance after the service instance was created, Oracle SOA Cloud Service does **not** set the WebLogic Plug-in Enabled control in Oracle WebLogic Server for you. This behavior differs from the behavior when a load balancer is added to a service instance while the service instance is being created.

For details, see [Understanding the use of "WebLogic Plugin Enabled"](#).

Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance

Oracle SOA Cloud Service does not provide any interfaces for controlling configuring the OTD load balancer for an Oracle SOA Cloud Service instance. Instead, you use the Oracle Traffic Director administration console to configure the load balancer.

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in to Console using the credentials defined when provisioning your service instance.
2. For service instances running Oracle Traffic Director 12c refer to topics in *Administering Oracle Traffic Director*:
 - Features of Oracle Traffic Director
 - Overview of Administration Tasks

For information about the topology of OTD instances in an Oracle SOA Cloud Service instance, see About the Deployment Topology in *Using Oracle Java Cloud Service*.

Remove the Oracle Traffic Director Load Balancer from an Oracle SOA Cloud Service Instance

You can remove the Oracle Traffic Director (OTD) load balancer from an Oracle SOA Cloud Service instance.

Usage Notes:

- If you have manually imported any certificates into OTD, you must reimport these certificates into the Managed Server or other load balancer (if you are configuring a new load balancer).
- Ensure that OTD is in running state before removing it using REST API.
- After removing OTD:
 - If you are not using a DNS name and using an OTD IP address (see [Register a Custom Domain Name with a Third-Party Registration Vendor](#)) and you removed OTD load balancer, make sure your runtime URLs are using the Administration Server IP address instead of the OTD IP address.
 - URLs for all Managed Servers such as b2bconsole, mftconsole, and composer should be accessible using the Administration Server IP address instead of the OTD IP address.
 - If you are using multinode cluster, then all incoming traffic will be routed to Managed Server1 only.
 - Optionally, you can add Oracle Cloud Infrastructure load balancer.


To remove the OTD load balancer:

1. From a Linux VM, run the following REST API command:

```
curl -i --user "user:password"
  -X PUT -H "X-ID-TENANT-NAME:identity-domain"
  -H "Content-Type:application/
vnd.com.oracle.oraclecloud.provisioning.Service+json" -d "{}"
  https://rest_server_url:/paas/api/v1.1/instancemgmt/identity-
domain/services/SOA/instances/servicename/servicecomponent
```

Example:

```
curl -i --user "myservicesusername:myservicespassword"
  -X PUT -H "X-ID-TENANT-
NAME:idcs-829b09c9d34b49be834e824ns810001"
  -H "Content-Type:application/
vnd.com.oracle.oraclecloud.provisioning.Service+json" -d "{}"
  https://psm.us.oraclecloud.com/paas/api/v1.1/instancemgmt/
idcs-829b09c9d34b49be834e824ns810001/services/SOA/instances/SOAtest/
servicecomponent
```

2. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open WebLogic Server Administration Console**.
3. In the Change Center, click **Lock & Edit**.

4. In the **Domain Structure** pane, expand the **Environment** node, then **Clusters**, and click the cluster name.
5. On the **Configuration: http** tab, set **Frontend Host** to an empty value (if not already done) and set **Frontend HTTP Port** to 0.
6. On the **Configuration: General** tab, scroll down to the **Advanced** section and expand it.
7. Set **WebLogic Plug-In Enabled** to **Yes**.
8. Click **Save** and activate the changes.
9. Restart the Oracle SOA Cloud Service instance from the Oracle SOA Cloud Service Console.
10. Verify the URLs by accessing the following Managed Server URLs using the Administration Server 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`

Access an Oracle SOA Cloud Service Instance After Provisioning

Topics:


- [Access an Administration Console for Software that a Service Instance Is Running](#)
- [Access a VM Through a Secure Shell \(SSH\)](#)
- [Access a VM Through Virtual Network Computing \(VNC\)](#)
- [Access a VM Through PuTTY](#)

Access an Administration Console for Software that a Service Instance Is Running

From an Oracle SOA Cloud Service instance, you can access the administration consoles for the software that the service instance is running.

You can access these consoles:

- WebLogic Server Console
- Fusion Middleware Control
- Load Balancer Console
- Oracle Service Bus Console
- Managed File Transfer Console
- B2B Console
- Worklist Application
- BAM Composer

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select the command to open the console that you want to access.
A new browser opens and you are redirected to the selected console's login page. If the server is protected with a self-signed certificate, you are warned that this certificate is not trusted.
2. Accept the certificate.
For example, if you are using Firefox, select **I Understand the Risk**.
3. Follow the remaining browser-dependent steps to accept the certificate.
For example, if you are using Firefox, the Add Security Exception dialog appears and you would select **Confirm Security Exception**.
4. When the console login page appears, enter the log-in credentials you entered for WebLogic Administrator when you created the service instance.

Access a VM Through a Secure Shell (SSH)

You can access the services and resources that an Oracle SOA Cloud Service instance's VM provides by logging into the VM as the `opc` user through SSH. You can use any SSH utility you want. For example, if you are using Windows, you might use PuTTY; if you are using Linux, you might use OpenSSH.

Notes:

- Only the `opc` user can remotely connect to your VMs. You cannot use SSH to connect to a VM as the `oracle` user. After successfully connecting to a VM, tasks such as starting and stopping the server and accessing the administrative logs should only be performed by the `oracle` user.
- Oracle pushes regular OPC/PSM related updates to the VMs to support interaction between the Oracle Cloud Portal and the VMs silently. Oracle does not send notifications of these updates as they only affect Oracle owned files and scripts that should not be modified, and the updates do not require any down-time either.
- VM start and stop is controlled by SSH access. SSH access is not allowed when Oracle SOA Cloud Service quota reaches the limit. When you try to access SSH a quota limit message is displayed.

Topics:

- [Connect to the Administration Server or Load Balancer VM](#)
- [Connect to a Managed Server VM](#)
- [Create an SSH Tunnel](#)
- [Switch VM Users](#)
- [Add an SSH Public Key](#)

Connect to the Administration Server or Load Balancer VM

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

To access a VM through SSH:

1. In the [Oracle SOA Cloud Service Console](#), click the service instance associated with the VM you want to access.

The Oracle SOA Cloud Service instance page is displayed with the Overview tile in focus, displaying detailed information about the service instance.

2. From the list of virtual machines, note the **Public IP** address of the Administration Server or the load balancer, depending on which VM you want to access.

This address will be specified in the typical octet format (111.111.111.111).

 **Note:**

The console displays public IP addresses only for the Administration Server and the load balancer VMs, not for the Managed Server VMs. For more information, see [Connect to a Managed Server VM](#).

3. 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
```

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

To download PuTTY, go to <http://www.putty.org/>.

- 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.
5. 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. In the [Oracle SOA Cloud Service Console](#), click the service instance associated with the VM you want to access.

The Oracle SOA Cloud Service Instance page is displayed with the Overview tile in focus, displaying detailed information about the service instance.

2. From the list of virtual machines, identify the following information:
 - The **Public IP** address of the Administration Server VM (used as the proxy).
 - The **Host** name of the Managed Server VM to which you want to connect.

3. 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
```

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

To download PuTTY, go to <http://www.putty.org/> and click the **You can download PuTTY here** link.

- 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 Cloud Service 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 Cloud Service instance as an alternative to creating an SSH tunnel. However, use caution and consider possible security implications before opening up ports to external access. For more information, see [Manage Access Rules for an Oracle SOA Cloud Service Instance](#).

If a resource provided by a VM uses a port that is not directly accessible through the Internet, you can access that resource by creating an SSH tunnel to the port. For example, you can use an SSH tunnel to connect a local Integrated Development

Environment (IDE) such as Eclipse to the dedicated deployment port (9001) of the Administration Server.

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

Tutorial

To set up an SSH tunnel to a VM:

1. In the [Oracle SOA Cloud Service Console](#), click the service instance associated with the VM you want to access.

The Oracle SOA Cloud Service Instance Overview page is displayed.

2. From the list of virtual machines, note the **Public IP** address of the Administration Server or the Load Balancer, depending on which VM you want to access.

This address will be specified in the typical octet format (111.111.111.111).

Note:

The console displays public IP addresses only for the Administration Server and the Load Balancer VMs, not for the managed server VMs. For more information, see [Connect to a Managed Server VM](#).

3. 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 through 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
```

4. 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**.

5. 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.

Switch VM Users

You can change users on an Oracle SOA Cloud Service VM in order to perform specific administration tasks.

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

```
sudo useradd myuser
```



Note:

There is no default password for the `opc` user.

Switching to the `oracle` User

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.

Enter the following to become the `oracle` user:

```
sudo su - oracle
```



Note:

There is no default password for the `oracle` user.

Switching to the `root` User

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

Enter the following to become the `root` user:

```
sudo -s
```



Note:

Avoid using the `root` user except to perform privileged OS administration tasks.


Add an SSH Public Key

You can add secure shell (SSH) public keys to an Oracle SOA Cloud Service instance.

You might need to add a new SSH public key to an Oracle SOA Cloud Service instance if the SSH private key that you use to access the service instance becomes lost or corrupted. Or, you might need to comply with your organization's security policies or regulations.

To generate an SSH key pair, see [Generate a Secure Shell \(SSH\) Public/Private Key Pair](#).

To add an SSH public key:

1. In the [Oracle SOA Cloud Service Console](#), click  for the instance to which you want to add a new SSH public key and select **Add SSH Access**.
A dialog displays the value of the most recently added public key.
2. Specify the new public key by completing one of the following:
 - Select **Upload a new SSH Public Key value from file** and then use your browser to upload a public key file from your local computer.
 - Select **Key Value**. Delete the previous public key value from the input field and then enter or paste the new value. Be sure not to include other characters that aren't part of the key, such as spaces.
3. Click **Add New Key**.

Access a VM Through Virtual Network Computing (VNC)

You can access the services and resources that an Oracle SOA Cloud Service 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 a Oracle SOA Cloud Service 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.

In order create a VNC session on a VM, you must first identify the public IP address and connect to it with SSH:

1. Use the `ssh` command to [connect to the VM](#):

```
ssh -i private_key opc@VM_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:

```
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 Cloud Service 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.

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. 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:

```
./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* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

Perform Lifecycle Operations on an Oracle SOA Cloud Service Instance

Topics:

- [Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs](#)
- [Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance](#)
- [Scale an Oracle SOA Cloud Service Instance](#)
- [Add Storage to a Node](#)
- [Manage Tags for a Service Instance](#)
- [Change the License Type for an Oracle SOA Cloud Service Instance](#)
- [Back Up and Restore an Oracle SOA Cloud Service Instance](#)
- [Delete an Oracle SOA Cloud Service Instance](#)

Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs

You can stop or start an Oracle SOA Cloud Service instance and, when the service instance is running, start, stop, and restart individual Managed Server or load balancer VMs.

Topics:

- [About Stopping or Starting an Oracle SOA Cloud Service Instance and Individual VMs](#)
- [Stop, Start, or Restart an Oracle SOA Cloud Service Instance](#)
- [Restart the Administration Server VM](#)
- [Stop, Start, or Restart Managed Server and Load Balancer VMs](#)
- [Stop or Start WebLogic Servers](#)

About Stopping or Starting an Oracle SOA Cloud Service Instance and Individual VMs

You can stop or start an Oracle SOA Cloud Service instance. When the service instance is running, you can stop, start, and restart individual Managed Server or load balancer VMs.

Note:

The stop and restart procedures stop VMs. If you want to shut down the WebLogic Administration Server or Managed Server processes running on the VMs, without stopping the VMs, see *Shutting Down and Starting the WebLogic Server Managed Servers and Administration Server Processes on VMs* in *Using Oracle Java Cloud Service*. You might want to do this if you have other processes besides the servers running on the VMs and you do not want to shut down these other processes.

Why Stop an Oracle SOA Cloud Service Instance?

Stopping an Oracle SOA Cloud Service instance frees up compute resources used by the service instance's VMs.

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

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

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

When an Oracle Cloud Infrastructure instance is stopped, billing depends on the compute shape used to create the instance. Oracle SOA Cloud Service supports only standard shapes, which means that stopping an Oracle SOA Cloud Service instance always pauses billing. See [Resource Billing for Stopped Instances](#) in the Oracle Cloud Infrastructure documentation.

- **Starting the service instance:** All VMs on which the Administration Server, Managed Server, and load balancer are running are started. You can restart the Administration

Server, and stop, start, or restart the Managed Servers and load balancer VMs individually.

 **Note:**

Block storage should not be added manually by using the Oracle Compute Cloud Service because VM restart detaches that block storage. To reattach the block storage, you must use the Oracle Compute Cloud Service. However, block storage added manually is not deleted when an Oracle SOA Cloud Service instance is restarted. You must delete it manually. Instead of attaching block storage manually, add storage by scaling a node. For more information, see [Scale an Oracle SOA Cloud Service Node Up or Down](#).

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

If an Oracle SOA Cloud Service instance is running:

- You can restart the VMs on which the Administration Server, Managed Server, or load balancer are running if you are experiencing problems with the server that would warrant a reboot. The restart operation is the same as stopping the server or load balancer VM, then starting it immediately.
- You can stop the VMs on which the Managed Server or the load balancer are running to free up resources and stop metering those resources. You might also want to stop the service instance instead of scaling, keeping the server or load balancer ready for a later time. If you stop all but one Managed Server VM, you might want to stop the load balancer VM because it is not needed.
- You can start a Managed Server or load balancer VM if it is stopped and you want to use it again. Metering begins again.


How Do I Monitor the Stop, Start, or Restart Operation?

You can monitor progress of a stop, start, or restart operation on the Activity section of the Oracle SOA Cloud Service Instance Overview page. The Oracle SOA Cloud Service Instance Overview page is described in [About the Oracle SOA Cloud Service User Interface](#).

The Activity section indicates what kind of operation is in progress, and whether it is in progress or complete. When the operation ends, the start and end time of the operation is displayed.

Stop, Start, or Restart an Oracle SOA Cloud Service Instance

To stop, start, or restart an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click  for the instance you want to stop or start and select **Start**, **Stop**, or **Restart**.
2. Click **OK** in the confirmation dialog.

A yellow status icon is displayed adjacent to the service instance icon while the instance is in the process of stopping or starting.

When the operation completes, the Oracle SOA Cloud Service instance is stopped, started, or restarted. The yellow icon is no longer displayed. A red icon is


displayed when the instance is stopped. The entry for the instance shows that the operation has ended.

Repeat these steps for all nodes in the cluster.

Restart the Administration Server VM

You can restart the VM on which the Administration Server is running in an Oracle SOA Cloud Service instance that is in a running state.

To restart the Administration Server:


1. In the [Oracle SOA Cloud Service Console](#), click the name of the instance whose server you want to restart.
2. On the Overview page, click the  Menu icon adjacent to the Administration Server row and select **Restart**.
3. In the confirmation dialog, click **OK**.

A yellow status icon is displayed next to the service icon.

The Administration Server VM starts. The yellow icon is no longer displayed.

Stop, Start, or Restart Managed Server and Load Balancer VMs

You can stop, start, or restart the VMs on which the Managed Servers or the load balancer are running in an Oracle SOA Cloud Service instance if the service instance is in a running state. Restarting a Managed Server or load balancer VM is the same as stopping it, then starting it.

1. In the [Oracle SOA Cloud Service Console](#), click on the name of the instance whose servers you want to stop, start, or restart.
2. On the Overview page, click the  Menu icon to the right of the Managed Server or load balancer row and select **Stop**, **Start**, or **Restart**.
3. Click **OK** in the confirmation dialog.

The Managed Server or load balancer VM is stopped, started, or restarted.

Stop or Start WebLogic Servers

You can stop or start the WebLogic Servers using WebLogic Scripting Tool (WLST) commands and the WebLogic Server Administration Console.

Oracle SOA Cloud Service is built on top of Oracle Java Cloud Service, which in turn is built on top of Oracle WebLogic Server. When you create an Oracle SOA Cloud Service instance, an Oracle WebLogic domain is provisioned across all machines that are part of that Oracle SOA Cloud Service instance.

An Oracle WebLogic domain is made up of a set of WebLogic Server instances that work together to host and operate your Java EE applications. Within the domain only one WebLogic Server instance is responsible for administrative operations, such as creating new server instances or deploying applications. That privileged server is referred to as the *Administration Server*, whereas all the rest are *Managed Servers*.

The Administration Server also hosts the WebLogic Server Administration Console.

To stop the WebLogic servers:

- [Stop the Managed Servers](#)
- [Stop the Administration Server](#)


To start the WebLogic servers, reverse the order in which you stopped the servers:

- [Start the Administration Server](#)
- [Start the Managed Servers](#)

Stop or Start Managed Servers

You can stop or start the Managed Servers through the WebLogic Server Administration Console.

To stop or start Managed Servers:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open WebLogic Server Console**. Log in using the credentials you provided when you created the service instance.
2. Under **Domain Structure**, expand **Environment**.
3. Select **Servers**.
4. On the Configuration page, note the state of the Administration Server state and the Managed Servers.
5. Select the **Control** tab.
6. Click the check box to the left of each Managed Server name.
7. Click **Stop** or **Start**.
8. On the Server Life Cycle Assistant, click **Yes**.

If stopping, the server state changes to SHUTTING DOWN; if starting, the server state changes to STARTING.

9. Click the **Refresh** icon.

The server state changes to SHUTDOWN (if stopping) or RUNNING (if starting).

Stop or Start the Administration Server

You can stop or start the Administration Server 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](#):

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

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Check to see 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 where environment setup is located:

```
cd /u01/data/domains/domain_name/bin
```

For example:

```
cd /u01/data/domains/OurServi_domain/bin
```

5. Set up the environment.

```
./setDomainEnv.sh
```

6. Start WLST:

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

7. To connect to the Node Manager, use the WLST `nmConnect` command:

```
nmConnect  
('username', 'password', 'host', 'nmPort', 'domainName', 'domainDir', 'nmType')
```

Parameter	Description	Example
username	WebLogic Server username you specified when you created the service instance.	
password	WebLogic Server password you specified when you created the service instance.	
host	The host name of the Node Manager. This is typically of the format <i>instanceName-wls-1</i> .	ourserviceinstance-wls-1
nmPort	Port number of the node manager.	5556
domainName	Name of the domain. You can find the domain name on the Oracle SOA Cloud Service Instance Overview page.	OurServi_domain
domainDir	Path to the domain. In Oracle SOA Cloud Service, the domain directory is <i>/u01/data/domains/<i>domainName</i></i> .	<i>/u01/data/domains/OurServi_domain</i>
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')
```

For more information about `nmConnect` parameters, see *WLST Command Reference for WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

8. Stop or start the Administration Server:

- To stop the Administration Server, follow the steps in [Stop or Start 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()
```

Disable Load Balancer Traffic to Suspend an Oracle SOA Cloud Service Instance

You can disable the load balancer to suspend an Oracle SOA Cloud Service instance temporarily, blocking any new traffic from being delivered to the instance. This is useful when you want to perform routine maintenance on an Oracle SOA Cloud Service instance, but do not want to stop the instance. Once the maintenance activities have been completed, you can reenables the load balancer to allow traffic to be delivered.


See also [Administer the Load Balancer for an Oracle SOA Cloud Service Instance](#).



Note:

If a load balancer is not configured, you cannot suspend the Oracle SOA Cloud Service instance.

To disable the load balancer:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance with the cluster that you want to scale out.
2. On the Overview page, click the instance menu  icon (in the header) and select **Disable Load Balancer**.
3. In the confirmation prompt, click **Yes, Disable Load Balancer**.

Scale an Oracle SOA Cloud Service Instance

You can scale an Oracle SOA Cloud Service instance by scaling a cluster or a node. Determine what you need to scale from metrics associated with the service instance. For example, if response times are long, consider scaling out the cluster. Or if heap usage is high, consider scaling up the nodes in the cluster.

You cannot scale a service instance if the service instance is under maintenance such as during patching or backing up.

Topics:

- [Scale Out or In](#)
- [Scale Up or Down](#)
- [View Scaling Requests](#)



Note:

For information about using REST resources to scale Oracle SOA Cloud Service instances, see REST API for Oracle SOA Cloud Service.

Scale Out or In

Scale an Oracle SOA Cloud Service 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.



Note:

A scale out or in operation requires some down time as servers on the nodes in the Oracle SOA Cloud Service cluster are automatically restarted after the scale operation. Before scaling, make sure that there are no active running processes on the servers.

Topics:

- [About Scaling Out an Oracle SOA Cloud Service Cluster](#)
- [About Scaling In an Oracle SOA Cloud Service Cluster](#)
- [About the Impact of Scaling on JMS Transport URLs](#)
- [Scale Out an Oracle SOA Cloud Service Cluster](#)
- [Scale In an Oracle SOA Cloud Service Cluster](#)

About Scaling Out an Oracle SOA Cloud Service Cluster

Scaling **out** an Oracle SOA Cloud Service cluster adds one node to the cluster.

 **Notes:**

- If you scale out a cluster after scaling any of its nodes, the new node has the compute shape and the amount of storage with which the service instance was originally created. To ensure that all nodes in your cluster are equivalent, you must scale the new node to match the other nodes in your cluster, as described in [Scale an Oracle SOA Cloud Service Node Up or Down](#).
- Adding a node to a cluster increases the billing of the Oracle SOA Cloud Service instance.
- If any patches were applied after provisioning the Oracle SOA Cloud Service, 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](#).

Before scaling out an Oracle SOA Cloud Service cluster, ensure that all these conditions are met:

- You have the Oracle SOA administrator role as described in [About Oracle SOA Cloud Service Roles and User Accounts](#).
- The service instance is **not** under maintenance.

If any of these conditions are not met, the scaling operation fails and Oracle SOA Cloud Service logs an error message.

Oracle SOA Cloud Service logs a message when scaling out is started or completed, or when a failure is detected. You can view these messages as explained in [View Scaling Requests](#).

If an attempt to scale out a cluster fails, Oracle SOA Cloud Service does the following:

- Logs any diagnostic information.
- Sets the status of the service instance to `RUNNING` to allow other operations to continue.
- Returns the service instance to its original shape.
- Deletes the VM that it created to run the additional managed server instance.

For steps to scale out an Oracle SOA Cloud Service cluster, see [Scale Out an Oracle SOA Cloud Service Cluster](#).

About Scaling In an Oracle SOA Cloud Service Cluster

Scaling **in** an Oracle SOA Cloud Service cluster removes the selected node from the cluster.

Before scaling in an Oracle SOA Cloud Service cluster, ensure that the cluster contains at least one managed server node in addition to the node for the administration server and first managed server. You cannot scale in a cluster that contains only the node for the administration server and first managed server. If you no longer require that node, you must delete the entire service instance. For instructions, see [Delete an Oracle SOA Cloud Service Instance](#).

By default, Oracle SOA Cloud Service scales in a cluster gracefully by shutting down the managed server instance before removing the managed server instance from the cluster and terminating its VM. To ensure that the node is removed even if the managed server instance is unresponsive, you can choose to forcibly scale in a cluster.

If an attempt to scale in a cluster fails, Oracle SOA Cloud Service does the following:

- Logs any diagnostic information.
- Sets the status of the service instance to `RUNNING` to allow other operations to continue.
- Cleans up any stale resources.

For steps to scale in an Oracle SOA Cloud Service cluster, see [Scale In an Oracle SOA Cloud Service Cluster](#).

About the Impact of Scaling on JMS Transport URLs

When you add (scale out) or remove (scale in) nodes, you must reconfigure the JMS transport URIs in Oracle Service Bus.

The JMS transport in Oracle Service Bus is configured with JMS URIs of the following format:

```
jms://cluster_address/connection_factory/UDQ
```

For example, if you do not reconfigure the JMS URI after scaling in (such as removing the second node in a two-node cluster), sending messages to UDQ results in the following exception:

```
The invocation resulted in an error: [JMSPool:169803]JNDI lookup of the JMS connection factory weblogic.jms.ConnectionFactory failed:  
javax.naming.ServiceUnavailableException: slc07pjl-soaqa-2vm-otd-0616-osb-jcs-wls-2 [Root exception is java.net.UnknownHostException: slc07pjl-soaqa-2vm-otd-0616-osb-jcs-wls-2].
```

Scale Out an Oracle SOA Cloud Service Cluster

You can scale out an Oracle SOA Cloud Service cluster to add one node to the cluster. When you scale out, Oracle SOA Cloud Service creates a new Managed Server VM.


For more information about scaling out an Oracle SOA Cloud Service cluster, see [About Scaling Out an Oracle SOA Cloud Service Cluster](#).

Note:

A scale out operation requires some down time as servers on the nodes in the Oracle SOA Cloud Service cluster are automatically restarted after the scale operation. Before scaling, make sure that there are no active running processes on the servers.

To scale out an Oracle SOA Cloud Service cluster:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance with the cluster that you want to scale out.

2. On the Overview page, click the **Add Node**  icon or click  (in the header) and select **Scale Out**.

The Scale Out dialog is displayed.

3. To confirm you want to scale out the cluster, click **Scale Out**.

4. After a few moments, click the **Refresh**  icon to update the page.

You may need to click the icon more than once to see changes.

After a few moments of processing, the new node appears on the Overview page and you can see the number of nodes increased by one. For a description of the items in the node line item, see [About the Oracle SOA Cloud Service User Interface](#).

At any time during the scaling process, you can check its status by opening the Activity page from the Oracle SOA Cloud Service Console. You can see the scale-out status in the activity table.

 **Note:**

After scaling out, you must restart the Administration Server and all Managed Servers. This applies to both Oracle SOA Cloud Service and Oracle Service Bus domain configuration types. Failure to restart servers after scaling out can impact functionality.

Scale In an Oracle SOA Cloud Service Cluster

You can scale in an Oracle SOA Cloud Service cluster to remove a selected node from the cluster. When you scale in, Oracle SOA Cloud Service removes the selected Oracle WebLogic Server managed server instance and the VM that it is running on.

For more information about scaling in an Oracle SOA Cloud Service cluster, see [About Scaling In an Oracle SOA Cloud Service Cluster](#).

 **Note:**

A scale in operation requires some down time as servers on the nodes in the Oracle SOA Cloud Service cluster are automatically restarted after the scale operation. Before scaling, make sure that there are no active running processes on the servers.

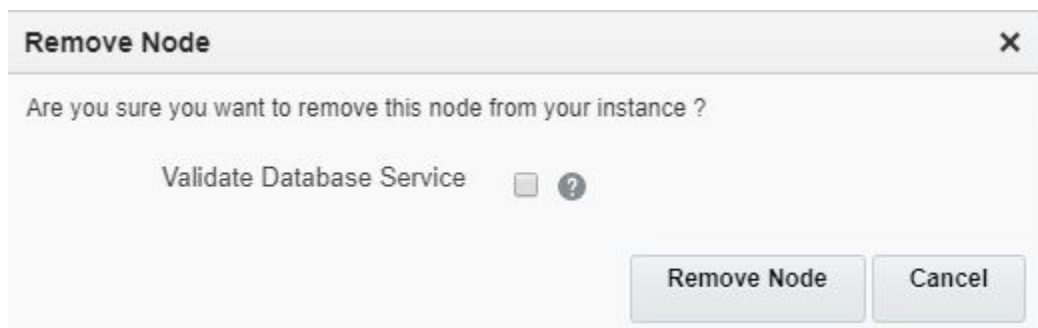
To scale in an Oracle SOA Cloud Service cluster:


1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance with the cluster that you want to scale in.

2. On the Overview page, click the  menu for the node you want to remove and select **Remove Node**.

The Remove Node dialog box is displayed.

3. In the Remove Node dialog box:



- Optionally, to ensure that database connectivity is still active, select the **Validate Database Service** check box, then enter the Administration User Name and Password.
 - Click **Remove Node**.
4. After a few moments, click the **Refresh**  icon to update the page.
You may need to click the icon more than once to see changes.

After a few moments of processing, the node is removed from the Overview page and you can see the number of nodes decreased by one. At any time during the scaling process, you can check its status by opening the Activity page from the Oracle SOA Cloud Service Console. You can see the scale-in status in the activity table.

 **Note:**

After scaling in, you must restart the Administration Server and all Managed Servers. This applies to both Oracle SOA Cloud Service and Oracle Service Bus domain configuration types. Failure to restart servers after scaling out can impact functionality.

Scale Up or Down

Scale an Oracle SOA Cloud Service node 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. The compute shape specifies the number of Oracle Compute Units (OCPU) and amount of memory (RAM) that you want to allocate to the node.

 **Note:**

A scale up or down operation requires some down time as servers on the Oracle SOA Cloud Service 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.]

Topics:

- [About Scaling an Oracle SOA Cloud Service Node Up or Down](#)
- [Scale an Oracle SOA Cloud Service Node Up or Down](#)

About Scaling an Oracle SOA Cloud Service Node Up or Down

You can scale only the Administration Server node and Managed Server nodes in a WebLogic Server cluster. Oracle SOA Cloud Service does not support scaling for other nodes in a service instance, such as the load balancer node.

You must scale each node in a cluster individually. You cannot scale all nodes in a cluster in a single operation.

**Note:**

Changing the compute shape to a higher value increases the billing of the Oracle SOA Cloud Service instance.

Oracle SOA Cloud Service provides a set of compute shapes that are optimized for different use cases. Choose from a set of all-purpose and memory-intensive shapes. The larger the compute shape, the greater the processing power:

- To meet the demands of heavier workloads, scale up the compute shape of a node by choosing a larger compute shape.

For example, changing the compute shape from OC1M to OC2M or from VMStandard2.1 to VMStandard2.2 doubles the capacity of the node from one OCPU to two OCPUs and doubles the amount of RAM allocated to the node.

- To save costs if the workload is lightened, scale down the compute shape of a node by choosing a smaller compute shape.

For example, changing the compute shape from OC2M to OC1M or from VMStandard2.2 to VMStandard2.1 reduces the capacity of the node by half from two OCPUs to one OCPU and reduces the amount of RAM allocated to the node by half.

**Note:**

To optimize performance and balance the load on Managed Server instances correctly, ensure that the compute shapes of all nodes in a cluster are the same. When routing requests to Managed Server instances, the load balancer treats all Managed Server instances as being equivalent.

For steps to scale an Oracle SOA Cloud Service node, see [Scale an Oracle SOA Cloud Service Node Up or Down](#).

Scale an Oracle SOA Cloud Service Node Up or Down

You can scale an Oracle SOA Cloud Service node 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. The compute shape specifies the number of Oracle Compute Units (OCPU) and amount of memory (RAM) that you want to allocate to the node.

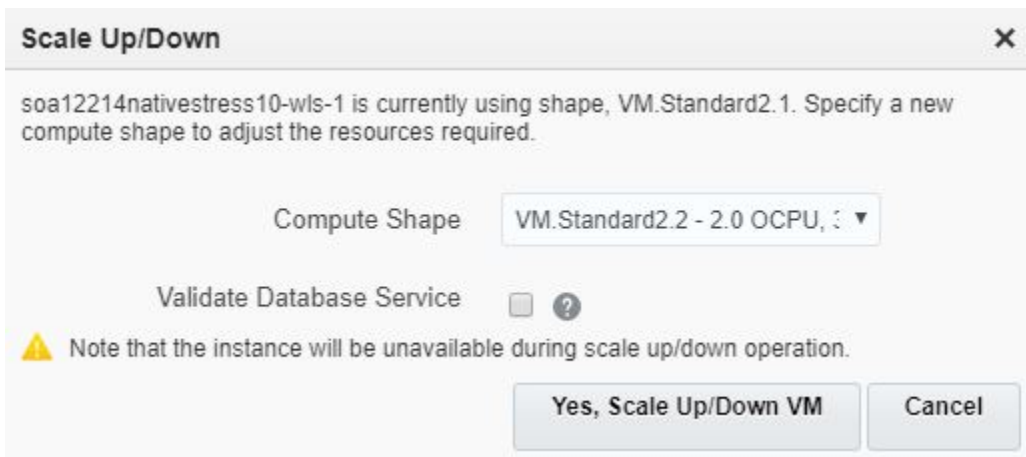
For more information about scaling an Oracle SOA Cloud Service node, see [About Scaling an Oracle SOA Cloud Service Node Up or Down](#)

 **Note:**

A scale up or down operation requires some down time as servers on the Oracle SOA Cloud Service 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.]

To scale an Oracle SOA Cloud Service node up or down:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance with the node that you want to scale up or down.
2. On the Overview page, click the  menu for the node, and choose **Scale Up/Down**.
The Scale Up/Down dialog box opens.
3. In the Scale Up/Down dialog box:




- Specify the new compute shape of the node: to scale up the node, choose a larger compute shape than the current compute shape; to scale down, choose a smaller computer shape.
 - (Optional) Select the **Validate Database Service** check box to validate the status of the database service before scaling the node up or down, then enter the administration user name and password.
4. Click **Yes, Scale Up/Down VM**.

While Oracle SOA Cloud Service is applying your changes, the service instance is in Maintenance mode, the state of the node is Configuring, and any servers running on the node are stopped. After applying your changes, Oracle SOA Cloud Service starts any servers that should run on the node.

View Scaling Requests

Use the Oracle SOA Cloud Service Console to view the status of ongoing scaling requests, and the success or failure of previous requests.

To view the status of ongoing or past scaling requests:

1. In the [Oracle SOA Cloud Service Console](#), click the **Activity** tab.
2. Click  adjacent to a scaling activity in the table.

Add Storage to a Node

You can add storage to a node that is running out of space. When you add storage to a node, an Oracle Compute Cloud Service storage volume is created and attached to the node's VM.

Notes:

- After you add storage to a node, that node is restarted. If there are other nodes in the cluster, they are not restarted.
- You cannot remove storage from a node.

The new storage volume created remains attached and available to the node's VM even when the service instance is restarted or is stopped and then started. Also, this storage volume exists until you delete the service instance, at which time the storage volume is also deleted.

You can add the storage to the following existing volumes:

- Middleware storage volume
- Domain storage volume
- Backup storage volume (Administration Server node only)


For details about these volumes, see [About the Disk Volumes](#).

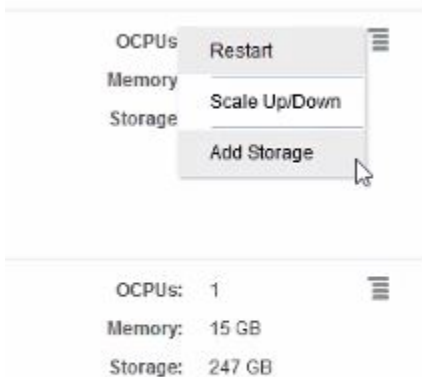
You can add storage a maximum of five times to a storage volume.

Caution:

Before adding storage to the Middleware or Domain storage volume, back up the service instance to avoid the risk of data loss. For instructions, see [Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance](#).

To add storage to a node:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance to which you want to add storage.
2. On the Overview page, click the  menu for the node, and choose **Add Storage**.



The Add Storage dialog box opens.

3. In the Add Storage dialog box, specify the size in GB you want to add to the node for each volume. As noted in the dialog, the minimum size you can add is 50GB.



4. Click **Yes, Add Storage**.

! Important:

The node to which storage is added is restarted. If there are other nodes in the cluster, they are not restarted.

Manage Tags for a Service Instance

A tag is a key or a key-value pair that you can assign to your Oracle SOA Cloud Service instances. You can use tags to organize and categorize your instances, and to search for them.


Topics:

- [Create, Assign, and Unassign Tags](#)
- [Find Tags and Instances Using Search Expressions](#)

Create, Assign, and Unassign Tags

You can create and assign tags to Oracle SOA Cloud Service instances while creating the instances or later. When you no longer need certain tags for an instance, you can unassign them.

To assign tags to an instance or to unassign tags:

1. In the [Oracle SOA Cloud Service Console](#), click  for the instance to which you want to assign tags and select **Manage Tags** or **Add Tags**.
If any tags are already assigned, then the menu shows **Manage Tags**; otherwise, it shows **Add Tags**.
2. In the Manage Tags dialog box, create and assign the required tags, or unassign tags:
 - In the **Assign** section, select the **Tags** that you want to assign to the instance.
 - If the tags that you want to assign don't exist, then select **Create and Assign** in the **Tags** field, and click just above the field. Enter the required new tags in the **Enter New Tags** field.
 - To unassign a tag, in the **Unassign** section, look for the tag that you want to unassign, and click the **X** icon next to the tag.

Note:

You might see one or more tags with the key starting with `ora_`. Such tags are auto-assigned and used internally. You can't assign or unassign them.

3. After assigning and unassigning tags, click **OK** for the tag assignments to take effect.

Find Tags and Instances Using Search Expressions

A tag is an arbitrary key or a key-value pair that you can create and assign to your Oracle SOA Cloud Service instances. You can use tags to organize and categorize your instances, and to search for them. Over time, you might create dozens of tags,

and you might assign one or more tags to your instances. To search for specific tags and to find instances that are assigned specific tags, you can use filtering expressions.

Search for Instances with Tags

From the Instances page of the web console, select **Tags**, and then enter a *search expression* in the **Search** field.

For example, you can search for the instances that are assigned a tag with the key `env` and any value starting with `dev` (example: `env:dev1`, `env:dev2`), by entering the search expression `'env': 'dev%'`.

Instances



Similarly, when you use the REST API to find tags or to find instances that are assigned specific tags, you can filter the results by appending the optional `tagFilter=expression` query parameter to the REST endpoint URL.

- To find specific tags: `GET paas/api/v1.1/tags/{identity_domain}/tags?tagFilter={expression}`
- To get a list of instances that are assigned specific tags: `GET paas/api/v1.1/instancemgmt/{identity_domain}/instances?tagFilter={expression}`

Syntax and Rules for Building Tag-Search Expressions

- When using cURL to send tag-search API requests, enclose the URL in double quotation marks.

Example:

```
curl -s -u username:password -H "X-ID-TENANT-NAME:acme" "restEndpointURL/paas/api/v1.1/instancemgmt/acme/instances?tagFilter='env'"
```

This request returns all the tags that have the key `env`.

- Enclose each key and each value in single quotation marks. And use a colon (`:`) to indicate a key:value pair.

Examples:

```
'env'
'env': 'dev'
```

- You can include keys or key:value pairs in a tag-filtering expression.

Sample Expression	Description	Sample Search Result
'env'	Finds the tags with the key <code>env</code> , or the instances that are assigned the tags with that key.	The following tags, or the instances that are assigned any of these tags: env:dev env:qa
'env': 'dev'	Finds the tag with the key <code>env</code> and the value <code>dev</code> , or the instances that are assigned that tag.	The following tag, or the instances that are assigned this tag env:dev

- You can build a tag-search expression by using actual keys and key values, or by using the following wildcard characters.

% (percent sign): Matches any number of characters.

_ (underscore): Matches one character.

Sample Expression	Description	Sample Search Result
'env': 'dev%'	Finds the tags with the key <code>env</code> and a value starting with <code>dev</code> , or the instances that are assigned such tags. Note: When you use <code>curl</code> or any command-line tool to send tag-search REST API requests, encode the percent sign as <code>%25</code> .	The following tags, or the instances that are assigned any of these tags: env:dev env:dev1
'env': 'dev_'	Finds the tags with the key <code>env</code> and the value <code>devX</code> where <code>X</code> can be any one character, or finds the instances that are assigned such tags.	The following tags, or the instances that are assigned any of these tags: env:dev1 env:dev2

- To use a single quotation mark (`'`), the percent sign (`%`), or the underscore (`_`) as a literal character in a search expression, escape the character by prefixing a backslash (`\`).

Sample Expression	Description	Sample Search Result
'env': 'dev _%'	Finds the tags with the key <code>env</code> and a value starting with <code>dev_</code> , or the instances that are assigned such tags.	The following tags, or the instances that are assigned any of these tags: env:dev_1 env:dev_admin

- You can use the Boolean operators AND, OR, and NOT in your search expressions:


Sample Expression	Description	Sample Search Result
'env' OR 'owner'	Finds the tags with the key <code>env</code> or the key <code>owner</code> , or the instances that are assigned either of those keys.	The following tags, or the instances that are assigned <i>any of these tags</i> : env:dev owner:admin
'env' AND 'owner'	Finds the instances that are assigned the tags <code>env</code> <i>and</i> <code>owner</code> . Note: This expression won't return any results when used to search for tags, because a tag can have only one key.	The instances that are assigned <i>all of the following tags</i> : env:dev owner:admin
NOT 'env'	Finds the tags that have a key other than <code>env</code> , or the instances that are assigned such tags. Note: Untagged instances as well will satisfy this search expression.	The following tags, or the instances that are assigned <i>any of these tags</i> or no tags: owner:admin department
('env' OR 'owner') AND NOT 'department'	Finds the tags that have the key <code>env</code> or the key <code>owner</code> but not the key <code>department</code> , or the instances that are assigned such tags.	The following tags, or the instances that are assigned <i>any of these tags</i> : env:dev owner:admin

Change the License Type for an Oracle SOA Cloud Service Instance

If your account has both Bring Your Own License (BYOL) and Oracle SOA Cloud Service entitlements, you can change the license type of an existing service instance.

When you create an Oracle SOA Cloud Service instance, you can change the license type from BYOL to a cloud license or vice versa after the instance is created. For information about subscriptions and licenses, see [About Oracle SOA Cloud Service Subscriptions and Licenses](#)

To change the license type for an Oracle SOA Cloud Service instance:

- In the [Oracle SOA Cloud Service Console](#), click  for the instance and select **Change License Type**.
- In the Change License Type dialog box, select one of the following options:
 - For a cloud subscription licence: **Subscribe to a new Oracle SOA Cloud Service software license and the Oracle SOA Cloud Service.**

- For BYOL: **My organization already owns Oracle middleware software licenses. Bring my existing middleware software license to the Oracle SOA Cloud Service.**
3. Click **Change**.

Back Up and Restore an Oracle SOA Cloud Service Instance

This section explains how to back up and restore an Oracle SOA Cloud Service instance.

Topics:

- [About Backup and Restoration of Oracle SOA Cloud Service Instances](#)
- [Typical Workflow for Backing Up and Restoring an Oracle SOA Cloud Service Instance](#)
- [Update Backup and Recovery Credentials](#)
- [Configure Automated Backups for an Oracle SOA Cloud Service Instance](#)
- [Disable Backups for an Oracle SOA Cloud Service Instance](#)
- [Disable Coordinated Backups for an Oracle SOA Cloud Service Instance](#)
- [Delete a Backup](#)
- [Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance](#)
- [Restore an Oracle SOA Cloud Service Instance from a Backup](#)
- [Return an Oracle SOA Cloud Service Instance to Service After Restoration from a Backup](#)

About Backup and Restoration of Oracle SOA Cloud Service Instances

By backing up your Oracle SOA Cloud Service instances, you can preserve them in a particular state. If you later make configuration changes to a service that you don't want, you can undo them by restoring the service instance's configuration data from a backup. You can also restore the software to its current official patch set update (PSU) level.

Topics:

- [Contents of a Backup](#)
- [How Backups Are Initiated](#)
- [Where Backups Are Stored](#)
- [What Happens During a Backup](#)
- [How Restorations Are Initiated](#)

Contents of a Backup

What a backup contains depends on whether the backup is an **incremental backup** or a **full backup**.

For details about the volumes that are backed up, see *About the Disk Volumes in Using Oracle Java Cloud Service*.

Topics:

- [Contents of an Incremental Backup](#)
- [Contents of a Full Backup](#)
- [Links Between an Incremental Backup and Its Related Full Backup](#)
- [Items that Are Not Backed Up](#)

Contents of an Incremental Backup

An incremental backup contains only runtime artifacts of each managed virtual machine in the service instance.

**Note:**

All incremental backups are automated scheduled backups. You cannot create an incremental backup on demand.

While creating an incremental backup, Oracle SOA Cloud Service promotes the backup to a full backup if any of the following conditions are met:

- The configuration data of the service instance has been restored since the last scheduled full backup.
- The service instance has been scaled out since the last scheduled full backup.
- Oracle SOA Cloud Service can now reach a virtual machine that it could not reach during the last scheduled full backup.
- The last full scheduled backup is no longer available.

You can recognize a promoted backup in the list of available backups from its type and creation time. Any full, automated backup created at the scheduled time for an incremental backup has been promoted.

Contents of a Full Backup

A full backup contains all the runtime artifacts required to restore the service instance's configuration data.

Specifically, a full backup contains these items:

- The Oracle WebLogic Server domain configuration of the service instance, which consists of these items:
 - The `$DOMAIN_HOME` volume of each virtual machine
Managed Server persistent stores that are not stored in the Oracle Database Classic Cloud Service database deployment are stored under `$DOMAIN_HOME`. Examples of Managed Server persistent stores are transaction logs and Java Message Service (JMS) providers.
 - Oracle WebLogic Server domain configuration files in the `$MW_HOME` volume of the Administration Server virtual machine
- Oracle Traffic Director configuration for the load balancer

 **Note:**

Oracle SOA Cloud Service does **not** back up any software, including Oracle Fusion Middleware software installed on the `$MW_HOME` volume. You are responsible for ensuring that you can re-install any software that you have installed on a service instance's VMs if necessary.

Links Between an Incremental Backup and Its Related Full Backup

Each incremental backup is linked to the last full backup that was performed before the incremental backup. As a result, each full backup is linked to all incremental backups that were performed between that full backup and the next full backup.

You can restore a service instance from an incremental backup without the need to restore the full backup to which the incremental backup is linked. In this situation, you are responsible for ensuring that the service instance is in a consistent state after the service instance is restored. See [Restore an Oracle SOA Cloud Service Instance from a Backup](#).

However, you **cannot** delete or archive a full backup to which one or more incremental backups are linked. If you want to delete or archive a full backup to which incremental backups are linked, you must delete or archive the linked backups first. See [Delete a Backup](#).

Items that Are Not Backed Up

Oracle SOA Cloud Service ensures that backups contain only the volumes that are needed for a proper restoration of a service instance.

Therefore, the following items are **not** backed up:

- Users' custom volumes
- The `$JDK_HOME` volume, which contains the JDK software
- Software binary files in the `$MW_HOME` volume

How Backups Are Initiated

Backups are initiated in several different ways.

- Oracle SOA Cloud Service initiates scheduled automated backups on the following default schedule:
 - Full backups are initiated weekly starting 12 hours after a service instance was created, rounded to the nearest five-minute interval.
For example, if a service instance is created at 1:01 PM on a Monday, full backups are initiated at 1:00 AM on Tuesdays.
 - Incremental backups are initiated every day except the day of a full backup at the same time that full backups are initiated.
For example, if a service instance is created at 1:01 PM on a Monday, incremental backups are initiated at 1:00 AM every day except Tuesdays.

You can change the schedule on which automated backups are initiated as explained in [Configure Automated Backups for an Oracle SOA Cloud Service Instance](#).

 **Note:**

You cannot configure how often backups are performed, only when they are performed.

- You can initiate a backup immediately without having to wait for the next scheduled backup as explained in [Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance](#).
- Oracle SOA Cloud Service initiates a **full** backup immediately before an Oracle SOA Cloud Service instance is patched.
- Oracle SOA Cloud Service initiates an **incremental** backup immediately before an Oracle SOA Cloud Service instance is scaled in or scaled out.

Where Backups Are Stored

Oracle SOA Cloud Service stores all backups in an Oracle SOA Cloud Service container. To speed up restorations from recent backups, Oracle SOA Cloud Service also keeps a local copy of any backup it has recently created.

 **Note:**

Do not attempt to download the backup files generated by Oracle SOA Cloud Service. These files are encrypted and not accessible offline. You must use Oracle SOA Cloud Service to restore a service instance from a backup.

How Backups in a Storage Container Are Stored

By default, Oracle SOA Cloud Service stores backups in the container that was specified when the service instance was created. You can choose to store the backups in a different container as explained in [Configure Automated Backups for an Oracle SOA Cloud Service Instance](#).

Oracle SOA Cloud Service automatically deletes a backup when the retention period for the backup has elapsed.

How Local Copies of Backups Are Stored

Oracle SOA Cloud Service stores local copies in a dedicated volume mounted on the block storage attached to the virtual machine where the Administration Server is running. A backup fails if there is insufficient free space on this volume.

How long Oracle SOA Cloud Service keeps the local copy of a backup before deleting it depends on the extent of the backup:

- For an incremental backup, Oracle SOA Cloud Service keeps the local copy for seven days.

- For a full backup, Oracle SOA Cloud Service keeps the local copy for as long as the local copy of its last related incremental backups is kept, or for seven days, whichever is longer.

How Backups and Local Copies Are Deleted Automatically

After completing the day's scheduled backup, Oracle SOA Cloud Service deletes any backups or local copies that are due to be deleted that day. If the scheduled backup fails because of insufficient space, backups and local copies that are due to be deleted are still deleted.



Note:

When an Oracle SOA Cloud Service instance is deleted, all its backups are deleted.

What Happens During a Backup

During a backup of an Oracle SOA Cloud Service instance, the service instance continues to run and all applications deployed to the service instance remain available.

To prevent configuration changes during a backup, Oracle SOA Cloud Service locks the Oracle WebLogic Server domain. After locking the domain, Oracle SOA Cloud Service backs up files on each node as described in [Contents of a Backup](#).



Note:

Do **not** attempt to start the administration server while a backup is in progress.

While the backup is in progress, you cannot start any other management operation on the service instance.

When the backup is complete, Oracle SOA Cloud Service unlocks the Oracle WebLogic Server domain. If the backup is a scheduled backup, Oracle SOA Cloud Service also cleans up aged backups as follows:

- It deletes from local storage all backups old enough to be stored only in the Oracle Cloud Storage Service container.
- It deletes from wherever they are stored any remaining copies of backups whose retention period has elapsed.

If the scheduled backup fails because of insufficient space, the aged backups are still cleaned up.

To back up the database, Oracle SOA Cloud Service uses Recovery Manager (RMAN). The backup of the database is coordinated with the backup of other volumes.



Note:

Oracle SOA Cloud Service does not automatically remove transaction records when backing up a service instance. Therefore, you must remove transaction records after you restore a service instance from a backup.

How Restorations Are Initiated

Restorations are initiated in a couple different ways.

- You can initiate a restoration as explained in [Restore an Oracle SOA Cloud Service Instance from a Backup](#).
- Oracle SOA Cloud Service initiates a restoration after a failed attempt to patch a service instance to return the service instance to the state it was in before the failed attempt.

Typical Workflow for Backing Up and Restoring an Oracle SOA Cloud Service Instance

To back up and restore an Oracle SOA Cloud Service instance, consider this typical workflow.



Note:

Except where noted, the table provides one or more links to information about how to perform each task by using the web-browser-based Oracle SOA Cloud Service administration console. For information about using REST endpoints to perform these tasks, see REST API for Oracle SOA Cloud Service


Task	Description	More Information
Configure automated backups for an Oracle SOA Cloud Service instance	Customize the following properties of automated backups for an Oracle SOA Cloud Service instance: <ul style="list-style-type: none"> • When automated backups are performed • Where backups more than seven days old are stored • How long new backups are retained 	Configure Automated Backups for an Oracle SOA Cloud Service Instance
Initiate an on-demand backup of an Oracle SOA Cloud Service instance	Create a backup immediately without having to wait for the next scheduled backup.	Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance
Delete a backup	Delete a backup that you no longer require to release storage or prevent an Oracle SOA Cloud Service instance from being restored from the backup.	Delete a Backup


Task	Description	More Information
Restore an Oracle SOA Cloud Service instance from a backup	Return an Oracle SOA Cloud Service instance to a particular state or recover a service instance after a loss of data.	Restore an Oracle SOA Cloud Service Instance from a Backup
Return an Oracle SOA Cloud Service instance to service after restoration from a backup	Modify a restored service instance to return it to the state you require and perform steps to return the service instance to service that Oracle SOA Cloud Service does not automate.	Return an Oracle SOA Cloud Service Instance to Service After Restoration from a Backup

Update Backup and Recovery Credentials

Use the Oracle SOA Cloud Service Console to update the storage container and credentials used to access backup storage resources.

To update backup and recovery credentials:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the instance you want to back up.
2. On the Overview page, click the **Administration** tile.
3. Click  adjacent to **Available Backups** and select **Configure Backups**.
4. Complete the following fields:

Field	Description
Storage Container	<p>Oracle Cloud Infrastructure: Enter the URL of an existing bucket in Oracle Cloud Infrastructure Object Storage in the following format: <code>https://swiftobjectstorage.region.oraclecloud.com/v1/account/bucket</code>.</p> <p>For example: <code>https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/myCompany/myBucket</code>.</p> <p>Oracle Cloud Infrastructure Classic: Enter the name of the Oracle Cloud Infrastructure Object Storage Classic container used to provide storage for your service instance backups using the following format: <code>Storage-storage_identitydomain/containername</code>.</p> <p>For example: <code>Storage-us4112opcsa01/InsightBackup</code>.</p> <div style="border: 1px solid #0070c0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>Before you switch the Storage Container to a new URL, make sure that existing backups are deleted. You may get an error if the instance has backups present, as these will not be accessible after switching containers.</p> </div>
Username	<ul style="list-style-type: none"> • Oracle Cloud Infrastructure Classic: Enter the user name of the Oracle Cloud Infrastructure Object Storage Classic service user with access permissions to the container you specified earlier. If the container does not exist, then enter the user name of a service administrator. • Oracle Cloud Infrastructure: Enter the user name of the Oracle Cloud Infrastructure Object Storage user with access permissions to the bucket you specified earlier. (Not available on Oracle Cloud at Customer).
Password	<ul style="list-style-type: none"> • Oracle Cloud Infrastructure Classic: Enter the password of the user that you specified. • Oracle Cloud Infrastructure: Enter the auth token generated in Oracle Cloud Infrastructure for the user that you specified. (Not available on Oracle Cloud at Customer).

If **Configure Backups** is disabled, and Oracle SOA Cloud Service backups are failing because of incorrect credentials, then you can enable backups and reset with new credentials using the following REST API:

```
curl -v -i -X POST -u "MyservicesUsername:MyservicesPassword" -d @enable.json -H "Content-type:application/json" -H "X-ID-TENANT-NAME:identityDomain" https://restServerURL/paas/api/v1.1/instancemgmt/identityDomain/services/SOA/instances/instanceName/backupconfi
```


Example command:

```
curl -v -i -X POST -u "MyUser@company.com:MyServicesPassword" -d
@enable.json -H "Content-type:application/json" -H "X-ID-TENANT-
NAME:idcs-7dc693e80d9b469480d7afe00e743931" https://
psm.us.oraclecloud.com/paas/api/v1.1/instancemgmt/
idcs-7dc693e80d9b469480d7afe00e743931/services/SOA/instances/SOADev/
backupconfi
```

Sample enable.json file:

```
{
  "backups": "ENABLE",
  "cloudStorageContainer": "https://foo.storage.oraclecloud.com/v1/
MyService-bar/MyContainer",
  "cloudStorageUser": "NewOrExistingStorageUserName",
  "cloudStoragePassword": "NewStoragepassword"
}
```

After running this command, monitor the job activity. Once it is successful, the **Configure Backups** button will be enabled, storage credentials are updated with the new credentials, and backups should succeed.

Configure Automated Backups for an Oracle SOA Cloud Service Instance

Use the Oracle SOA Cloud Service Console to configure automated backups to customize when the service instance is backed up and how backups are stored.

You can customize the following properties of the service instance:

- **When automated backups are initiated.** By default, backups are performed at the following times:
 - Full backups are initiated weekly starting 12 hours after the service instance was created, rounded to the nearest five-minute interval.
For example, if a service instance is created at 1:01 PM on a Monday, full backups are initiated at 1:00 AM on Tuesdays.
 - Incremental backups are initiated every day except the day of a full backup at the same time that full backups are initiated.
For example, if a service instance is created at 1:01 PM on a Monday, incremental backups are initiated at 1:00 AM every day except Tuesdays.

Note:

You cannot configure how often backups are performed, only when they are performed.

- **Where backups are stored.**
 - **Oracle Cloud Infrastructure:** Stored in the Oracle Cloud Infrastructure bucket that was provided when the service instance was created.

- **Oracle Cloud Infrastructure Classic:** Stored in the Oracle Cloud Infrastructure Object Storage Classic container that was provided when the service instance was created.

 **Note:**

- If you change the password for the administrator of the Oracle Cloud Infrastructure Classic container, you must specify the new password in the Oracle Cloud Infrastructure Classic Account Details section.
- If you change the swift password for the administrator of the Oracle Cloud Infrastructure Object bucket, you must specify the new password in the Oracle Cloud Infrastructure Account Details section.

- **How long new backups are retained.** By default, incremental backups are retained for 30 days.

Full backups are retained until their last related incremental backup is no longer available. For example, if two consecutive full backups are three days apart, the older full backup is retained two extra days.

 **Note:**


The additional retention period for full backups is fixed and you cannot change it.

Because the changes affect only one service instance, you can configure different values for these properties for each of your service instances.

 **Note:**

You **cannot** configure automated backups for an Oracle SOA Cloud Service instance while the service instance is being backed up.

To configure automated backups for an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to configure automated backups.
2. On the Overview page, click the **Administration** tile.
3. Click  adjacent to **Available Backups** and select **Configure Backups**.
4. In the Configure Backups dialog box, set the options to configure automated backups for the service instance.
 - a. In the **Schedule** section, set options to configure when automated backups are performed:

 **Note:**

All times must be for the Coordinated Universal Time (UTC) time zone, not your local time zone.

Option	Description
Full Backup	From the drop-down lists, select the day of the week and the time of day UTC when you want full backups to be performed.
Incremental Backup	From the drop-down list, select the time of day UTC when you want incremental backups to be performed.

- b. In the **Set new retention to** field, enter the number of days that you want new **incremental** backups to be retained.

Full backups are retained until their last related incremental backup is no longer available. For example, if two consecutive full backups are three days apart, the older full backup is retained two extra days. The additional retention period for full backups is fixed and you cannot change it.

The change affects only backups that are created after you save your configuration changes. The number of days that existing backups are retained is not affected.

5. Click **Save**.

Disable Backups for an Oracle SOA Cloud Service Instance

Use the Oracle SOA Cloud Service Console to disable automated backups.

You can also disable automated backups. To disable automated backups for an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to configure automated backups.
2. On the Overview page, click the **Administration** tile.

This exposes the **Backup** tab.

3. Click **Disable Backups**.

In the confirmation message screen, click **Disable Backups**.

Disable Coordinated Backups for an Oracle SOA Cloud Service Instance

Use the Oracle SOA Cloud Service Console to disable coordinated backups, that is, decouple Oracle SOA Cloud Service backups and DBaaS backups.

To disable coordinated backups for an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to update coordinated backups.
2. On the Overview page, click the **Administration** tile.

This exposes the **Backup** tab.

3. From the menu next to Available Backups, select **Configure Backups**.

In the Configure Backups dialog box, deselect the **Coordinated Backups** check box.

4. Click **Save**.

Note that DBaaS automatic backups can be initiated using the DBaaS scheduler and can no longer be initiated by Oracle SOA Cloud Service.

Delete a Backup

Use the Oracle SOA Cloud Service Console to delete a backup that you no longer require to release storage or prevent an Oracle SOA Cloud Service instance from being restored from the backup.


Note:

You can delete a full backup only if no incremental backups are linked to it. If you attempt to delete a full backup to which one or more incremental backups is linked, the attempt fails.

To delete a backup:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to delete a backup.
2. On the Overview page, click the **Administration** tile.

This exposes the **Backup** tab.

3. From the list of available backups, click the  menu for the backup and select **Delete**.

If you want to delete a full backup to which incremental backups are linked, you must delete or archive the linked backups first. If you attempt to delete a full backup to which one or more incremental backups is linked, the attempt fails.

For information about how to archive a backup, see “Archive and Download a Backup” in REST API for Oracle SOA Cloud Service.

4. When prompted, confirm that you want to delete the backup.

Initiate an On-Demand Backup of an Oracle SOA Cloud Service Instance

You can create a backup immediately without having to wait for the next scheduled backup.

Create a backup when making major changes to your service instance, for example, in these situations:

- Before any configuration changes that you may need to undo
- Before deploying an application
- After deploying an application

Note:

Do not attempt to start the administration server while a backup is in progress.

To initiate an on-demand backup of an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to configure automated backups.
2. On the Overview page, click the **Administration** tile.

This exposes the **Backup** tab.

3. Click **Back Up Now**.

The Back Up Now dialog box opens.

4. In the Back Up Now dialog box, set the following options:

Option	Description
Current retention period is	The number of days the backup will be retained. This value can be changed by clicking Configure Backups in the Backup tab.
Notes	Up to 255 characters of free-form text to provide additional information about the backup. This text is displayed in the Notes field for the backup in the list of available backups. Provide information to enable an administrator to determine when to restore from the backup, for example, why the backup was created, or the state of the service instance at the time of the backup.

5. Click **Back Up**.

The Backup page is updated to show that the backup is in progress.

While the backup is in progress, you cannot start any other management operation on the service instance.

When the backup is complete, it is added to the list of available backups on the Backup page.

Restore an Oracle SOA Cloud Service Instance from a Backup

You can restore an Oracle SOA Cloud Service instance from a backup to return the service instance to a particular state or recover the service instance after a loss of data.

Note:

If you restore a service instance's configuration files from a backup in which the hosts do not match the hosts in the service instance, Oracle SOA Cloud Service handles the mismatch as follows:

- If the service instance contains any managed server hosts that are not in the backup, Oracle SOA Cloud Service warns you that it cannot restore the managed server hosts that are not part of the backup.

Before trying to restore again, you can scale in the service instance to delete the nodes that correspond to these managed server hosts. See [Scale In an Oracle SOA Cloud Service Cluster](#).

If you choose to continue without scaling in the service instance, Oracle SOA Cloud Service asks you to confirm that you understand that the service instance will be scaled in automatically.

- If the backup contains any hosts that are not in the service instance, Oracle SOA Cloud Service does **not** attempt to remove the managed servers on these hosts from the administration server configuration. You must use Oracle WebLogic Server to remove the managed servers on these hosts from the administration server configuration.


After you restore a service instance's configuration files from a backup that does not match the service instance, you might need to modify the restored service instance to return it to the state you require. See [Return an Oracle SOA Cloud Service Instance to Service After Restoration from a Backup](#).

You can restore a service instance from an incremental backup without the need to restore the full backup to which the incremental backup is linked. In this situation, you are responsible for ensuring that the service instance is in a consistent state after the service instance is restored.

Restoration from a backup that is stored on block storage is faster than restoration from a backup that is stored in an Oracle Cloud Infrastructure Object Storage Classic container.

Before restoring an Oracle SOA Cloud Service instance from a backup, you must disable the load balancer for the service instance as explained in [Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance](#).

To restore an Oracle SOA Cloud Service instance from a backup:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to delete a backup.
2. On the Overview page, click the **Administration** tile, then the **Backup** tab.
3. From the list of available backups, click the  menu for the backup and select **Restore**.

 **Note:**

If you choose to restore from an incremental backup, you are responsible for ensuring that the service instance is in a consistent state after the service instance is restored.

4. In the dialog box, select the types of files that you want to restore and click **Restore**.

 **Note:**

You cannot use Oracle SOA Cloud Service to restore the database. To restore the database, you must use Oracle Database Cloud Service to restore from the associated database backup as identified by its RMAN tag. For instructions, see *Restoring from a Specific Backup* in *Administering Oracle Database Classic Cloud Service*.

The Backup page is updated to show that the restoration is in progress. While the restoration is in progress, you cannot start any other management operation on the service instance.

When the restoration is complete, it is added to the restoration history in the Backup page.

Return an Oracle SOA Cloud Service Instance to Service After Restoration from a Backup

After restoring an Oracle SOA Cloud Service instance from a backup, you must perform additional steps to return the service instance to service. You may also need to modify the service instance to return it to the state you require.

If a service instance has been scaled since a backup was created, the topology of the service instance and the topology of the backup no longer match. If you restore the service instance's configuration files from the backup, Oracle SOA Cloud Service handles such topology mismatches as follows:

- If the service instance contains any managed server hosts that are not in the backup, Oracle SOA Cloud Service warns you that it cannot restore the managed server hosts that are not part of the backup.

Before trying to restore again, you can scale in the service instance to delete the nodes that correspond to these managed server hosts.

If you choose to continue without scaling in the service instance, Oracle SOA Cloud Service asks you to confirm that you understand that the service instance will be scaled in automatically.

- If the backup contains any hosts that are not in the service instance, Oracle SOA Cloud Service does not attempt to remove the managed servers on these hosts from the administration server configuration. You must use Oracle WebLogic Server to remove the managed servers on these hosts from the administration server configuration.

You must also remove a restored service instance's transaction logs and enable the load balancer for the service instance to resume the handling of incoming requests.

To return an Oracle SOA Cloud Service instance to service:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance that you want to return to service after restoration.
2. On the Overview page, click the **Administration** tile.
This exposes the **Backup** tab.
3. Click the ► arrow to open the Restore History list.
4. Click the text **Status Completed** for the last successful restoration in the Restore History list.
A set of progress messages for the restoration is displayed.
5. Examine the progress messages to determine whether the backup contained any hosts that are not in the service instance.
6. If the backup contained any hosts that are not in the service instance, modify the service instance as follows:
 - a. Use Oracle WebLogic Server to remove the managed servers on these hosts from the administration server configuration.
 - b. If you require your service instance to contain the number of nodes in the backup, scale out the service instance.
7. If you scaled in the service instance to delete any nodes and you require your service instance to contain the number of nodes it contained before you restored it, scale out the service instance.
8. Remove the service instance's transaction records.
Oracle SOA Cloud Service does not provide any tools for removing a service instance's transaction records. Instead, use Oracle WebLogic Server for this purpose.
See:
 - [Access a VM Through a Secure Shell \(SSH\)](#)
 - "How to Remove Transaction Records" in *Developing JTA Applications for Oracle WebLogic Server* (12.2.1.4 | 12.2.1.3 | 12.2.1.2 | 12.1.3).
9. Enable the load balancer for the service instance as explained in [Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance](#).

Delete an Oracle SOA Cloud Service Instance

When you no longer require an Oracle SOA Cloud Service instance, you can delete it.


Only an administrator can delete a service instance, as described in [About Oracle SOA Cloud Service Roles and User Accounts](#).



Note:

When you delete an instance, everything is deleted, *including backups*.

To delete an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Delete**.
2. Enter the database administrator user name and password and click **Delete**.
The database itself is not deleted. Only the repository and schemas created for the Oracle SOA Cloud Service instance are deleted.
Once deleted, the Oracle SOA Cloud Service is removed from the list of service instances displayed on the Oracle SOA Cloud Service Console and storage and OCPUs are released..
3. (Optional) If you try to delete a service instance, and the service instance is not deleted properly, click the **Retry Delete** button to try to delete the service instance again.
Service instances are not deleted properly when failed resources are not cleaned up completely.
When you click **Retry Delete**, the software cleans up the fails resources and attempts to delete the service instance.
The **Retry Delete** button is displayed for as long as the failed resources exist. If this is the case, click the **Retry Delete** button and wait. Repeat this process for as long as the **Retry Delete** button is displayed.

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 hostname of the Managed Server.

See [Creating an SSH Tunnel to a Port in the Virtual Machine](#).

Change JVM Heap Size Settings

When you provision an Oracle SOA Cloud Service instance and specify a compute shape, the JVM heap size for WebLogic Server and Load Balancer processes is determined automatically.

Default Heap Sizes

The compute shape you select for a WebLogic Server cluster determines the availability of RAM on VMs in this cluster, and the amount of available RAM is used to determine the preset heap size for the JVM processes running on the VMs.

The following table shows the Oracle SOA Cloud Service JVM heap size settings for each compute shape.

Compute Shape	Min Heap Size	Max Heap Size	Configured Garbage Collector
OC1M	256 MB	10 GB	Garbage First (-XX:+UseG1GC)
OC2M	256 MB	24 GB	Garbage First (-XX:+UseG1GC)
OC3M	256 MB	24 GB	Garbage First (-XX:+UseG1GC)
OC4M	256 MB	24 GB	Garbage First (-XX:+UseG1GC)

Custom Heap Sizes

After provisioning a service instance, you can change the heap size using the WebLogic Server Administration Console. See these topics in *Administration Console Online Help for Oracle WebLogic Server*:

- Increasing the heap size for a Managed Server ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).
- Set Java options for servers started by Node Manager ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)). Specify the Java option to increase the heap size; for example: `-Xmx3g`.

The heap size is also set when you choose a shape for the load balancer. You cannot change the heap size for the load balancer.

Perform Database Operations for an Oracle SOA Cloud Service Instance

Topics:

- [Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database](#)
- [Tune the Database Parameters](#)
- [Discover the Default Database Password](#)
- [Change the Database Schema and Wallet Passwords](#)

Replace an Existing Oracle Cloud Infrastructure Database with a New Oracle Cloud Infrastructure Database



This topic applies only to Oracle Cloud Infrastructure.

Best Practices:

- This procedure is applicable only for Oracle SOA Cloud Service instances, not for Oracle Managed File Transfer Cloud Service 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 Cloud Service domain.
- You should already have an Oracle SOA Cloud Service environment provisioned with an Oracle Cloud Infrastructure 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 **SOADataSource** > **Configuration** tab > **Connection Pool** tab > **URL** field.

For example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=olddb-scan.subnetname.vcnname.oraclevcn.com) (PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=oldPDB.subnetname.vcnname.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](#).

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.vcnname.oraclevcn.com" SOATest_domain
```

7. Complete the following steps for all nodes of the Oracle SOA Cloud Service 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/
SOADDataSource-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/
OraSDPMDDataSource-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

```

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

- e. 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.vcnname.oraclevcn.com) (PORT=1521)))

```

```
(CONNECT_DATA=(SERVICE_NAME=newPDB.subnetname.vcnname.oraclevcn.com))
```

- f. Optionally, run the RCU utility to drop the old database schemas.

Tune the Database Parameters

When you subscribed to an Oracle Database Cloud Service instance, you selected the computing power for the instance's virtual machine from a list of supported Oracle CPU (OCPU) and processor RAM combinations. The values for some database initialization parameters are the same for the OC1M (1 OCPU, 15 GB RAM) and OC3M (4 OCPU, 60 GB RAM) combinations, which may cause performance issues. This section describes how to set these database parameters and perform additional tasks to improve performance.



Note:

If you modify database parameter settings from the default settings assigned during instance provisioning, you must restart the database for the new settings to take effect.

To tune the database parameters:

1. Connect with the `SYS` user account.
2. Execute the following SQL syntax in SQL*Plus:

```
SQL> alter system set distributed_lock_timeout = 1400 scope = spfile;  
alter system set Processes = 1500 scope = spfile;  
alter system set db_securefile = ALWAYS;
```

3. To achieve better throughput, resize the **redo log** to be 2 GB.
4. Create the data files for the Oracle SOA schema with the initial size equal to the maximum size allowed. Otherwise, data source-related errors are reported. For example:

```
SQLRecoverableException: IO Error: Socket read timed out
```

5. If you turn on the archive log for the database, the system can run out of connections for the `SOADatasource`. Its Maximum Capacity is set to 300 when the archive log mode is off. As a workaround, set the following parameters:
 - a. Set the **Maximum Capacity** for `SOADatasource` to 400.
 - b. Reduce the counts for the following worker managers:
 - Set the count for `SOAIncomingRequests_maxThreads` to 60.
 - Set the count for `SOAInternalProcessing_maxThreads` to 150.
6. Remove the expired archive files to prevent a disk full error.
 - a. Connect with the `SYS` user account.
 - b. Execute the following SQL syntax in SQL*Plus:

```
SQL> alter system set db_flashback_retention_target = 45 scope=both;  
restart DB
```

- c. Run the `delArch.sh` script shown below to periodically delete the expired archive log files.

```
#!/bin/sh
#####
##                                     ##
##          Purge Database Archive Logs          ##
##                                     ##
#####
source /home/oracle/.bashrc
test -z ${ORACLE_HOME} && echo "Please set ORACLE_HOME first"
&&
exit 1;
test ! -d ${ORACLE_HOME} && echo "Please make sure you have set
ORACLE_HOME correctly:
${ORACLE_HOME}" && exit 1;

#delete ${1} archivelog until time 'SYSDATE-1/(24*6)';
function rmArch(){
${ORACLE_HOME}/bin/rman target / <<EOF
crosscheck archivelog all;
delete ${1} archivelog until time 'SYSDATE-1/(24*6)';
YES
delete backup;
YES
delete datafilecopy all;
YES
exit
EOF
}

totalcount=0

#interval=${1:-1800}
interval=${1:-300}
while [ : ]
do
rmArch $2
ts=$(date)
let "totalcount=totalcount+1"
echo ""
echo ""
echo "====="
echo "=="                               "=="
echo "=="          SUMMARY          "=="
echo "=="                               "=="
echo "====="
echo ""
echo ""
tname='v${asm_diskgroup}';
tname2='v${recovery_file_dest}';
${ORACLE_HOME}/bin/sqlplus -s sys/syspassword as sysdba <<EOF

set feedback 0
set serveroutput on
```

```

execute dbms_output.put_line('Disk Group space usage (In GigaByte)');
col total format 999,999,999.00
col available format 999,999,999.00
SELECT ROUND(total_mb / 1024) "TOTAL", ROUND(free_mb / 1024 )
"AVAILABLE" FROM ${tname} ;

execute dbms_output.put_line('Archive Log space usage (In Gigabyte)');

col space_total format 999,999,999.00
col prc_used format 999,999,999.00
SELECT ROUND(SPACE_LIMIT / (1024*1024*1024))
SPACE_total,ROUND(((SPACE_USED / (1024*1024*1024)) * 100) /
(SPACE_LIMIT / (1024*1024*1024)), 2) PRC_USED FROM ${tname2};
EOF
echo "TotalCount: $totalcount"
echo "Last run at $ts"
echo "Will start another run in $interval seconds"
sleep $interval

done

```

Tune the Oracle WebLogic Server:

- Add the following JVM argument to the `Domain_Home/bin/setStartupEnv.sh` file:

```
-XX:ReservedCodeCacheSize=1024m
```

Discover the Default Database Password

After provisioning, database schemas are created with a default password.

To find the default database password:

1. Connect to the Administration Server VM through SSH. See [Connect to the Administration Server or Load Balancer VM](#).
2. Change to the `oracle` user.

```
sudo su - oracle
```

3. Enter the following command:

```
python /u01/app/oracle/tools/jcs/WLS/paas/bin/platform/python/pythonUtils/
atp_db_util.py generate-schema-password
```

4. In the command output, note the default password that was set by the provisioning script.

Change the Database Schema and Wallet Passwords

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

You must change the password for the Oracle schemas to meet Oracle security policies, corporate security policies or government regulations, or in response to a perceived security threat. By default, the password expires 180 days after your service instance is created.

Password expiration leads to the following scenarios:

- The following Oracle SOA Cloud Service instance-specific datasources fail:
 - EDNDataSource
 - mds-owsm
 - EDNLocalTxDataSource
 - mds-soa
 - OraSDPMDDataSource
 - SOADataSource
 - SOALocalTxDataSource
- The following non-Oracle SOA Cloud Service instance-specific datasources fail and the failure to connect to schemas might 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.

For Oracle SOA Cloud Service instances provisioned in Oracle Cloud Infrastructure Classic, to change the password for the Oracle Required Schemas found in the associated database (see [Database](#)):

- If the instance was created after November 2017 (release 18.2.5), you can use the Oracle SOA Cloud Service Console. See [Change the Database Schema Password Using the Oracle SOA Cloud Service Console](#).
- If the instance was created before November 2017 (release 18.2.5), you must directly modify the configuration of both the database and your WebLogic Server domain. See [Change the Database Schema Password Manually](#).

For Oracle SOA Cloud Service instances provisioned in Oracle Cloud Infrastructure, to change the password for the Oracle Required Schemas found in the associated database (see [Database](#)), you must directly modify the configuration of both the database and your WebLogic Server domain. See [Change the Database Schema Password Using the Oracle SOA Cloud Service Console](#).

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

**Note:**

The following schemas are updated during the update schema password operation:

Entity	Schema
WebLogic Server	IAU
	IAU_APPEND
	IAU_VIEWER
	MDS
	OPSS
	STB
	WLS
	WLS_RUNTIME
Oracle SOA Cloud Service	SOAINFRA
	UMS
	ESS
	MFT

**Note:**

If your service instance was created before November 2017 (release 18.2.5), you cannot use the Oracle SOA Cloud Service Console to change the schema password. You must perform these modifications manually on your service instance.

Topics:

- [Change the Database Schema Password Using the Oracle SOA Cloud Service Console](#)
- [Change the Database Schema Password Manually](#)
- [Update the DBFS Wallet Password](#)

Change the Database Schema Password Using the Oracle SOA Cloud Service Console




This topic applies only to Oracle Cloud Infrastructure Classic.

If you want to change the password for the Oracle Database schemas used by your Oracle SOA Cloud Service instance, and your service instance was created after November 2017 (release 18.2.5), then you can use the Oracle SOA Cloud Service console to change the Oracle schema password in the Oracle Database Classic Cloud Service deployment, and to update your service instance to use the new password.

To change the database schema password using the Oracle SOA Cloud Service Console:

1. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance whose schema password you want to change.
2. At the bottom of the Overview page, expand **Associations**.
3. From the list of associations for this service instance, identify the association with these characteristics:

- **Service Type** - Oracle Database Cloud Service
 - **Type** - Depends On
4. Click **Manage Association**  for this association, and then select **Update Database Credentials**.
This menu option is only available for the Infrastructure database association. It is not available for Application databases.
 5. Complete the following input fields:

Field	Description
Database Administrator Username	Enter the name of the system administrator for the selected database deployment.
Password	Enter the password for the database administrator.
New Schema Password	Enter a new password for the Oracle schemas in the selected database deployment. 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: \$, #, _.

6. Click **Update**.
You can monitor the operation's progress from this page or from the **Activity** page. Oracle SOA Cloud Service updates the database credentials, the WebLogic Server domain configuration, and the bootstrap credentials. If your service instance is running WebLogic Server 12.1.3, then all server processes are restarted as well.
7. Update the wallet password. See [Update the DBFS Wallet Password](#).

Change the Database Schema Password Manually

To change the password for the database schemas used by your Oracle SOA Cloud Service instance manually, you must modify the configuration of both the database and your WebLogic Server domain.

For Oracle SOA Cloud Service instances provisioned in Oracle Cloud Infrastructure Classic:

- If the instance was created after November 2017 (release 18.2.5), you can use the Oracle SOA Cloud Service Console to change the database schema password. See [Change the Database Schema Password Using the Oracle SOA Cloud Service Console](#).
- If the instance was created before November 2017 (release 18.2.5), you must use the manual steps provided here.

For Oracle SOA Cloud Service instances provisioned in Oracle Cloud Infrastructure, you must use the manual steps provided here.

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

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

2. If the WebLogic Servers are running and the WebLogic Server Administration Console is accessible, change the password for all the corresponding data sources from the Weblogic Server Administration Console.
3. If the WebLogic Servers are not running and WebLogic Server console is inaccessible, manually change the passwords in the WebLogic Server configuration.
4. Update the bootstrap credentials using the WebLogic Scripting Tool (WLST).
5. Start the Administration Server with the Node Manager, and then start the Managed Servers.

To change the database schema password manually:

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

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

- a. Use the `ssh` command to [connect to the Administration Server](#) and get the value of the schema prefix.

```
ssh -i private_key opc@IP_address_of_admin_server_VM  
cat /u01/app/oracle/private/schemaPrefix
```

The schema prefix value returned is similar to the following:
SP255951777

- b. Log in to the database deployment node.

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

- c. Connect to the database deployment.

```
sqlplus / as sysdba
```

Use the username provided when provisioning the database deployment.

If your database deployment is Oracle Database Classic Cloud Service 12c, the following step is also required:

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

Use the PDB name provided during Oracle SOA Cloud Service provisioning.

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

For Fusion Middleware 12.1.3	For Fusion Middleware 12.2.1.x
<code>schema_prefix_IAU</code>	<code>schema_prefix_DBFS</code>
<code>schema_prefix_IAU_APPEND</code>	<code>schema_prefix_ESS</code>
<code>schema_prefix_IAU_VIEWER</code>	<code>schema_prefix_IAU</code>
<code>schema_prefix_MDS</code>	<code>schema_prefix_IAU_APPEND</code>
<code>schema_prefix_OPSS</code>	<code>schema_prefix_IAU_VIEWER</code>
<code>schema_prefix_STB</code>	<code>schema_prefix_MDS</code>
	<code>schema_prefix_OPSS</code>
	<code>schema_prefix_SOAINFRA</code>
	<code>schema_prefix_STB</code>
	<code>schema_prefix_UMS</code>
	<code>schema_prefix_WLS</code>
	<code>schema_prefix_WLS_RUNTIME</code>

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

```
ALTER USER schema_prefix_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_IAU ACCOUNT UNLOCK;
```

 **Note:**

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

2. Update all the datasources from the WebLogic Server Administration Console to reflect the new password.
 - a. Log in to the WebLogic Administration Console and navigate to the Services — Datasources menu on the Domain Structure box.
 - b. Click **Lock & Edit**.
 - c. For each datasource, navigate to the Datasource Name — Configuration — Connection Pool tab and update the Password and Confirm Password field with the new password.
 - d. Click **Save**, then **Activate**.
 - e. Stop all the WebLogic Servers.

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

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

Proceed to Step 4.

3. If the WebLogic Server is not running or the Administration Console is not accessible:
 - a. Encrypt the new schema password and Update Data Source Configuration files:

```
ssh -i private_key opc@ipaddress_of_Admin_VM
sudo su oracle
cd /u01/data/domain/domain_name
```

Ensure WebLogic Servers are not running. If running, stop the processes:
Find the process IDs:

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

Kill processes:

```
kill -9 pid
```

then run:

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

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

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

- 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:

For Fusion Middleware 12.1.3	For Fusion Middleware 12.2.1.x
LocalSvcTblDataSource-jdbc.xml	EDNDataSource-jdbc.xml
opss-auditview-jdbc.xml	EDNLocalTxDataSource-jdbc.xml
mds-owsm-jdbc.xml	ess-oracle-int-jdbc.xml
opss-datasource-jdbc.xml	ess-oracle-jdbc.xml
opss-audit-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
	SOADDataSource-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](#):

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

- b. Change to the `oracle` user:

```
sudo su - oracle
```

- c. Start WLST:

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

- d. 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](#):

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

b. Change to the `oracle` user:

```
sudo su - oracle
```

c. Start WLST.

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

d. Connect to the Node Manager.

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

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

For 11g:

```
u01/app/oracle/middleware/wlserver_10.3/common/nodemanager/  
nodemanager.properties
```

For 12c:

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

- **Administration Server name** —

```
cd /u01/data/domains/domain_name/servers.
```

Look for the server name ending in `adminserver`.

Run the `nmConnect` command.

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

e. Start the Administration Server.

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

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

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

6. Update the wallet password. See [Update the DBFS Wallet Password](#).**7.** Restart the Oracle SOA Cloud Service instance from the [Oracle SOA Cloud Service Console](#). See [Stop, Start, or Restart an Oracle SOA Cloud Service Instance](#)

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 manually regenerate the DBFS wallet with a new password.

To update the wallet password:

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

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

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 temp file to store the `prefix_DBFS` user credentials. For example:

```
vi /var/tmp/dbfsp
```

In the file, enter:

6. Enter the new database credentials three times in the `dbfsp` file on three different lines. For example:

```
ab#$12CDaf40f1c  
ab#$12CDaf40f1c  
ab#$12CDaf40f1c
```

If you need to find out the default database credentials, see [Discover the Default Database Password](#).

7. Create a new wallet directory:

```
mkdir wallet
```

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.

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/middleware/dbclient
export LD_LIBRARY_PATH=/u01/app/oracle/middleware/dbclient/lib
export TNS_ADMIN=/u01/data/domains/SOACS_domain/dbfs
```

where `SOACS_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 the trace log files to ensure there are no errors:

```
/u01/app/oracle/middleware/dbclient/bin/dbfs_client -o wallet /
@ORCL -o direct_io /u01/soacs/dbfs_directio -otrace_file=/tmp/
db1.txt
/u01/app/oracle/middleware/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/soacs
```

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.

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 Cloud Service 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/ OraSDPMApDefRcvErrorQ1_auto	OraSDPM/Queues/ OraSDPMApDefRcvErrorQ1
dist_OraSDPM/Queues/ OraSDPMApDefRcvQ1_auto	OraSDPM/Queues/OraSDPMApDefRcvQ1
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
dist_OraSDPM/Queues/ OraSDPMEngineSndQ1_auto	OraSDPM/Queues/OraSDPMEngineSndQ1
dist_OraSDPM/Queues/ OraSDPMWSRcvQ1_auto	OraSDPM/Queues/OraSDPMWSRcvQ1

Settings for UMSJMSSystemResource

Configuration | Subdeployments | Targets | Security | Notes

This page displays general information about a JMS system module and its resources. It also allows you to configure new resources and access existing resources.

Name: UMSJMSSystemResource
The name of this JMS system module. [More Info...](#)

Scope: Global
Specifies if the JMS system module is accessible within the domain, a partition, or a resource group template. [More Info...](#)

Descriptor File Name: jms_ums_jmsSystemResource-jms.xml
The name of the JMS module descriptor file. [More Info...](#)

This page summarizes the JMS resources that have been created for this JMS system module, including queue and topic destinations, connection factories, JMS templates, destination sort keys, destination quota, distributed destinations, foreign servers, and store-and-forward parameters.

[Customize this table](#)

Summary of Resources

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	Type	JNDI Name	Subdeployment	Targets
dist_OraSDPM/Queues/OraSDPMApDefRcvErrorQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMApDefRcvErrorQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMApDefRcvQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMApDefRcvQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMDriverDefSndQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMDriverDefSndQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMEngineCmdQ_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMEngineCmdQ	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMEnginePendingRcvQ_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMEnginePendingRcvQ	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMEngineRcvQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMEngineRcvQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMEngineSndQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMEngineSndQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
dist_OraSDPM/Queues/OraSDPMWSRcvQ1_auto	Uniform Distributed Queue	OraSDPM/Queues/OraSDPMWSRcvQ1	UMSJMSSubdeployment	UMSJMSServer_auto_1, UMSJMSServer_auto_3
OraSDPM/QueueConnectionFactory	Connection Factory	OraSDPM/QueueConnectionFactory	Default Targeting	slc12ma_cluster
Priority	Destination Key	N/A	N/A	N/A

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.

Create the User Messaging Service JMS Server

On a cluster, you would 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.

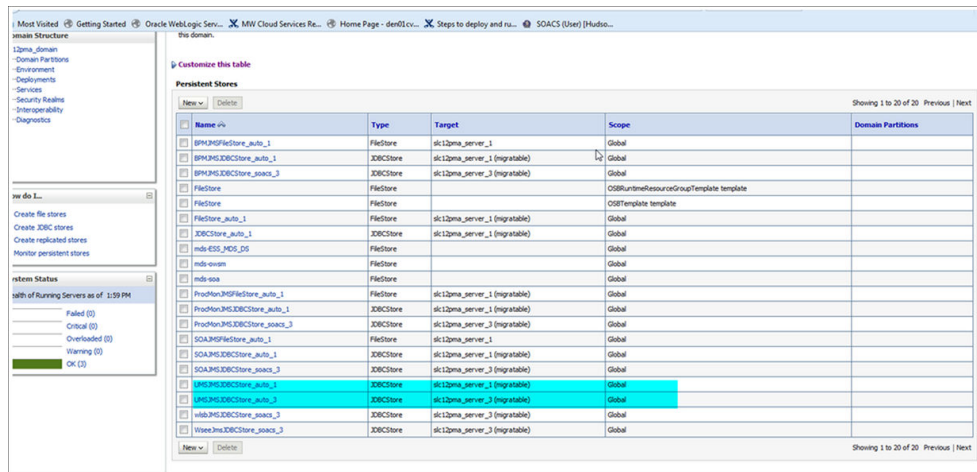
JMS Servers (Filtered - More Columns Exist)						
Click the <i>Lock & Edit</i> button in the Change Center to activate all the buttons on this page.						
Name	Persistent Store	Target	Current Target	Health	Scope	Domain Partitions
BPMJMServer_auto_1	BPMJMSJDBCStore_auto_1	slc12pma_server_1 (migratable)	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	
wljbJMServer	FileStore				OSRuntimeResourceGroupTemplate template	
wljbJMServer	FileStore				OSSTemplate template	
wljbJMServer_auto_1	JDBCStore_auto_1	slc12pma_server_1 (migratable)	slc12pma_server_1	OK	Global	
wljbJMServer_soacs_3	wljbJMSJDBCStore_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**.



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 UMS Adapter 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.

- Restart the Administration Server and Managed Servers from the Oracle SOA Cloud Service Console. See [Restart the Administration Server VM](#) and [Stop, Start, or Restart Managed Server and Load Balancer VMs](#).

Component Name	Installed	Status	Resource Adapter	Cluster	Scope
SocketAdapter	Installed		Resource Adapter		Global
state-management-provider-memory-rar	Active	✔ OK	Resource Adapter	slc12pma_adminserver, slc12pma_cluster	Global
SOAPAdapter	Active	✔ OK	Resource Adapter	slc12pma_cluster	Global
usermessagingdriver-apns	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-email	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-extension	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-gcm	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-mpmp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-twitter	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingdriver-xmpp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
usermessagingserver	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
worklistapp	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global
wsn-gm	Active	✔ OK	Enterprise Application	slc12pma_cluster	Global

Configure Mail Sessions

You can configure the User Messaging Service to send emails to SSL-configured external mail servers using Oracle SOA Cloud Service 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 Cloud Service 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 Cloud Service instances using IP networks, verify if pinging 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 Cloud Service 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 Cloud Service Instance

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

 **Note:**

To import a CA-issued SSL certificate to the load balancer, see [Import a CA-Issued SSL Certificate to the Load Balancer](#).

1. Log in to the Admin server node as an Oracle user.
2. Execute the following `openssl` command:

Email Server	Command Used
Yahoo	<code>openssl s_client -connect smtp.mail.yahoo.com:465 > yahoocert.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>
Gmail	<code>openssl s_client -connect smtp.gmail.com:465 > 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 case of **Office 365**, two certificates are presented. Run the following command to display the certificates:

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

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

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

```
keytool -import -alias smtp.yahoo.com -keystore /u01/app/oracle/
middleware/wlserver/server/lib/DemoTrust.jks -file yahoo.cer -storepass
DemoTrustKeyStorePassPhrase
```

 **Note:**

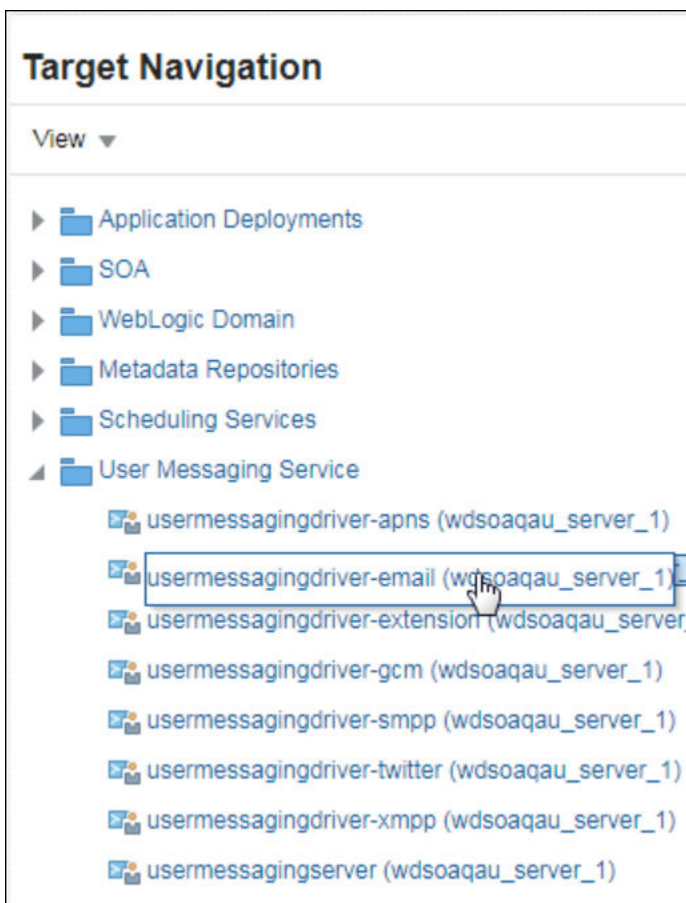
For SOA 12.2.1.2 users, the trust store being used may be KSS. In `setDomainEnv.sh` verify if there is an entry for **Demotrust.jks**. Else, follow these steps to add the certificate to KSS:

- a. Log in to Oracle Enterprise Manager Fusion Middleware Control Console.
 - b. Expand the Weblogic Domain and navigate to **Security** and then **Keystore**.
 - c. Click the arrow next to **system**, select **trust** and then click **Manage** to manage the certificates in the trust keystore.
 - d. Click **Import**. The Import Certificate dialog is displayed.
 - e. In the Certificate Type, select **Trusted Certificate**, enter a unique alias, paste the certificate string or browse for the certificate file, and click **OK**.
5. Restart the Administration Server and Managed Servers from the Oracle SOA Cloud Service Console. See [Restart the Administration Server VM](#) and [Stop, Start, or Restart Managed Server and Load Balancer VMs](#).

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.

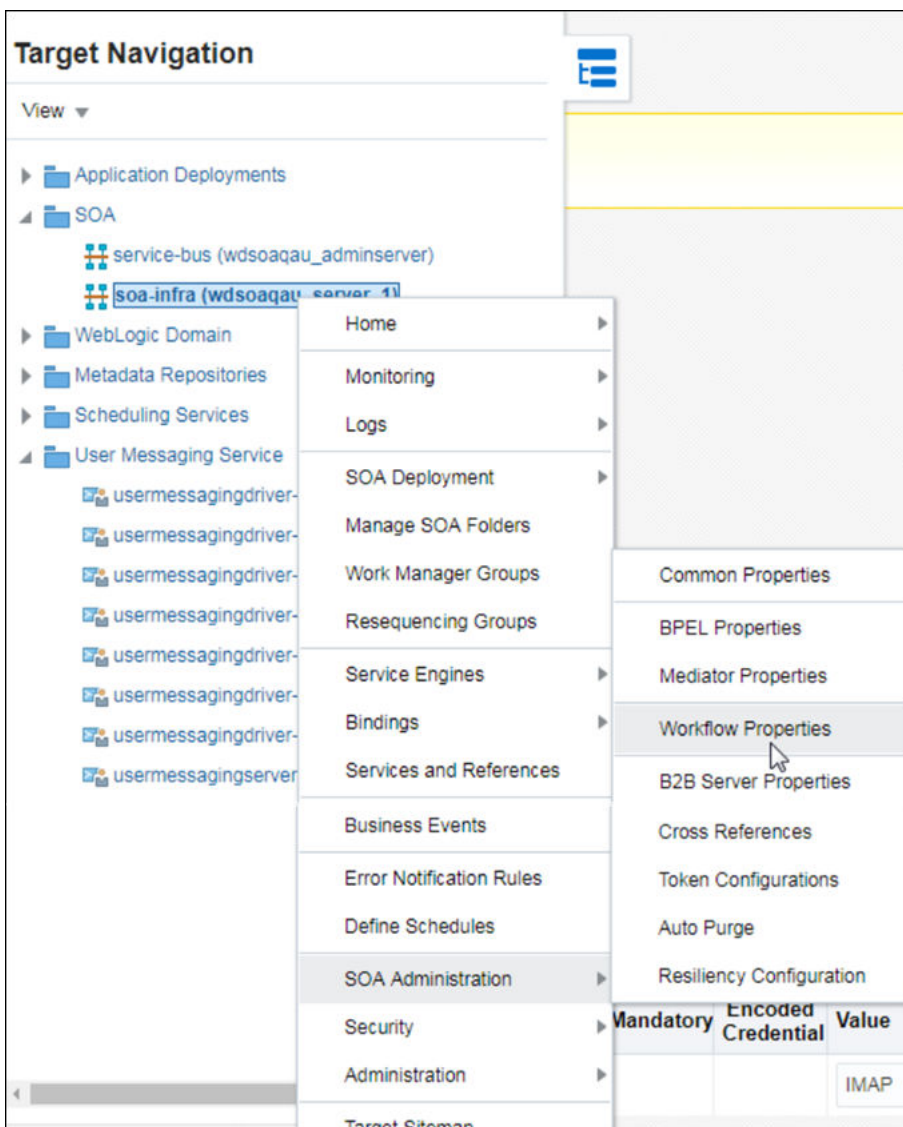
 **Note:**

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.



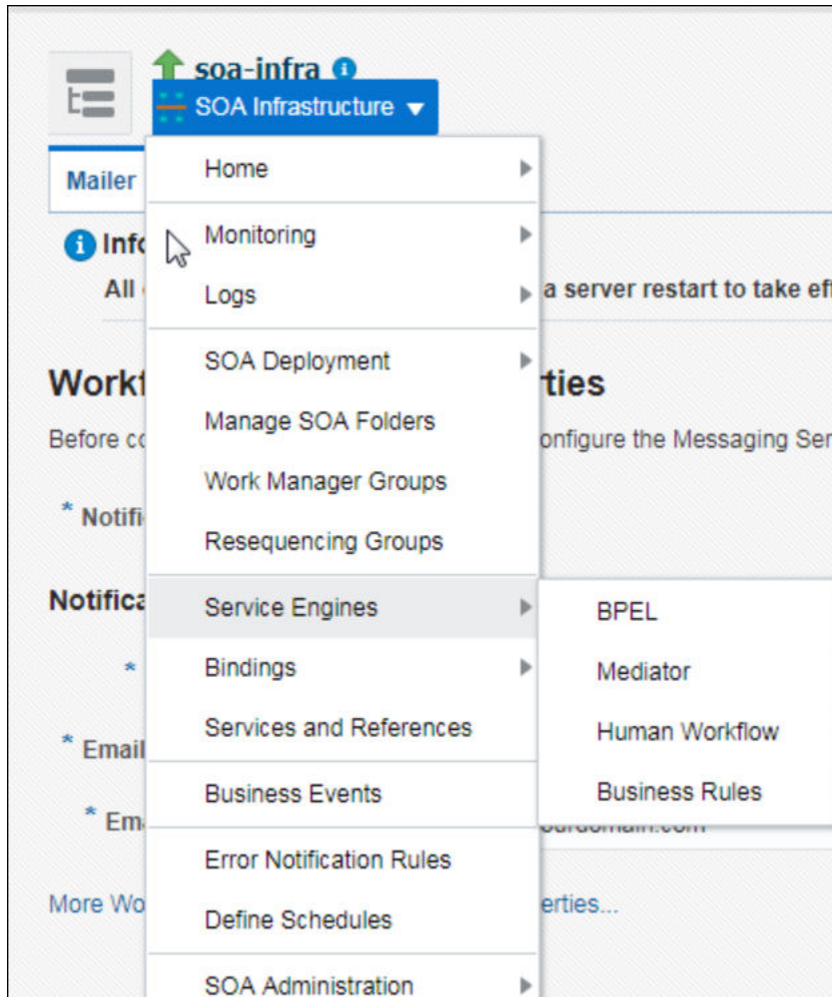
5. Click **Apply**.

Verify Mail Configuration Settings

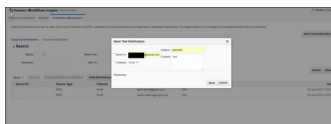
You can test your mail server configuration by sending a test mail.

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 happens to the intended recipient

7

Secure an Oracle SOA Cloud Service Instance

Security in Oracle SOA Cloud Service spans many topics, including authentication, authorization, password management, and network security.

Topics:

- [About Security in Oracle SOA Cloud Service](#)
- [About Authenticating Users](#)
- [Configure Network Security](#)
- [Import Certificates of External Web Services with HTTPS in Oracle SOA Cloud Service](#)

About Security in Oracle SOA Cloud Service

You can secure applications deployed to your Oracle SOA Cloud Service instance through the capabilities of Oracle Cloud and Oracle WebLogic Server.

An Oracle SOA Cloud Service 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 Cloud Service 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.

About Authenticating Users

Oracle SOA Cloud Service is comprised of multiple components, each with its own identity stores, authentication options and administrative tools.

Topics:

- [About Users in Oracle SOA Cloud Service](#)
- [About Authentication Options](#)
- [Manage Passwords for Oracle SOA Cloud Service](#)
- [Relocate Oracle SOA Cloud Service to a Different Identity Domain](#)

About Users in Oracle SOA Cloud Service

There are multiple types of users associated with Oracle SOA Cloud Service. Each has its own purpose and is found in a specific identity store.

Cloud Users

When an Oracle Cloud account is created that includes Oracle SOA Cloud Service, the default administrator is given the SOA Administrator role. Only Oracle Cloud users with this role can create and manage Oracle SOA Cloud Service instances with either the console, CLI or REST API. Users in your account who have the Identity Domain Administrator role can create additional cloud users and grant them the SOA Administrator role. Similar roles exist for the other services available in Oracle Cloud. For more information, refer to:

- Add Users, Assign Policies and Roles in *Getting Started with Oracle Cloud*
- For Oracle Cloud Infrastructure: [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation
- For Oracle Cloud Infrastructure Classic: Managing Users, User Accounts, and Roles in *Managing and Monitoring Oracle Cloud*

Oracle SOA Cloud Service stores backups of service instances in Oracle Cloud Infrastructure Object Storage Classic. Consequently, each service instance is also configured with the credentials for an Oracle Cloud user who has read/write access to Oracle Cloud Infrastructure Object Storage Classic. See [About Backup and Restoration of Oracle SOA Cloud Service Instances](#).

WebLogic Server Administrators

An Oracle SOA Cloud Service 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. When you create a service instance you provide the credentials for the initial user in this WebLogic security realm. This user has the Administrator role and can perform all WebLogic Server administrative operations through either the WebLogic Server Administration Console, Fusion Middleware Control, WebLogic Scripting Tool (WLST) or WebLogic REST API. You can also use the default WebLogic administrator to create additional WebLogic administrators and assign them specific roles and privileges. For example, users with the Deployer role can deploy SOA applications to the domain.

By default, the domain in an Oracle SOA Cloud Service instance is configured to use the embedded LDAP identity store for WebLogic Server roles, users and policies. This embedded LDAP is hosted in the Administration Server and is replicated to all Managed Servers in the domain. If the default security configuration does not meet your requirements, you can modify the default security realm or create a new one with any combination of WebLogic and custom security providers. To learn more about WebLogic security, see [Understanding Security for Oracle WebLogic Server \(12.2.1.4 | 12.2.1.3 | 12.2.1.2 | 12.1.3\)](#).

Application Users

SOA applications deployed to the WebLogic Server domain in your Oracle SOA Cloud Service instance can have security policies that protect the applications against unauthorized access. WebLogic Server supports various security providers that assign an identity to the requesting user or software entity. For example, WebLogic Server can determine the identity of an application user by validating a user name and password.

By default, the domain in an Oracle SOA Cloud Service instance is configured to use the embedded LDAP identity store for both WebLogic administrators and application users. You can use standard WebLogic tools like the WebLogic Server Administration Console to manage users, groups, roles and policies in the embedded LDAP.

If the default security configuration does not meet your requirements, you can modify the default security realm or create a new one with any combination of WebLogic and custom security providers. For large production applications, Oracle recommends that you use a proper identity management system such as Oracle Identity Management instead of the embedded LDAP.

Database Users

An Oracle SOA Cloud Service instance requires access to at least one Oracle database. Oracle SOA Cloud Service provisions your chosen database with the Oracle Fusion Middleware (FMW) schema and also connects the WebLogic Server domain in your service instance to this database. When you create a service instance you provide appropriate credentials to access and update this FMW database.

You can also connect your service instance to additional relational databases by using standard WebLogic tools like the WebLogic Server Administration Console. Just as with the FMW database, you must provide the necessary credentials to connect to these application databases.

 **Note:**

If your database is running Oracle Database 12c, users can be scoped to the container database (CDB) or a pluggable database (PDB). To connect to a specific PDB from WebLogic Server, be sure to specify user credentials in the target PDB and not the CDB.

To learn more about database connectivity in WebLogic Server see *Administering JDBC Data Sources for Oracle WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

A component of your WebLogic Server domain is Oracle Platform Security Services (OPSS), which requires a connection to your service instance's FMW database. The credentials for this database connection are stored in a separate file named `jps-config.xml`.

Load Balancer Administrators

Your Oracle SOA Cloud Service instance can optionally include a load balancer running Oracle Traffic Director. The load balancer distributes application traffic to the servers in the WebLogic Server domain. Traffic Director has an Administration/Managed server architecture similar to WebLogic Server, along with its own identity store. When you create a service instance, the same WebLogic Server administrator credentials that you provide are also used as the default Traffic Director credentials. This user has full administrative access to the Load

Balancer console and other Traffic Director tools. You can also use the Load Balancer console to create additional Traffic Director administrators. See [Control and Configure an Oracle Traffic Director Load Balancer for an Oracle SOA Cloud Service Instance](#).

VM OS Users

Each Oracle SOA Cloud Service instance is associated with a Secure Shell (SSH) public key. Using the matching private key, you can SSH to the underlying virtual machines (VMs) running WebLogic Server and the load balancer. SSH to a VM as the `opc` OS user and then switch to the `oracle` OS user in order to manage Oracle SOA Cloud Service software like WebLogic Server, or to install additional Oracle software. The `opc` user has root privileges to the OS if you need to modify the OS configuration, create additional OS users, or install additional OS packages. See [Access a VM Through a Secure Shell \(SSH\)](#).

About Authentication Options

Get an overview of the different ways in which you can determine the identity of a user or system that is accessing an application running in Oracle SOA Cloud Service. Clients can authenticate against an external LDAP or database, or their identities can be validated with different token technologies like SAML.

By default, cloud users and application users are managed by different security frameworks and are located in different identity stores. Consequently, these users support different authentication options.

Single Sign-On (SSO) is the ability for a user to authenticate once and then gain access to many different application components, even though these components may have their own authentication schemes. SSO enables users to login securely to all their applications, web sites and mainframe sessions with just one identity.

Cloud Authentication

In order to create and manage cloud services such as Oracle SOA Cloud Service, Oracle Cloud users are authenticated against a specific identity domain and with a username and password. See "Cloud Users" in [About Users in Oracle SOA Cloud Service](#).

WebLogic Server Authentication

An Oracle WebLogic Server domain defines a security realm that controls authentication, authorization, role mapping, credential mapping and security auditing across all of the servers in the domain. These services are implemented as *security providers*. WebLogic Server includes many types of built-in providers and you can also build your own. Authentication providers in particular establish trust for a user by validating credentials or tokens. They can also identify any groups to which the user belongs, in order to make access decisions.

You can also configure multiple authentication providers in a single security realm. For example, consider a scenario in which the WebLogic Server administration users are located in one LDAP while application users are found in a different LDAP.

This table describes some of the authentication options available in a WebLogic Server security realm.

Authentication Option	Description
Embedded LDAP (default)	<p>Each user's credentials and group memberships are maintained in an Lightweight Directory Access Protocol (LDAP) server that is hosted in the domain's Administration Server and replicated to all Managed Servers in the domain. Oracle does not recommend using the embedded LDAP for large production applications.</p> <p>See "Managing the Embedded LDAP Server" in <i>Administering Security for Oracle WebLogic Server</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).</p>
External LDAP	<p>WebLogic Server includes authentication providers that are compatible with Oracle Internet Directory, Microsoft Active Directory, iPlanet, Open LDAP or any other LDAP-compliant server. These providers differ primarily in how they are configured by default to match typical directory schemas for their corresponding LDAP server.</p> <p>If this LDAP server is hosted outside of the VMs in your Oracle SOA Cloud Service instance, you may need to enable network communication between your VMs and the LDAP server. See Manage Access Rules for an Oracle SOA Cloud Service Instance.</p> <p>See "Configuring LDAP Authentication Providers" in <i>Administering Security for Oracle WebLogic Server</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).</p>
Relational Database	<p>WebLogic Server includes authentication providers that use a relational database as a data store for users, passwords and groups. These providers are configured by default with a typical SQL database schema to support these entities, but you can also customize this default configuration to match your database's existing schema.</p> <p>To use the database authentication providers, you must create a data source in the domain to establish connectivity to the database. If you selected this database when you created your Oracle SOA Cloud Service instance, a data source already exists. If this database is hosted outside of the VMs in your Oracle SOA Cloud Service instance, you may need to enable network communication between your VMs and the database.</p> <p>See:</p> <ul style="list-style-type: none"> • Manage Access Rules for an Oracle SOA Cloud Service Instance • "Configuring RDBMS Authentication Providers" in <i>Administering Security for Oracle WebLogic Server</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3)
SAML	<p>In perimeter authentication, a system outside of WebLogic Server establishes trust through tokens. WebLogic Server can generate and consume Security Assertion Markup Language (SAML) tokens (assertions), and supports both SAML 1.1 and SAML 2.0.</p> <p>See in <i>Administering Security for Oracle WebLogic Server</i>:</p> <ul style="list-style-type: none"> • Configuring Identity Assertion Providers (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3) • Configuring Single Sign-On with Web Browsers and HTTP Clients Using SAML (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3)

Manage Passwords for Oracle SOA Cloud Service

You may need to update the various credentials used to run a service instance, in order to meet corporate security policies or government regulations, or in response to a perceived security threat.

The specific tools and procedures you use to modify passwords depends on the type of user and where it is stored in the environment. In addition, there are consequences to changing

certain system users because other resources in the environment use these credentials as well.

For general information about users, see [About Users in Oracle SOA Cloud Service](#).

User	Updating the Password	Updating Dependencies
Cloud User	<p>To update your Oracle Cloud password, see Change and Manage Your Passwords in <i>Getting Started with Oracle Cloud</i>.</p> <p>If you are an Identity Domain Administrator, you can reset other users' passwords. See Resetting User Passwords in <i>Managing and Monitoring Oracle Cloud</i>.</p>	<p>When you create an Oracle SOA Cloud Service instance you provide the location of an Oracle Cloud Infrastructure Object Storage Classic container along with credentials to access and update backup files in this storage container. If you change the password for this cloud user, you also need to update the backup configuration of your service instance. Otherwise, automated and manual backups may fail.</p> <p>See Configure Automated Backups for an Oracle SOA Cloud Service Instance.</p>
WebLogic Server Administrator	<p>By default your Oracle WebLogic Server domain is configured to use the embedded LDAP security provider as the identity store for users, passwords and groups. This includes the WebLogic Server administrator user whose credentials you initialize when you create the Oracle SOA Cloud Service instance.</p> <p>You can use any available WebLogic Server tools to modify user credentials in the embedded LDAP, including the Administration Console, WLST and REST API. To use the Administration Console, see "Modify Users" in Administration Console Online Help for Oracle WebLogic Server (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).</p>	<p>Administrative credentials are required in order to boot the servers in your domain. A boot identity file is a text file that contains encrypted user credentials for starting and stopping an instance of WebLogic Server. If you change the password for this user, you must also update any boot identity files that use the same credentials. These files are located on the VM file system. Replace the current encrypted password with your new password. Otherwise, servers may fail to boot if you attempt to restart them.</p> <p>See "Boot Identity Files" in Administering Server Startup and Shutdown for Oracle WebLogic Server (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).</p> <p>For information on using SSH to access Oracle SOA Cloud Service VMs, see Access a VM Through a Secure Shell (SSH).</p>

User	Updating the Password	Updating Dependencies
Load Balancer Administrator	<p>If you add a load balancer to your Oracle SOA Cloud Service instance when you initially create it, the load balancer is configured with the same credentials as the WebLogic Server administrator. If you add a load balancer at a later time, you have the option to provide different credentials. In either case use the Load Balancer Console to change this user's password.</p> <p>For service instances running Oracle Traffic Director 12c, see Configure WebLogic Server Users in <i>Administering Oracle WebLogic Server with Fusion Middleware Control</i>. Be sure to access the console for the load balancer, and not for the WebLogic Server domain.</p> <p>For service instances running Oracle Traffic Director 11g, see Securing Access to the Administration Server in <i>Oracle Traffic Director Administrator's Guide</i>.</p>	None
Database User	<p>The Oracle WebLogic Server domain in an Oracle SOA Cloud Service instance is automatically configured with several JDBC data sources. Each data source connects to an Oracle Database Classic Cloud Service database deployment. You specify the database name and credentials for these data sources when you create the service instance.</p> <p>If you modify the password for one of the database users, the data sources in the WebLogic domain may fail to connect to the database. Use one of the standard WebLogic administrative interfaces to modify the connection properties of the existing data sources. See "Configuring JDBC Data Sources" in <i>Administering JDBC Data Sources for Oracle WebLogic Server</i> (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3).</p>	<p>When you create a service instance, you select one database deployment to host the Oracle Required Schema and you provide appropriate database credentials. If you modify the password of this database user, you must perform an additional task. Use the WebLogic Scripting Tool (WLST) to execute the <code>modifyBootStrapCredential</code> command and then restart the Administration Server.</p> <pre>modifyBootStrapCredential (jpsConfigFile='/u01/data/ domains/<i>DOMAIN_NAME</i>/ config/ fmwconfig/jps- config.xml', username='SCHE MA_PREFIX_OPSS', password='NEW_PASSWORD')</pre>

User	Updating the Password	Updating Dependencies
Application User	<p>By default your Oracle WebLogic Server domain is configured to use the embedded LDAP security provider as the identity store for users, passwords and groups. This includes any custom application users you've defined.</p> <p>You can use any available WebLogic Server tools to modify user credentials in the embedded LDAP, including the Administration Console, WLST, and REST API. To use the Administration Console, see "Modify Users" in <i>Administration Console Online Help for Oracle WebLogic Server (12.2.1.4 12.2.1.3 12.2.1.2 12.1.3)</i>.</p> <p>Alternatively, you can customize your WebLogic domain to use other security providers for users and passwords, such as a database or an LDAP server. In general, you do not use WebLogic Server to directly modify user credentials in these external identity stores. Instead use the native administrative tools offered by these resources. For more information about security providers, see About Authentication Options.</p>	None

Relocate Oracle SOA Cloud Service to a Different Identity Domain



This topic does not apply to Oracle Cloud at Customer.

An Oracle Cloud account administrator has the ability to move your Oracle SOA Cloud Service entitlement to another identity domain in the same account.

When you activate an order in Oracle Cloud, services in the order are typically activated in a default identity domain within the account. If necessary you can relocate Oracle SOA Cloud Service from one identity domain to another. However, you must delete any existing service instances prior to relocating the service.

See *Relocating a Service Entitlement to Another Identity Domain* in *Managing and Monitoring Oracle Cloud*.

During the relocation process, the service administrator will be added to the target identity domain but other Oracle Cloud users and administrators will not. The identity domain administrator will need to create any other users and administrators in the target identity domain, and to assign them the appropriate roles. If applicable, the bulk user import and role assignment features can be used for this task. For more information, see:

- [Add Users, Assign Policies and Roles](#) in *Getting Started with Oracle Cloud*

- For Oracle Cloud Infrastructure: [Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console](#) in the Oracle Cloud Infrastructure documentation.
- For Oracle Cloud Infrastructure Classic: Managing Users, User Accounts, and Roles in *Managing and Monitoring Oracle Cloud*

Configure Network Security

By default, an Oracle SOA Cloud Service instance is accessible only through secure protocols like SSL and SSH, and only using specific ports. But you're able to customize the default security configuration to support different access rules and security policies.

To provide the highest level of network security, Oracle SOA Cloud Service implements an "access by exception" architecture. You must explicitly grant network access to your service instance for administrators, application users or other cloud services. Similarly, if you want your service instance to be accessible over a non-secure protocol like HTTP, you must change the default configuration.

Topics:

- [About the Default Access Ports](#)
- [Manage Access Rules for an Oracle SOA Cloud Service Instance](#)
- [Enable HTTP Access to an Oracle SOA Cloud Service Instance](#)
- [Enable Communication Between Oracle SOA Cloud Service Instances](#)
- [Configure SSL for an Oracle SOA Cloud Service Instance](#)

About the Default Access Ports

To use Oracle resources through Oracle SOA Cloud Service, access them through the default ports.

Ports Available from Within the Oracle Cloud Network

Resource	Protocol	Default Port for Release 16.4.5 and Earlier	Default Port for Release 17.1.3 and Later
Oracle WebLogic Server Administration Console	HTTP	7001	9071
Oracle Fusion Middleware Control	HTTP	7001	9071
Managed Server	HTTP	8001	9073
	HTTPS	8002	9074
Database	SQL Net	1521	1521

Ports Available from Outside the Oracle Cloud Network

Resource	Protocol	Default Port
Oracle WebLogic Server Administration Console	HTTPS	7002

Resource	Protocol	Default Port
Oracle Fusion Middleware Control	HTTPS	7002
Oracle Traffic Director Administration Console	HTTPS	8989
End user applications when the load balancer is enabled	HTTP	80*
	HTTPS	443
End user applications when the load balancer is disabled and there are multiple managed servers	HTTP	9073*
	HTTPS	9074
End user applications when the load balancer is disabled and there is only one managed server	HTTP	80*
	HTTPS	443
Service instance VM	SSH	22
Oracle Traffic Director VM	SSH	22

The diagram in About the Deployment Topology in *Administering Oracle Java Cloud Service* illustrates port allocation in an Oracle SOA Cloud Service VM deployment topology.



Note:

If a service instance is created with the Create New Oracle SOA Cloud Service Instance wizard, the HTTP port is disabled. You cannot enable the HTTP port for such a service instance through any of the interfaces to Oracle SOA Cloud Service, such as the Service Console or the REST API.

* For end user applications, the default ports depend on how the service instance was created:

If the service instance was created by using the Create New Oracle SOA Cloud Service Instance wizard, the default ports are as follows:

- If a load balancer is enabled, the HTTP port is disabled and the HTTPS port is 443 by default.
- If a load balancer is not present and the service instance contains more than one managed server, the HTTP port is disabled and the HTTPS port is 8002/9074.
- If a load balancer is not present and the Oracle SOA Cloud Service instance contains only one managed server, the server ports are 443 for HTTPS and disabled for HTTP.

If the service instance was created by using the REST API, the default ports are as follows:

- If a load balancer is present, the default ports for applications are 80 for HTTP and 443 for HTTPS. You can reconfigure these ports.
- If a load balancer is not present and the Oracle SOA Cloud Service instance contains more than one managed server, the default ports are 8001/9073 for HTTP and 8002/9074 for HTTPS.

- If a load balancer is not present and the Oracle SOA Cloud Service instance contains only one managed server, the managed server ports are set to 80 and 443 respectively. You can reconfigure these ports.

You can continue to use HTTPS port 8081 to access an application running on an existing service instance that was created by using the Create New Oracle SOA Cloud Service Instance wizard. In this case, HTTP port 8080 is disabled and you can no longer use this port to access your application.

For information about creating a service instance by using the REST API, see [Provision a New Service Instance](#) in *REST API for Oracle SOA Cloud Service*.

Accessing Oracle SOA Cloud Service URLs Externally Using a Public IP Address

Oracle SOA Cloud Service URLs can be accessed externally using a public IP address. Use port 80 with the HTTP protocol and port 443 with the HTTPS protocol. This redirects access to port 8001. For example, to access the B2B console using HTTPS:

```
https://public_IP_address:443/b2bconsole
```

Manage Access Rules for an Oracle SOA Cloud Service Instance

Access rules enable you to control network access to the VMs that make up your Oracle SOA Cloud Service instance. Each rule has a source, a destination, a destination port and a transport protocol.

For example, you can create an access rule that enables:

- A database VM to access a specific port on your Managed Server VMs
- Public Internet access to a specific port on the Administration Server VM

Oracle SOA Cloud Service creates several *default* rules on a new service instance, such as public access to the Administration Server and load balancer VMs on port 22 (SSH). Some of these are *system* rules, which cannot be disabled. Do not modify or delete system generated access rules that are marked **DO NOT MODIFY**. For information about the default access ports in a service instance, see [About the Default Access Ports](#).

Prior to creating an access rule, ensure that the destination VM is configured to listen on the chosen ports. For example, on VMs running Oracle WebLogic Server you can configure network channels to control the listen ports for your Administration Server and Managed Servers. Refer to "Configuring Network Resources" in *Administering Server Environments for Oracle WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

Topics:

- [Manage Access Rules for Instances in Oracle Cloud Infrastructure](#)
- [Manage Access Rules for Instances in Oracle Cloud Infrastructure Classic](#)

Manage Access Rules for Instances in Oracle Cloud Infrastructure



This topic does not apply to Oracle Cloud Infrastructure Classic.

Before you start creating an access rule in Oracle Cloud Infrastructure, gather the following details:

- The region in which the pod is being provisioned such as **us-ashburn-1** or **us-phoenix-1**

- Oracle Cloud Infrastructure Console login details:
 - Oracle Cloud Infrastructure login URL.
For example: `https://console.us-ashburn-1.oraclecloud.com`
 - Cloud tenant name.
For example: `oic1`
 - User ID and password.
- Compartment name.

To create an access rule for an Oracle SOA Cloud Service instance in Oracle Cloud Infrastructure:

1. Navigate to the Oracle Cloud Infrastructure Console.
For example: `https://console.us-ashburn-1.oraclecloud.com`.
2. Enter the **Cloud Tenant** name.
For example: `oic1`.
3. Enter the **User Name** and **Password**.
4. Open the navigation menu and click **Compute**. Under **Compute**, click **Instances**.
5. Select the compartment name from the list. For example:
ManagedCompartmentForPaas.
In the selected compartment, you will see available instances.
6. Click your instance to view its details. In the instance details page, click the **subnet** link.
7. In the list of subnets, locate the subnet your instance was created in and click any security list next to the subnet.
8. On the Security Lists page, click **Edit All Rules**.
9. Add an ingress rule for port 7522 by setting the values as follows:
 - **Source Type** – CIDR
 - **Source CIDR** – 0.0.0.0/0
 - **IP Protocol** – TCP
 - **Source Port Range** – All
 - **Destination Port Range** - 7522
10. Click **Save Security List Rules** to save the security rules.

 **Note:**

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

Manage Access Rules for Instances in Oracle Cloud Infrastructure Classic



This topic applies only to Oracle Cloud Infrastructure Classic.

Topics:

- [Create a New Access Rule](#)
- [Enable or Disable an Access Rule](#)
- [Delete an Access Rule](#)

Create a New Access Rule



This topic applies only to Oracle Cloud Infrastructure Classic.


To control network access to the nodes in your Oracle SOA Cloud Service instance, you can define access rules.



Note:

See also [Security Lists](#) in the Oracle Cloud Infrastructure documentation.


To create a new access rule for an Oracle SOA Cloud Service instance:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Access Rules**.
The Access Rules page is displayed, showing the list of all access rules.
2. Click **Create Rule**.
The **Create Access Rule** dialog is displayed.
3. Specify a unique **Rule Name**. Optionally, specify a rule **Description**.
The name must begin with a letter, and can contain numbers, hyphens, or underscores. The length cannot exceed 50 characters. When you create a rule, you cannot use prefixes `ora_` or `sys_`.
4. Specify a **Source** for the rule:
 - **PUBLIC-INTERNET** — Any host on the internet.
 - **OTD** — The Oracle Traffic Director load balancer VMs.
 - **WLS_ADMIN_SERVER** — The WebLogic Server Administration Server VM.
 - **WLS_MANAGED_SERVER** — The WebLogic Server Managed Server VMs.
 - **DB** — The database specified when the Oracle SOA Cloud Service instance was created. If your service instance is configured with more than one database, you can select which database to use for the source.
 - **Custom** — A custom list of addresses from which traffic should be allowed. In the field that displays below when you select this option, enter a comma-separated list of

the subnets (in CIDR format, such as 192.123.42.1/24) or IPv4 addresses for which you want to permit access.

5. Choose a **Destination** for the rule:
 - **OTD** — The Oracle Traffic Director load balancer VMs.
 - **WLS_ADMIN_SERVER** — The WebLogic Server Administration Server VM.
 - **WLS_MANAGED_SERVER** — The WebLogic Server Managed Server VMs.

The source and the destination must be different.
6. Specify the **Destination Port(s)** through which the source will access the destination.

You can specify a single port or a range of ports (such as 7001–8001).
7. Specify the transport **Protocol** (TCP or UDP) with which the source will access the destination.
8. Click **Create**.
9. To manage the existing access rules on the Access Rules page, click the  Menu icon for a rule and choose an option:
 - **Enable** — Rules of type USER or DEFAULT can be enabled. Rules of type SYSTEM cannot.
 - **Disable** — Rules of type USER or DEFAULT can be disabled. Rules of type SYSTEM cannot.
 - **Delete** — Rules of type USER can be deleted. Rules of type DEFAULT or SYSTEM cannot.


Enable or Disable an Access Rule




This topic applies only to Oracle Cloud Infrastructure Classic.

You can dynamically enable or disable existing access rules for an Oracle SOA Cloud Service instance.

Access rules control the network access to the nodes in your service instance, and to external access from the internet. When a service instance is provisioned, Oracle SOA Cloud Service defines several default access rules. You can enable or disable these rules to control access to specific port numbers on specific nodes. Make sure you consider the possible security implications before you open ports to external access.

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Access Rules**.

The Access Rules page is displayed, showing the list of all access rules.
2. On the Access Rules page, beside the rule, click **Actions** , and then select **Enable** or **Disable**.

You can enable or disable `USER` and `DEFAULT` type rules. You cannot disable `SYSTEM` type rules.
3. When prompted for confirmation, click **Enable** or **Disable**.



Delete an Access Rule

You can delete an access rule for an Oracle SOA Cloud Service instance.

Access rules control the network access to the nodes in your service instance, and to external access from the internet. Deleting a rule disables access to specific port numbers on specific nodes.

You can delete only user-created access rules. You cannot delete system-generated access rules.

You cannot modify the configuration of an existing access rule. You must delete the rule and recreate it.

1. Access your service console.
2. Beside the service that you want to modify, click **Manage this instance** , and then select **Manage Access Rules**.
3. On the Access Rules page, beside the rule, click **Actions** , and then select **Delete**.
You can delete `USER` type rules. You cannot delete `SYSTEM` or `DEFAULT` type rules.
4. When prompted for confirmation, click **Delete**.

To return to either the Instances page or the Overview page for the selected service instance, click the locator links at the top of the page.

Enable HTTP Access to an Oracle SOA Cloud Service Instance

If you create an Oracle SOA Cloud Service instance by using the web console rather than the REST API, HTTPS access is enabled by default but HTTP access is disabled. You can enable HTTP access on the load balancer after you have created the service instance. These instructions assume a load balancer has been enabled in your service instance. If there is no load balancer, you must instead create a network channel on all Managed Servers in your Oracle WebLogic Server domain. Refer to "Configuring Network Resources" in *Administering Server Environments for Oracle WebLogic Server* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#) | [12.1.3](#)).

By default the load balancer in your service instance listens for HTTP traffic on port 8080. However, the load balancer VM automatically redirects incoming traffic on port 80 to port 8080.


Topics:

- [Enable the HTTP Port on the Load Balancer](#)
- [Create an Access Rule for the HTTP Port](#)

Enable the HTTP Port on the Load Balancer

You must enable a port on the load balancer (Oracle Traffic Director) to accept HTTP traffic from the public Internet to your Oracle SOA Cloud Service instance.

Access to the Load Balancer Console is disabled by default. To enable the HTTP port on the load balancer:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in using the credentials defined when provisioning your service instance.

If you created your service instance using the Oracle SOA Cloud Service Console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.

Access the load balancer configuration (for example, `opc-config`) and click the



Target Navigation icon. Expand the **Traffic Director** folder and click the name of the Traffic Director configuration.

2. Navigate to the Listeners in this configuration and click **Traffic Director Configuration** and select **Administration > Listeners**.
3. Click **http-listener-1**.
4. Select the **Enabled** checkbox.
5. Click **OK**.
6. click **OK** to activate your changes.

The next task is to create an access rule for the port on the load balancer.

Create an Access Rule for the HTTP Port

You must create an access rule to allow public access to the load balancer (Oracle Traffic Director) through the HTTP port.

If you provisioned this service instance in an Oracle Cloud Infrastructure region, instead you must use the Oracle Cloud Infrastructure Console to create the access rules (security list). See [Configure Security Lists](#) and Security Lists in the Oracle Cloud Infrastructure Services Documentation.

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Access Rules**.

The Access Rules page is displayed, showing the list of all access rules.

2. Click **Create Rule**.

The **Create Access Rule** dialog is displayed.

3. Specify a unique name for the access rule.

The name must begin with a letter, and can contain numbers, hyphens, or underscores. The length cannot exceed 50 characters. You cannot use prefixes `ora_` or `sys_`.

4. Enter `Permit public http to OTD server` for the description.
5. Select **PUBLIC-INTERNET** for the source.
6. Select **OTD** for the destination.
7. Enter `80` as the port and accept the default protocol (TCP).
8. Click **Create**.
9. Refresh the page periodically. The access rule will appear on the Access Rules table after it is created.

You can now access your application by using the default HTTP port:

```
http://IP_of_load_balancer/context_root
```

Enable Communication Between Oracle SOA Cloud Service Instances

The default access rules in an Oracle SOA Cloud Service instance only permit communication between Managed Server VMs and the database, and between Managed Server VMs and the load balancer (if enabled). Use custom access rules to enable communication between the Managed Servers of different service instances.

The architecture of a business application may span multiple tiers, where each application tier is a separate Oracle SOA Cloud Service instance. Similarly, certain integration features of Oracle WebLogic Server enable applications to easily communicate across multiple domains, such as Foreign JNDI Providers and Foreign JMS Servers. In these scenarios, you must use access rules to explicitly permit network communication between service instances.

Identify the host names of the VMs in your *first* service instance. The host names typically use the format `domainName-wls-number`.

For example, if your domain name is `myjcs1` and this domain consists of 3 VMs, the VM host names would typically be:

- `myjcs1-wls-1`
- `myjcs1-wls-2`
- `myjcs1-wls-3`

You can also refer to the Instance Overview page in the Oracle SOA Cloud Service Console. Locate the **Host** property of each VM.

Before you begin, use an SSH client to connect to the Administration Server VM of the *first* service instance. See [Connect to the Administration Server or Load Balancer VM](#).

1. From your SSH session on the Administration Server, use the `nslookup` command to identify the corresponding IP address of each host name.

For example:

```
nslookup myjcs1-wls-2
```

```
Name:   myjcs1-wls-2.compute-myaccount.oraclecloud.internal
Address: 10.11.12.13
```

2. In the [Oracle SOA Cloud Service Console](#), click  adjacent to your *second* service instance and select **Access Rules**.

The Access Rules page is displayed, showing the list of all access rules.

3. Click **Create Rule**.

The Create Access Rule dialog is displayed.

4. Specify a unique **Rule Name**, such as `myjcs1-to-myjcs2`.
5. For **Source**, select the `custom` option. Enter a comma-separated list of the IP addresses for the *first* service instance.

For example: `10.11.12.13,10.11.12.14,10.11.12.15`

6. Select `WLS_MANAGED_SERVER` for the **Destination**.
7. Specify `8001` as the **Destination Port**.

 **Note:**

If you customized your Managed Servers to listen on additional ports, you can specify them as a comma-separated list such as `8001,9001`.

8. Accept the default **Protocol** (TCP).
9. Click **Create**.

Configure SSL for an Oracle SOA Cloud Service Instance

Secure Socket Layer (SSL) is the most commonly-used method of securing data sent across the internet, and assures visitors that transactions with your application are secure. You can configure SSL between the client browser and the load balancer in your Oracle SOA Cloud Service instance to ensure that applications are accessed securely.

By default, SSL is already enabled within the software components of an Oracle SOA Cloud Service instance, including Oracle WebLogic Server and the load balancer. They are configured to use a self-signed SSL certificate that was generated by Oracle SOA Cloud Service. Clients will typically receive a message indicating that the signing CA for the certificate is unknown and not trusted.

Topics:

- [Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates \(with OTD\)](#)
- [Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates \(non-OTD\)](#)

Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates (with OTD)

This section provides the steps for setting up your Oracle SOA Cloud Service instance to use CA-verified SSL certificates.

 **Note:**

The steps here are for an Oracle SOA Cloud Service instance using Oracle Traffic Director (OTD). If you are not using OTD, see [Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates \(non-OTD\)](#).


Topics:

- [Create a Self-Signed SSL Certificate in the Load Balancer](#)
- [Import a CA-Issued SSL Certificate to the Load Balancer](#)
- [Associate the SSL Certificate With the Load Balancer](#)

Create a Self-Signed SSL Certificate in the Load Balancer


For development in Oracle SOA Cloud Service environments, you can use either a CA-issued or a self-signed certificate. You can create a self-signed certificate using the Load Balancer Console.

To obtain and use a CA-issued certificate instead, see [Import a CA-Issued SSL Certificate to the Load Balancer](#).

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in to Console using the credentials defined when provisioning your service instance.

If you created your service instance using the Oracle SOA Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.

Access the load balancer configuration (`opc-config`) by following the steps below:

- a. Once logged in to the OTD console, click the  icon.
- b. Expand the **Traffic Director** folder.
- c. Click on the load balancer configuration (`opc-config`).
2. Perform these steps to create a self-signed certificate:
 - a. Click **Traffic Director Configuration** and select **Security**, then **Manage Certificates**.
 - b. Click **Generate Keypair**.
 - c. Enter an **Alias** for the new certificate.
 - d. Set the **Common Name** to your custom domain name. For example, `example.com`.
 - e. Complete the remaining fields and click **OK**.

Import a CA-Issued SSL Certificate to the Load Balancer


For production Oracle SOA Cloud Service environments, it is recommended that you use a CA-issued SSL certificate. A CA-issued SSL certificate reduces the chances of experiencing a man-in-the-middle attack.

There are multiple CA vendors in the marketplace today, each offering different levels of service at varying price points. Research and choose a CA vendor that meets your service-level and budget requirements.

For a CA vendor to issue you a CA-issued SSL certificate, you need to provide the following information:


- Your custom domain name.
- Public information associated with the domain confirming you as the owner.
- Email address associated with the custom domain for verification.

Create a Certificate Signing Request (CSR) by using the Load Balancer Console and submit the CSR to the CA vendor. After receiving the CA-issued certificate, import it into the load balancer configuration:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in to Console using the credentials defined when provisioning your service instance.

If you created your service instance using the Oracle SOA Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.

Access the load balancer configuration (`opc-config`) by following the steps below:

- a. Once logged in the OTD console, click the  icon.
 - b. Expand the **Traffic Director** folder.
 - c. Click the Load Balancer configuration (`opc-config`).
2. Perform these steps to generate a CSR:
 - a. Click **Traffic Director Configuration** and select **Security > Manage Certificates**.
 - b. Click **Generate Keypair**.
 - c. Enter an **Alias** for the new certificate.
 - d. Set the **Common Name** to your custom domain name. For example, `example.com`.
 - e. Complete the remaining fields and click **OK**.
 - f. Select your new certificate and click **Generate CSR**.
 3. Save the generated CSR text, including the header line `-----BEGIN NEW CERTIFICATE REQUEST-----` and footer line `-----END NEW CERTIFICATE REQUEST-----`.

For example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC9jCCAd4CAQAwYDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAKNBMQwwCgYDVQQH
EwNTQ0ExDzANBgNVBAoTBk9yYWNsZTEPMA0GA1UECzMGT3JhY2x1MRQwEgYDVQQD
I+XY7ByYRma1XlM1cYoMUiKSnRHd1lUZMRwYHu4AZvrEMihKjB6YiC0F
-----END NEW CERTIFICATE REQUEST-----
```

The CSR includes the public key and other information that the CA vendor needs to verify the identity of the load balancer server.


4. Submit the CSR to your CA vendor to request a new CA-issued SSL certificate.
For more information about submitting the CSR, refer to your CA vendor documentation.
Your CA vendor uses the CSR information to validate the domain and provides you with a valid SSL certificate, typically via email.
5. Return to the Load Balancer Console for your service instance.
6. Perform these steps to import the CA-issued certificate:
 - a. Click **Traffic Director Configuration** and select **Security > Manage Certificates**.
 - b. Click **Import**.
 - c. Verify that **Certificate Type** is set to Certificate.

- d. Select the **Alias** of the certificate you generated earlier.
- e. You can paste the certificate text directly in the **Paste Certificate String Here** field, or click **Choose File** and select the certificate on your local file system. If you opt to paste the certificate text, be sure to include the headers `BEGIN CERTIFICATE` and `END CERTIFICATE`, including the beginning and ending hyphens.
- f. Click **OK**.

For more information about managing load balancer certificates, see "Managing Certificates" in *Administering Oracle Traffic Director* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#)).

Associate the SSL Certificate With the Load Balancer

After installing a CA-issued or self-signed SSL certificate to the load balancer, you must associate it with the HTTPS listeners in the load balancer's configuration. After the association is made, the load balancer will present the SSL certificate while processing any new HTTPS requests.

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in to Console using the credentials defined when provisioning your service instance.

If you created your service instance using the Oracle SOA Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.

2. Access the load balancer configuration (`opc-config`):

- a. Once logged in to the OTD console, click .

- b. Expand the **Traffic Director** folder.

- c. Click on the load balancer configuration (`opc-config`).

3. Click **Traffic Director Configuration** and select **Administration**, then **Listeners** to navigate to the listeners in this configuration.
4. Click **https-listener-1**.
5. In the **SSL/TLS Settings** section, select the default certificate (`opc-config`) in the **RSA Certificate** field.
6. Click **OK** to activate your changes.
7. Repeat from step 4 to update the certificate of any additional HTTPS listeners in this configuration.

This will propagate new certificates into the required wallets.

8. Click **https-listener-1**.
9. In the **SSL/TLS Settings** section, select your new certificate in the **RSA Certificate** field.
10. Click **OK** to activate your changes.
11. Repeat from step 8 to update the certificate of any additional HTTPS listeners in this configuration.
12. Optionally, click **Restart Instances** to restart the listeners.

 **Note:**

Alternatively, you can configure **SSL/TLS Settings** for an entire Virtual Server in the load balancer configuration.

After modifying a listener's certificate you must also restart the load balancer node(s) in your service instance for the change to take effect. See [Stop, Start, or Restart Managed Server and Load Balancer VMs](#).

For more information about the SSL settings of the load balancer, see "Configuring SSL/TLS Between Oracle Traffic Director and Clients" in *Administering Oracle Traffic Director* ([12.2.1.4](#) | [12.2.1.3](#) | [12.2.1.2](#)).

Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates (non-OTD)

This section provides the steps for replacing the identity and trust of Oracle SOA Cloud Service with custom identity and custom trust and registering the Oracle SOA Cloud Service server with digital certificates procured from public certificate authorities such as digicert or any other third party authority.

As a prerequisite, register the Oracle SOA Cloud Service domain with the public DNS for CA verification. In this documentation, the public IP of the Oracle SOA Cloud Service domain is registered with *mydomain.com* and the CA signed certificates are taken from *mydomain*.

The Enterprise Manager (EM) Console needs to be accessible using the public domain name.

 **Note:**

The steps here are for an Oracle SOA Cloud Service instance not using Oracle Traffic Director (OTD). If you are using OTD, see [Set Up Oracle SOA Cloud Service to Use CA-Verified SSL Certificates \(with OTD\)](#).

Topics:

- [Register a Domain Name for Oracle SOA Cloud Service](#)
- [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 Cloud Service

To register a domain name for Oracle SOA Cloud Service:

1. Register a domain for Oracle SOA Cloud Service 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 Cloud Service.

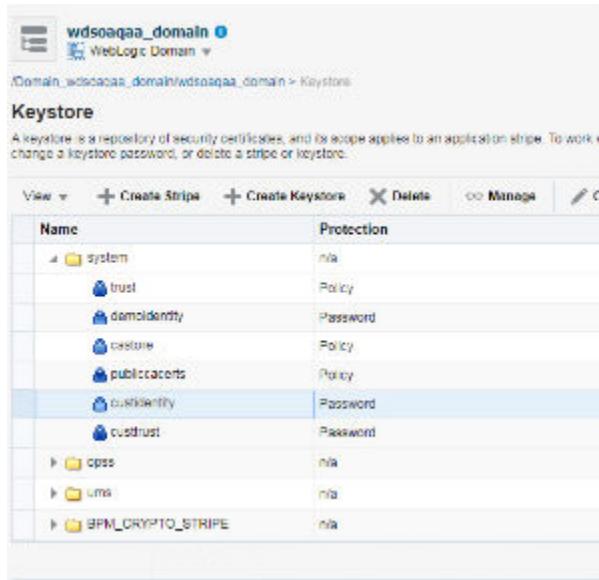
For example, register `soacs.oraclecloud.co.in` domain in `mydomain.com`, mapping to the public IP of Oracle SOA Cloud Service server.

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.

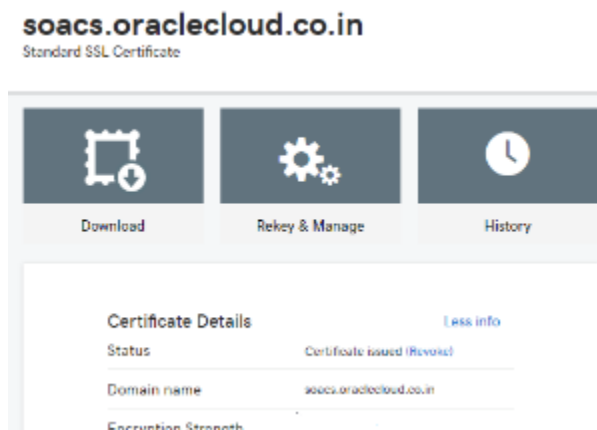
It is not mandatory to create identity and trust keystore under the `system` stripe that comes with Oracle SOA Cloud Service provisioning by default. You can create a new custom stripe and create identity and trust keystores under it.

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**.

- 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.



- 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
- Double-click the certificate chain for the root and intermediate certificates. You can see the full chain when you click on certification path.
- 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**.
- In the View Certificates popup, select the **Details** tab and click **Copy to File**.
- In the Certificate Export wizard, click **Next**, select **Base 64 encoded X.509 (CER)**, then click **Next**. Export the certificate.
- 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:

- Use WLST commands to import the certificate chain into the identity keystore (custIdentity):
 - 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 Log Out Preferences Record Help

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

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/custrust

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
```

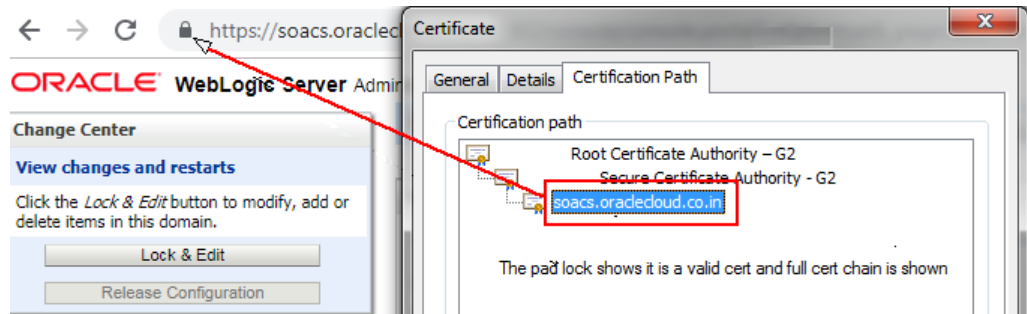
13. Save `boot.properties`.
14. To make changes in `SetDomainEnv.sh`, remove the following property:
`Djavax.net.ssl.trustStore=%WL_HOME%\server\lib\DemoTrust.jks`
15. To update the **Frontend Host Port**, update the host and port in the WebLogic Server Console to reflect the domain name and ports:
 - 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.

The screenshot shows the WebLogic Server Console interface. The breadcrumb navigation is: Home > Summary of Servers > wdsoaqa_server_1 > Summary of Clusters > wdsoaqa_cluster. The page title is 'Settings for wdsoaqa_cluster'. There are several tabs: Configuration (selected), Monitoring, Control, Deployments, Services, and Notes. Under the Configuration tab, there are sub-tabs: General, JTA, Messaging, Servers, Replication, Migration, Singleton Services, Scheduling, Overload, Health Monitoring, and HTTP (selected). A message says: 'Click the *Lock & Edit* button in the Change Center to modify the settings on this page.' Below this is a 'Save' button. A descriptive text says: 'This page allows you to define the HTTP settings for this cluster. These settings can be overridden by explicitly setting the member servers of this cluster'. There are three input fields: 'Frontend Host' with the value 'soacs.oraclecloud.co.in', 'Frontend HTTP Port' with the value '80', and 'Frontend HTTPS Port' with the value '443'. At the bottom is another 'Save' button.

16. Start the Node Manager, Administration Server, and Managed Server, in this order.

Verify the Environment

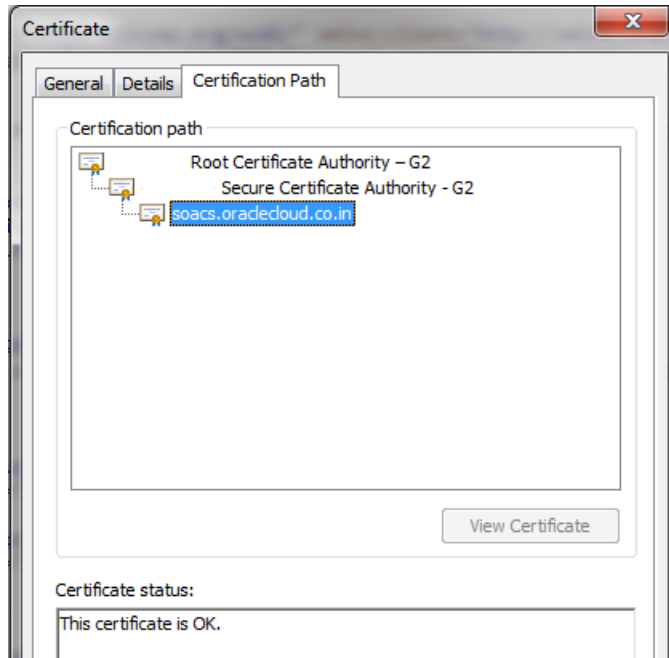
When you restart the environment, the Administration Server and Managed Server user interface shows the certificates as trusted:



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 Cloud Service

Perform the following steps to import the certificate chain. These steps prevent a `SSLHandshakeExceptions` error from occurring while invoking an HTTPS service.

- [Export the Certificate Chain of the HTTPS WSDL Called in Oracle SOA Cloud Service](#)
- [Import the Certificate Chain of the HTTPS WSDL Called in the Oracle SOA Cloud Service 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 Cloud Service

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 Cloud Service Trust Store



Note:

In a multinode cluster, the certificate chain must be imported to the keystores on all nodes of the cluster.

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.

- 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 and Managed Servers once the certificates are imported. This is required for both JKS- and KSS-based certificates. See [Stop or Start an Oracle SOA Cloud Service Instance and Individual VMs](#).

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

Troubleshoot Oracle SOA Cloud Service

These topics describe how to troubleshoot problems you might encounter while using Oracle SOA Cloud Service.

Topics:

- [Find Diagnostic Information to Help with Troubleshooting](#)
- [Problems Using IDCS as the Authentication Provider](#)
- [Problems with Creating Service Instances](#)
- [Problems with Deploying and Accessing Applications](#)
- [Problems with Failure of a Running Service When the Schema User Password Expires](#)
- [Problems with Scaling](#)
- [Problems with Patching and Rollback](#)
- [Problems with Backup and Restoration](#)
- [Problems with Restart](#)
- [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](#)
- [Problems Adding Block Storage to an Existing Oracle SOA Cloud Service](#)
- [Problems with Oracle Traffic Director Timing Out](#)

Find Diagnostic Information to Help with Troubleshooting

You can use the WebLogic Server Administration Console and other tools to find more information about problems with Oracle SOA Cloud Service 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](#)
- [Find Status Messages for Oracle SOA Cloud Service Instances](#)

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. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open WebLogic Server Administration Console**. Log in with credentials you entered for the WebLogic Administrator when you created the service instance.
2. In the Domains area, 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. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open WebLogic Server Administration Console**. Log in with credentials you entered for the WebLogic Administrator when you created the service 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**.

The log file you selected is displayed in the table.

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

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

Find Status Messages for Oracle SOA Cloud Service Instances

From the Oracle SOA Cloud Service Console, you can view status messages to determine why an attempt to create a service instance failed.

To find status messages for a failed attempt to create a service instance:

1. In the [Oracle SOA Cloud Service Console](#), expand the arrow next to **Instance Create or Delete History**.
2. Click on the name of the service instance you created or deleted, or click on **Details**.

A list of status messages is displayed. The messages trace the process for creating the service instance from the beginning to the point of failure. Success messages are displayed in addition to error messages.

Problems Using IDCS as the Authentication Provider

Oracle SOA Cloud Service 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 Cloud Service supports Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).

Problems with Creating Service Instances

You may experience problems when creating services.

In the process of creating a service, the operation failure becomes visible in the following way:

1. The service instance appears in the Services list in the Oracle SOA Cloud Service Console.
2. An **In progress...** message appears in the service instance details.
3. When the creation process fails, a **Failed** message is displayed and a red exclamation mark appears on the service instance's icon.
4. The service instance is listed in the **Service Create or Delete History** section.
5. Click on **Details** to view progress and error messages.

The most common sources of failure when creating a service instance include:

- Timeout errors
- SSH connection issues
- Incorrect credentials
- Database listener down

The following solutions apply to problems creating service instances for Oracle SOA Cloud Service:

My database is not listed in provisioning screens

Possible causes for not seeing your database listed in the provisioning wizard screens are:

- Required Oracle Cloud Infrastructure policies are not created. See “Create a Policy” in the tutorial [Creating the Infrastructure Resources Required for Oracle Platform Services](#) to add the following policy:

```
Allow service PSM to inspect database-family in compartment  
<compartment_name>
```
- The database is not a supported version.

- The database uses Logical Volume Management (LVM) storage, which is not supported.
- The database does not have backup storage, which is required.

Provisioning fails with incorrect PDB value

If provisioning fails with an incorrect pluggable database (PDB) value or you want to find out the PDB name in your database, use the following command:

```
SELECT PDB_ID, PDB_NAME, STATUS FROM DBA_PDBS ORDER BY PDB_ID;
```

I cannot create an Oracle SOA Cloud Service — Virtual Image instance when I choose a Oracle Database Classic Cloud Service — Virtual Image database deployment

A failure occurs when you attempt to create an Oracle SOA Cloud Service instance with a Oracle Database Classic Cloud Service — Virtual Image database deployment.

To prevent this failure, you must first configure the Oracle Database Classic Cloud Service — Virtual Image environment.

I receive a database connectivity error message

You may not be able to create an Oracle SOA Cloud Service instance because the `oracle` user does not have a password in Oracle Database Classic Cloud Service instances. To modify the properties of the `oracle` users so that the password does not expire, see [Problems Creating Instances](#).

I cannot create a service when I have many service instances

Your account may not have enough compute quota to create the service instance.

If you have instances you do not need, delete them. If you need all your service instances, contact Oracle Sales and Services to buy more quota for your account.

I cannot create a service instance, even after waiting for an hour

If service creation fails after one hour, the system may be experiencing a heavy load, and resources are not yet available.

Wait before you try again to create the service. If the problem persists, contact Oracle Support Services.

I cannot create a service instance when the service instance name is not unique

Oracle SOA Cloud Service instance creation can fail if the name you choose for the new service instance is identical to the name of another service instance, including a failed service instance. Also, the Oracle SOA Cloud Service instance name cannot be the same as the name of an Oracle SOA Cloud Service instance.

After an attempt to create an Oracle SOA Cloud Service instance fails, Oracle SOA Cloud Service may require some time to remove items that were created during the attempt. If the new and failed service instance names are identical, a naming conflict may occur and the attempt to create the new service instance may fail.



Note:

As a best practice, always ensure that your Oracle SOA Cloud Service instance names are unique.

I receive an error message stating that no database service is available

If you attempt to create an Oracle SOA Cloud Service using an Oracle Database Classic Cloud Service database deployment that does not have backups enabled (Destination=None), then provisioning fails and the following error message is issued:

```
There are no Oracle Database Cloud Service instances available for Service
Level:
Oracle Java Cloud Service
```

Create a new database deployment with backups enabled and specify this database deployment when you create a new Oracle SOA Cloud Service instance.

I encounter Intermittent provisioning failures for clustered instances based on WebLogic Server 12.2.1

Your attempt to create an Oracle SOA Cloud Service instance based on WebLogic Server release 12.2.1 can fail if you use the REST API to create an instance containing a large number of cluster members. You cannot create clustered instances by using the Oracle SOA Cloud Service user interface.

The cause of the problem is that an exclusive configuration lock acquired by one process is released by another process that successfully acquires another exclusive lock.

This problem is intermittent, so try again to provision a service instance. Alternatively, provision a smaller cluster and then scale out your nodes.

I encounter a database connection error when creating an Oracle SOA Cloud Service instance

In the process of creating an Oracle SOA Cloud Service Instance while using the Service Instance Creation Wizard, you may receive the following error message: Failed to connect to DBaaS Service.

To help identify the problem, confirm that the user name and password are correct by connecting to the database via sqlplus. Also, confirm that you have the correct privileges. For more information, see About Database as a Service Roles and Users.

If you have done these checks and do not see any issues, the problem might be that the `oracle` password has expired on the database node.

You can change the properties of the `oracle` user so that the password does not expire. See Problems Accessing Instances.

Problems with Deploying and Accessing Applications

Problems might occur when you attempt to deploy or access an application.

I can't deploy an application to an Oracle SOA Cloud Service instance based on WebLogic Server 11g

You can deploy an application that relies on Java EE 6 or Java EE 7 component jars such as JSF 2.0 to an Oracle SOA Cloud Service instance based on WebLogic Server 11g only if you manually package the relevant libraries for your application. Java EE 6 or Java EE 7 component jars such as JSF 2.0 are not packaged by default.

The recommended version for deploying this type of application is WebLogic Server 12c.

I can't access an application using the URL from the WebLogic Server Administration Console Testing tab

You cannot access a deployed application from the public internet if you use the URL displayed on the Testing tab of the WebLogic Server Administration Console. The URLs shown on this tab are internal to Oracle SOA Cloud Service. Instead, use the procedure in [Accessing an Application Deployed to an Oracle SOA Cloud Service Instance](#).

I can't access an application through the HTTP port

By default, you cannot access an application running on an instance through the HTTP port if the instance was created by using the Create New Oracle Java Cloud Service Instance wizard available from the Oracle Java Cloud Service Console. You must enable the HTTP port after you create the service instance. The instance is accessible, however, via HTTPS without manual intervention.

Both the HTTP and HTTPS ports are enabled by default if you created the Oracle Java Cloud Service instance by using the REST API.

To enable the HTTP for a service instance created with the wizard, you must enable a listener port on the load balancer, then create an access rule. If your service instance has a load balancer, see [Enabling HTTP Access to an Oracle Java Cloud Service Instance](#).

If your service instance does not have a load balancer, you must enable a network channel on all Managed Servers to ensure that they are listening on the port you are opening, then create the access rule. See [Create and Assign the Network Channel in Administering Server Environments for Oracle WebLogic Server](#).

See [Understanding the Default Access Ports in Using Oracle Java Cloud Service](#).

Problems with Failure of a Running Service When the Schema User Password Expires

An Oracle SOA Cloud Service 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 Cloud Service instance is created. You get 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
```

Another symptom of this problem is that a patch precheck, restoration, or scale out operation may fail.

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 [Change the Database Schema Password Manually](#).

Problems with Scaling

Problems might occur when you attempt a scaling operation.

The following solutions apply to problems with scale-in and scale-out with Oracle SOA Cloud Service.

My scale-out operation does not start

Your scale-out operation has been placed in the request queue, and it might be a few minutes before the operation is performed. Check status on the Activity tab of the Oracle SOA Cloud Service Console.

Wait before you try to scale out again. If the problem persists, contact Oracle Support Services.

My scale-in operation is not allowed

The managed server you selected for scale-in is on the same virtual machine as the administration server. Removing this virtual machine is not allowed.

Select another virtual machine to scale in.

My service is too busy to allow scaling

Your service has a pending maintenance operation such as backup or patching.

Wait until maintenance has completed before you try scaling again.

Scaling in fails when storage is full

A scale-in operation fails when local disk storage is full.

A scale-in operation attempts to create a backup before scaling in. If you initiate frequent backups, local storage can fill up because backups are retained for seven days. Unlike with patching, there is no pre-check operation to check for enough storage to perform the scaling operation.

If you create frequent backups, delete backups before scaling in to avoid this problem. See [Deleting a Backup](#).

Problems with Patching and Rollback

This section identifies some potential issues you may face after patching and rollback operations.

The following recommendations ensure that patching and rollback operations enable you to continue running your applications.

My identity key store and trust store are missing after a patching, rollback, or restoration operation

If you have identity key stores and trust stores, they can disappear after you apply a patch, roll back a patch, or restore a backup. You may have configured one of the following:

- Custom identity key store and custom trust store
- Custom identity key store and Java standard trust store
- WebLogic Server identity key store and WebLogic Server trust store

Patching, rollback, and restoration operations replace the directories you may have used to keep the custom key store and trust store, so they are essentially emptied.

To protect your key store and trust store, create the key stores and trust stores by using the OPSS KeyStoreService (KSS). See [Configuring the OPSS Keystore Service for Demo Identity and Trust](#) in *Administering Security for Oracle WebLogic Server*.

If you don't want to use the OPSS KeyStoreService, you can put the key store and trust store in the WebLogic domain created by Oracle Java Cloud Service.

It's particularly important to protect your key store and trust store for JDK patching. Each JDK patch replaces the previous version.

Before you apply a WebLogic Server patch:

- Do not put CA certificates in the existing demo keystores
- Do not put custom key stores and trust stores in the `<MW_HOME>/wlserver/lib` directory
- Do not put CA certificates anywhere on the system except in key stores

I receive a message stating that the virtual machines are unhealthy

You cannot apply a patch if the service's virtual machines are not in a healthy state.

Restore the service using a backup and try patching again.

I receive a message stating that the service is busy with another operation

You cannot apply a patch when the service is under maintenance, for example, scaling or backup.

Wait until the service is no longer under maintenance and try patching again.

Problems with Backup and Restoration

Problems might occur when you attempt backup or restoration.


The following solutions apply to problems with backup and restoration operations for Oracle SOA Cloud Service.

Oracle Traffic Director is not backed up

Typically, this occurs when the traffic director is currently busy servicing other requests.

Verify that Oracle Traffic Director is running and in a healthy state, and try backup again.

To check the health of the Oracle Traffic Director:

1. In the [Oracle SOA Cloud Service Console](#), click  for the desired service instance and select **Open Load Balancer Console**. Log in using the credentials defined when provisioning your service instance.
2. In the left panel, click **Services**.
The Services page is displayed on the right.
3. Click on the **Configurations** tab in the upper left corner of the console and select **opc-config**.
The Configuration table is displayed.
4. Notice whether a green check mark appears in the cell containing the load balancer name.
If there is a green check mark next to Instance Running, your load balancer is running and healthy. Otherwise, your load balancer is not running.

There is not enough space for my backup

The backup storage area does not have enough space for the backup operation to create the archive.

To check for available space, log in to the VM and check the size of the backup mounted directory under `/u01/data/backup`. See [Access a VM Through a Secure Shell \(SSH\)](#).

If there is not enough space for the backup, do one of the following:

- Delete any unwanted backups.
- Archive one or more backups to an Oracle Cloud Infrastructure Object Storage Classic container. See [Backup and Restore](#) in *REST API for Oracle SOA Cloud Service*.

Then increase the storage volume size used by the *fast recovery area* as necessary if you have a longer retention policy and extend the backup storage volume as described in [Administering Oracle Database Classic Cloud Service](#).

The restoration operation fails and generates an error about pre-check failure

Either one or more servers are currently unreachable, or there is not enough space on one of the storage volumes.

To find the reason for the restoration failure:

1. Navigate to the Backup page.
 - a. In the [Oracle SOA Cloud Service Console](#), click the name of the service instance for which you want to find the restoration status information.
 - b. On the Overview page, click the Administration tile.
The Oracle SOA Cloud Service Instance page is refreshed with the Administration tile in focus.
 - c. Click the Backup tab.
The Backup page is displayed.
2. Locate the icon for the restoration that failed.
3. Click on the date to the right of the icon.
A pop-up containing the status details is displayed.

If the problem is that a server is unreachable, the software automatically attempts a scale-in operation. Try restoring the service again.

If there is not enough space for the backup, do one of the following:

- Delete any unwanted backups.
- Archive one or more backups to an Oracle Cloud Infrastructure Console Object Storage Classic container. For more information, see [Backup and Restore in REST API for Oracle SOA Cloud Service](#).

One of my backups is showing a warning icon

When a scheduled backup is completed, Oracle SOA Cloud Service tries to move older backups from block storage and delete older backups from the Oracle Cloud Infrastructure Object Storage Classic container. If Oracle SOA Cloud Service cannot move or delete the older backups, the **newly completed** backup shows a warning

icon: 


This problem does not affect the newly completed backup. However, the presence of the older backups may cause future backups to fail because of insufficient space.

To prevent such failures, ensure that Oracle SOA Cloud Service can remove the older backups when the next scheduled backup is completed:

1. To find out why Oracle SOA Cloud Service could not move or remove the backups, place the cursor over the icon.
A text rollover appears that contains detailed information about why Oracle SOA Cloud Service could not move or remove the backups.

2. Correct the problem that prevented Oracle SOA Cloud Service from moving or removing the backups.

For example, to correct an access permission problem, ensure that the user name and password for the administrator of the Oracle Cloud Infrastructure Object Storage Classic container are correct. If necessary, change them as explained in [Configure Automated Backups for an Oracle SOA Cloud Service Instance](#)

3. When the next scheduled backup is completed, determine whether it shows the icon for a successful backup: 

- If so, no further action is required.
- If the next scheduled backup also shows the warning icon, contact Oracle Support Services.

Problems with Restart

You might experience unexpected side-effects after restarting an Oracle SOA Cloud Service instance or individual VMs. These effects can also occur after patching, which restarts VMs.

Restart fails after a scale down operation intended to remedy a quota breach

You can scale down a Oracle Database Classic Cloud Service database deployment or Oracle SOA Cloud Service instance if you have a quota breach in your account. Scaling down reduces compute resources. However, the automatic restart action can fail after scale-down.

For example, you could scale down a node from shape oc5 to oc3. Oracle SOA Cloud Service puts the service instance into Maintenance mode, changes the state of the node to Configuring, and stops any servers running on the node. After applying the changes, Oracle SOA Cloud Service is supposed to start the servers automatically. If the quota breach is not cleared by the time the orchestration is restarted with the smaller shape, the automatic server restart action could fail.

If the restart action fails, wait one hour for the quota breach to clear, then restart the service instance by using the Oracle SOA Cloud Service Console.

Monitor a VM's boot log

You can monitor the boot progress of individual VMs by using Oracle Cloud Infrastructure Compute Classic. See [Viewing the Boot Log of an Instance](#) in *Oracle Cloud Infrastructure Compute Classic*. Ignore information in this topic about the Compute API.

My custom storage volumes have become detached

Custom storage volumes you have added after creating an Oracle SOA Cloud Service instance will become detached after restart operations.

Do not attach custom storage volumes to a service instance's VMs. Any custom storage volumes are detached if the service instance is restarted.

If a service instance requires additional storage, add storage by scaling the service instance's nodes as explained in [Scaling an Oracle SOA Cloud Service Node](#).

My content changes on the Boot/OS volume are gone

See [About the Disk Volumes](#).

Problems with Connectivity

Problems might occur when you attempt to connect to an Oracle SOA Cloud Service instance.

The following solutions apply to problems with connectivity to an Oracle SOA Cloud Service instance.

My private key is lost or corrupted

When you create an Oracle SOA Cloud Service 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. See [Generate a Secure Shell \(SSH\) Public/Private Key Pair](#).
2. Add the new SSH public key to your existing service instance. See [Add an SSH Public Key](#).
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

For information about restarting the Administration Server through the Node Manager, see [Using WLST Commands to Restart the Administration Server](#).

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 Cloud Service instance, you must restart the Node Manager on each host.

- a. SSH to the second host:

```
ssh hostname
```

For example:

```
ssh ourserviceinstance-wls-2
```

You can find the hostname on the Oracle SOA Cloud Service Instance page in the Oracle Java Cloud Service user interface.

- 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



This topic does not apply to Oracle Cloud at Customer.

When you mount Oracle Database File System on non Administration Pods, Oracle Database File System mounts on first Managed Server node but not on the second Managed Server node.

To mount Oracle Database File System on a second Managed Server node:

1. Use the `ssh` command to connect to the scaled out Virtual Machine (VM) or the VM where you have created two or more node clusters:

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

For example:

```
ssh -i opc_rsa opc@123.123.12.34
```

2. Change to the `oracle` user.

```
sudo su - oracle
```

3. Copy the existing workaround script to `/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 to the `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 the `oracle` user.

```
sudo su - oracle
```

2. Run the following commands:


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

3. Use the `ssh` command to [connect to the Administration Server](#):

```
ssh -i opc_rsa opc@VM_IP_address
```

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 the mount on the second Managed Server node and file sharing is successful on Oracle Database File System.

Problems with a Database Deployment

Problem related to the database deployment used by Oracle SOA Cloud Service can occur.

Creating an opss datasource fails

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

To unlock the opss user account:

1. Log in to the database deployment's VM by using the private key.

```
ssh -i private-key opc@ip-address-of-db-vm
```

2. Change to user `oracle`.

```
cd $ORACLE_HOME/bin
```

3. Start `sqlplus`.

```
./sqlplus
```

4. Log in using the `system` user, and enter the password.

```
Enter user-name: system
Enter password: system_user_password
```

5. Unlock the account.

```
ALTER USER schema_prefix_opss ACCOUNT UNLOCK;
```

6. Change the password.

```
ALTER USER schema_prefix_opss IDENTIFIED BY new_password;
```

7. Exit `sqlplus`.

```
exit
```

Problems Opening the WebLogic Server Administration Console from Fusion Middleware Control

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

You can use the WebLogic Server Administration Console and Fusion Middleware Control to administer Oracle SOA Cloud Service 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
```

Problems Adding Block Storage to an Existing Oracle SOA Cloud Service

You can add block storage to an existing Oracle SOA Cloud Service, either through the user interface or through the command line. However, this process sometimes may result in DBFS mount failure. Under those circumstances, follow these steps to add block storage and remount the DBFS.

To add block storage to an existing Oracle SOA Cloud Service and remount the DBFS:

1. Unmount the DBFS directories using the `fusermount` command.

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

2. Follow the steps in [Scale an Oracle SOA Cloud Service Node Up or Down](#) to extend memory.
3. Mount the above directories back again.

The mount point is the logical file system and the actual file stays in the DBFS instance. To mount:

- a. Run `sudo su - oracle` to change to the `oracle` user.
- b. Run the following commands to recreate the DBFS mount points `dbfs_directio` and `dbfs`.

```
-bash-4.1$ $ORACLE_HOME/bin/dbfs_client -o wallet /@ORCL -o
direct_io/u01/soacs/dbfs_directio
-bash-4.1$ $ORACLE_HOME/bin/dbfs_client -o wallet /@ORCL -o
direct_io/u01/soacs/dbfs
```

- c. Run `-bash-4.1$ df -h` to validate the mount point setup.

You get details such as File system, Size Used, Avail Use%, and Mounted on.

Problems with Oracle Traffic Director Timing Out

When Oracle Traffic Director handles many requests simultaneously, exception errors can occur. To handle these requests, you must increase the timeout value.

```
<Error> <oracle.integration.platform.blocks.soap> <BEA-000000>
<Unable to dispatch request to
http://host/WebServices_WebLogicFusionOrderDemo_CreditCardAuthorization/
CreditAuthorizationPort due to
exception javax.xml.ws.WebServiceException: javax.xml.soap.SOAPException:
javax.xml.soap.SOAPException: Message send failed: Connection timed out
at
oracle.j2ee.ws.client.jaxws.DispatchImpl.invoke(DispatchImpl.java:1381)
```

```
        at
oracle.j2ee.ws.client.jaxws.OracleDispatchImpl.synchronousInvocationWith
hRetry( OracleDispatchImpl.java:237)
        at
oracle.j2ee.ws.client.jaxws.OracleDispatchImpl.invoke(OracleDispatchImp
l.java: 108)
. . .
. . .
```

To increase the timeout value for Oracle Traffic Director:

1. Log in to Oracle Traffic Director:

```
https://OTD_host:/8989
```

2. Click **Configurations**.
3. Click **Advanced Settings**.
4. Change the time out value to 3600.
5. Click **Save**.
6. Click **Deploy Changes**.

A

Patches Installed By Release

The bundle patches listed in this appendix are installed in instances provisioned with releases of Oracle SOA Cloud Service.

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](#).

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](#) (as the `opc` user):

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

2. Change to the `oracle` user:

```
sudo su - oracle
```

3. Enter the following command:

```
cat /u01/app/oracle/tools/downloadBinaries/soacs/  
toponame_version_patches.txt
```

For example:

```
cat /u01/app/oracle/tools/downloadBinaries/soacs/  
20.3.1.0.0_soaosbb2b_12.2.1.4_patches.txt
```

Example Output:

```
["p30549478_122140_Generic.zip", "p31396632_122140_Generic.zip"]
```

Sign in to [My Oracle Support](#) and search for the patch numbers to locate and download the patches.

Patch Releases

- [Patches Applied During Provisioning — 23.3.1](#)
- [Patches Applied During Provisioning — 23.2.2](#)
- [Patches Applied During Provisioning — 23.1.1 and 23.1.3](#)
- [Patches Applied During Provisioning — 22.4.2](#)
- [Patches Applied During Provisioning — 22.3.3](#)
- [Patches Applied During Provisioning — 22.1.3](#)
- [Patches Applied During Provisioning — 22.1.1](#)
- [Patches Applied During Provisioning — 21.4.3](#)
- [Patches Applied During Provisioning — 21.3.2 and 21.4.1](#)

- [Patches Applied During Provisioning — 21.2.1](#)
- [Patches Applied During Provisioning — 21.1.1](#)
- [Patches Applied During Provisioning — 20.4.1](#)
- [Patches Applied During Provisioning — 20.3.1](#)
- [Patches Applied During Provisioning — 20.2.3](#)
- [Patches Applied During Provisioning — 20.2.1](#)
- [Patches Applied During Provisioning — 19.4.3](#)
- [Patches Applied During Provisioning — 19.4.1](#)
- [Patches Applied During Provisioning — 19.3.2](#)
- [Patches Applied During Provisioning — 19.2.2](#)
- [Patches Applied During Provisioning — 19.2.1](#)
- [Patches Applied During Provisioning — 19.1.5](#)
- [Patches Applied During Provisioning — 19.1.3](#)
- [Patches Applied During Provisioning — 18.4.5](#)
- [Patches Applied During Provisioning — 18.4.3](#)
- [Patches Applied During Provisioning — 18.3.5](#)
- [Patches Applied During Provisioning — 18.3.3](#)
- [Patches Applied During Provisioning — 18.3.1](#)
- [Patches Applied During Provisioning — 18.2.5](#)
- [Patches Applied During Provisioning — 18.2.3](#)
- [Patches Applied During Provisioning — 18.2.1](#)
- [Patches Applied During Provisioning — 18.1.5](#)
- [Patches Applied During Provisioning — 18.1.3](#)
- [Patches Applied During Provisioning — 18.1.1](#)
- [Patches Applied During Provisioning — 17.4.5](#)
- [Patches Applied During Provisioning — 17.4.3](#)
- [Patches Applied During Provisioning — 17.4.1](#)
- [Patches Applied During Provisioning — 17.3.5](#)
- [Patches Applied During Provisioning — 17.3.3](#)
- [Patches Applied During Provisioning — 17.3.1](#)
- [Patches Applied During Provisioning — 17.2.5](#)
- [Patches Applied During Provisioning — 17.2.1](#)
- [Patches Applied During Provisioning — 17.1.3](#)
- [Patches Applied During Provisioning — 16.4.5](#)
- [Patches Applied During Provisioning — 16.4.1](#)
- [Patches Applied During Provisioning — 16.3.5](#)
- [Patches Applied During Provisioning — 16.3.3](#)

- [Patches Applied During Provisioning — 16.1.5](#)
- [Patches Applied During Provisioning — 15.4.5](#)

Patches Applied During Provisioning — 23.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 23.3.1.

Table A-1 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-2 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-3 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p31713053_122140_Linux-x86-64.zip
p30922431_122140_Generic.zip
p35445981_122140_Generic.zip
p35347020_122140_Generic.zip
p35720109_12214230501_Generic.zip
p34809489_122140_Generic.zip

Table A-4 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p35445981_122140_Generic.zip
p34809489_122140_Generic.zip

Table A-5 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p34824004_122140_Generic.zip

Patches Applied During Provisioning — 23.2.2

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 23.2.2.

Table A-6 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-7 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-8 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p31713053_122140_Linux-x86-64.zip
p30922431_122140_Generic.zip
p35255955_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-9 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p35255955_122140_Generic.zip

Table A-10 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p34824004_122140_Generic.zip

Patches Applied During Provisioning — 23.1.1 and 23.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 23.1.1 and 23.1.3.

Table A-11 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-12 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-13 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip

Table A-13 (Cont.) SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p34824004_122140_Generic.zip
p32121987_122140_Generic.zip
p34765492_122140_Generic.zip

Table A-14 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p34824004_122140_Generic.zip

Table A-15 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p34824004_122140_Generic.zip

Patches Applied During Provisioning — 22.4.2

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 22.4.2.

Table A-16 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-17 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip

Table A-17 (Cont.) MFT Service Type — 12.2.1.3.0

Bundle Name
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-18 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p34540715_122140_Generic.zip
p32121987_122140_Generic.zip
p34765492_122140_Generic.zip

Table A-19 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p34540715_122140_Generic.zip
p32463347_12214220827_Generic.zip
p32395225_12214220827_Generic.zip
p34765492_122140_Generic.zip

Table A-20 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p34195608_122140_Generic.zip

Patches Applied During Provisioning — 22.3.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 22.3.3.

Table A-21 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-22 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-23 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p34195608_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-24 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p34195608_122140_Generic.zip
p32463347_12214220315_Generic.zip

Table A-25 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p34195608_122140_Generic.zip

Patches Applied During Provisioning — 22.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 22.1.3.

Table A-26 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-27 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-28 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p33696548_122140_Generic.zip
p32121987_122140_Generic.zip
p31192457_12214211221_Generic.zip

Table A-29 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p33696548_122140_Generic.zip

Table A-30 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip

Table A-30 (Cont.) BAM Service Type — 12.2.1.4.0

Bundle Name
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p33696548_122140_Generic.zip

Patches Applied During Provisioning — 22.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 22.1.1.

Table A-31 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-32 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-33 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p33696548_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-34 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip

Table A-34 (Cont.) MFT Service Type — 12.2.1.4.0

Bundle Name
p33696548_122140_Generic.zip

Table A-35 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip
p33696548_122140_Generic.zip

Patches Applied During Provisioning — 21.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 21.4.3.

Table A-36 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-37 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-38 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p32957445_122140_Generic.zip

Table A-38 (Cont.) SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p32121987_122140_Generic.zip

Table A-39 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip
p33671996_12214210930_Generic.zip
p33672131_122140_Generic.zip

Table A-40 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip

Patches Applied During Provisioning — 21.3.2 and 21.4.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 21.3.2 and 21.4.1.

Table A-41 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32944190_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-42 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-43 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p32957445_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-44 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip

Table A-45 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip

Patches Applied During Provisioning — 21.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 21.2.1.

Table A-46 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32720399_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-47 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28354063_122130_Generic.zip

Table A-48 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p32656931_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-49 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip

Table A-50 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip

Patches Applied During Provisioning — 21.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 21.1.1.

Table A-51 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p28012051_122130_Generic.zip
p32260099_122130_Generic.zip
p32144336_122130_Generic.zip

Table A-52 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28423565_122130_Generic.zip

Table A-53 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p32337168_122140_Generic.zip
p32121987_122140_Generic.zip

Table A-54 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip

Table A-55 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip

Patches Applied During Provisioning — 20.4.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 20.4.1.

Table A-56 SOA and OSB and B2B Service Type — 12.2.1.3.0

Bundle Name
p31834649_122130_Generic.zip
p28012051_122130_Generic.zip
p30059259_122130_Generic.zip

Table A-57 MFT Service Type — 12.2.1.3.0

Bundle Name
p26798713_122130_Generic.zip
p26437061_122130_Generic.zip
p26503442_122130_Generic.zip
p27578074_122130_Generic.zip
p26720529_122130_Generic.zip
p28415151_122130_Generic.zip
p28415157_122130_Generic.zip
p28423565_122130_Generic.zip

Table A-58 SOA and OSB and B2B Service Type — 12.2.1.4.0

Bundle Name
p30549478_122140_Generic.zip
p31903409_122140_Generic.zip
p31700519_122140_Generic.zip

Table A-59 MFT Service Type — 12.2.1.4.0

Bundle Name
p30686755_122140_Generic.zip

Table A-60 BAM Service Type — 12.2.1.4.0

Bundle Name
p31047981_122140_Generic.zip
p30334074_122140_Generic.zip
p31466508_122140_Generic.zip

Patches Applied During Provisioning — 20.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 20.3.1.

Table A-61 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28489610_122130_Generic.zip
N/A	p28012051_122130_Generic.zip
N/A	p31402620_122130_Generic.zip

Table A-62 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Table A-63 SOA and OSB and B2B Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30549478_122140_Generic.zip
N/A	p31396632_122140_Generic.zip

Table A-64 MFT Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30686755_122140_Generic.zip

Table A-65 BAM Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p31047981_122140_Generic.zip
N/A	p30334074_122140_Generic.zip
N/A	p31466508_122140_Generic.zip

Patches Applied During Provisioning — 20.2.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 20.2.3.

Table A-66 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28720963_122130_Generic.zip
N/A	p28489610_122130_Generic.zip
N/A	p28012051_122130_Generic.zip

Table A-67 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Table A-68 SOA and OSB and B2B Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30995852_122140_Generic.zip
N/A	p30549478_122140_Generic.zip

Table A-69 MFT Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30686755_122140_Generic.zip

Table A-70 BAM Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p31047981_122140_Generic.zip
N/A	p30334074_122140_Generic.zip
N/A	p31466508_122140_Generic.zip

Patches Applied During Provisioning — 20.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 20.2.1.

Table A-71 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28720963_122130_Generic.zip
N/A	p28489610_122130_Generic.zip
N/A	p28012051_122130_Generic.zip

Table A-72 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Table A-73 SOA and OSB and B2B Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30995852_122140_Generic.zip
N/A	p30549478_122140_Generic.zip

Table A-74 MFT Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30686755_122140_Generic.zip

Patches Applied During Provisioning — 19.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.4.3.

Table A-75 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28720963_122130_Generic.zip
N/A	p28489610_122130_Generic.zip
N/A	p28012051_122130_Generic.zip

Table A-76 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Table A-77 SOA and OSB and B2B Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30995852_122140_Generic.zip
N/A	p30549478_122140_Generic.zip

Table A-78 MFT Service Type — 12.2.1.4.0

Name	Bundle Name
N/A	p30686755_122140_Generic.zip

Patches Applied During Provisioning — 19.4.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.4.1.

Table A-79 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28720963_122130_Generic.zip
N/A	p28489610_122130_Generic.zip

Table A-80 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Patches Applied During Provisioning — 19.3.2

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.3.2.

Table A-81 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p28720963_122130_Generic.zip
N/A	p28489610_122130_Generic.zip

Table A-82 MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26798713_122130_Generic.zip

Table A-82 (Cont.) MFT Service Type — 12.2.1.3.0

Name	Bundle Name
N/A	p26437061_122130_Generic.zip
N/A	p26503442_122130_Generic.zip
N/A	p27578074_122130_Generic.zip
N/A	p26720529_122130_Generic.zip
N/A	p28415151_122130_Generic.zip
N/A	p28415157_122130_Generic.zip
N/A	p28423565_122130_Generic.zip

Patches Applied During Provisioning — 19.2.2

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.2.2.

Table A-83 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p28720963_122130_Gener ic.zip	N/A
N/A	p28489610_122130_Gener ic.zip	N/A

Table A-84 MFT Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gener ic.zip	N/A
N/A	p26437061_122130_Gener ic.zip	N/A
N/A	p26503442_122130_Gener ic.zip	N/A
N/A	p27578074_122130_Gener ic.zip	N/A
N/A	p26720529_122130_Gener ic.zip	N/A
N/A	p28415151_122130_Gener ic.zip	N/A
N/A	p28415157_122130_Gener ic.zip	N/A
N/A	p28423565_122130_Gener ic.zip	N/A

Patches Applied During Provisioning — 19.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.2.1.

Table A-85 SOA Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
N/A	p23116819_121300_Gen eric.zip	N/A
Bundle Patch	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
N/A	p23756692_1213016071 9_Generic.zip	N/A
Cloud Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
N/A	p24347304_1213016071 9_Generic.zip	N/A
N/A	p23057550_1213016071 9_Generic.zip	N/A
N/A	p24485566_1213016071 9_Generic.zip	N/A
N/A	p22117696_1213016071 9_Generic.zip	N/A

Table A-86 OSB Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
N/A	p23116819_121300_Gen eric.zip	N/A
N/A	p23756692_1213016071 9_Generic.zip	N/A
N/A	p23057550_1213016071 9_Generic.zip	N/A

Table A-87 SOA and OSB Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
N/A	p23116819_121300_Gener ic.zip	N/A
N/A	p23756692_12130160719_ Generic.zip	N/A
N/A	p24347304_12130160719_ Generic.zip	N/A
N/A	p23057550_12130160719_ Generic.zip	N/A
N/A	p24485566_12130160719_ Generic.zip	N/A
N/A	p22117696_12130160719_ Generic.zip	N/A

Table A-88 API Manager Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1 (Bundle Patch 6)
Bundle Patch	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419 (Bundle Patch 12.1.3.0.1(ID:151209.1205))
Bundle Patch	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1 (DB Schema)
N/A	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3 (Core Template)
N/A	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0 (Adapter Pack)
N/A	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499

Table A-88 (Cont.) API Manager Service Type — 12.1.3

Name	Bundle Name	Description
N/A	p24325490_12130160419_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-89 B2B Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
N/A	p23116819_121300_Generic.zip	N/A
N/A	p23756692_1213016071_9_Generic.zip	N/A
N/A	p24347304_1213016071_9_Generic.zip	N/A
N/A	p23057550_1213016071_9_Generic.zip	N/A
N/A	p24485566_1213016071_9_Generic.zip	N/A
N/A	p25030652_1213016071_9_Generic.zip	N/A
N/A	p22117696_1213016071_9_Generic.zip	(Included Support for SHA2 in SMIME toolkit Patch)
N/A	p17217722_121300_Generic.zip	N/A
N/A	p25030652_1213016071_9_Generic.zip	N/A

Table A-90 MFT Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch	p23116819_121300_Generic.zip	(Bundle Patch 12.1.3.0.1(ID:151209.1205))

Table A-90 (Cont.) MFT Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-91 SOA and OSB and B2B Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	Uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch/Adapter Pack	p27846009_12212170627S OACSBundlePatch_Generi c.zip	Bundle Patch
N/A	p27758215_122120_Gener ic.zip	N/A

Table A-92 insight Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	Bundle Patch

Table A-93 MFT Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A

Table A-94 SOA and OSB and B2B Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p28720963_122130_Gen eric.zip	N/A
N/A	p28489610_122130_Gen eric.zip	N/A

Table A-95 MFT Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gen eric.zip	N/A
N/A	p26437061_122130_Gen eric.zip	N/A
N/A	p26503442_122130_Gen eric.zip	N/A
N/A	p27578074_122130_Gen eric.zip	N/A
N/A	p26720529_122130_Gen eric.zip	N/A
N/A	p28415151_122130_Gen eric.zip	N/A
N/A	p28415157_122130_Gen eric.zip	N/A
N/A	p28423565_122130_Gen eric.zip	N/A

Patches Applied During Provisioning — 19.1.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.1.5.

Table A-96 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p28720963_122130_Gener ic.zip	N/A
N/A	p28489610_122130_Gener ic.zip	N/A

Table A-97 MFT Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gener ic.zip	N/A
N/A	p26437061_122130_Gener ic.zip	N/A
N/A	p26503442_122130_Gener ic.zip	N/A
N/A	p27578074_122130_Gener ic.zip	N/A
N/A	p26720529_122130_Gener ic.zip	N/A
N/A	p28415151_122130_Gener ic.zip	N/A
N/A	p28415157_122130_Gener ic.zip	N/A
N/A	p28423565_122130_Gener ic.zip	N/A

Table A-98 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	uptake 16.4.1 Cloud Adapters for OSB

Table A-98 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A
N/A	p27758215_122120_Gener ic.zip	N/A

Table A-99 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A

Table A-100 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gen eric.zip	N/A
N/A	p25378006_122120_Gen eric.zip	N/A
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A

Table A-101 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-101 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-102 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A

Table A-103 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-103 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-104 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-105 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gener ic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_12130160719_ Generic.zip	N/A

Table A-106 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 19.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 19.1.3.

Table A-107 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p28720963_122130_Gen eric.zip	N/A
N/A	p28489610_122130_Gen eric.zip	N/A

Table A-108 MFT Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gen eric.zip	N/A
N/A	p26437061_122130_Gen eric.zip	N/A
N/A	p26503442_122130_Gen eric.zip	N/A
N/A	p27578074_122130_Gen eric.zip	N/A
N/A	p26720529_122130_Gen eric.zip	N/A
N/A	p28415151_122130_Gen eric.zip	N/A
N/A	p28415157_122130_Gen eric.zip	N/A
N/A	p28423565_122130_Gen eric.zip	N/A

Table A-109 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	uptake 16.4.1 Cloud Adapters for OSB

Table A-109 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25340179_122120_Gen eric.zip	N/A
N/A	p25372894_122120_Gen eric.zip	N/A
N/A	p25030652_122120_Gen eric.zip	N/A
N/A	p26448284_122120_Gen eric.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gen eric.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A
N/A	p27758215_122120_Gen eric.zip	N/A

Table A-110 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-111 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A

Table A-112 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-112 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-113 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A

Table A-114 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-114 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-115 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-116 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gen eric.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071 9_Generic.zip	N/A

Table A-117 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.4.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.4.5.

Table A-118 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p28720963_122130_Gener ic.zip	N/A
N/A	p28489610_122130_Gener ic.zip	N/A

Table A-119 MFT Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gener ic.zip	N/A
N/A	p26437061_122130_Gener ic.zip	N/A
N/A	p26503442_122130_Gener ic.zip	N/A
N/A	p27578074_122130_Gener ic.zip	N/A
N/A	p26720529_122130_Gener ic.zip	N/A
N/A	p28415151_122130_Gener ic.zip	N/A
N/A	p28415157_122130_Gener ic.zip	N/A
N/A	p28423565_122130_Gener ic.zip	N/A

Table A-120 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	uptake 16.4.1 Cloud Adapters for OSB

Table A-120 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A
N/A	p27758215_122120_Gener ic.zip	N/A

Table A-121 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A

Table A-122 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gen eric.zip	N/A
N/A	p25378006_122120_Gen eric.zip	N/A
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A

Table A-123 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-123 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-124 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A

Table A-125 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-125 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-126 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-127 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gener ic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_12130160719_ Generic.zip	N/A

Table A-128 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.4.3.

Table A-129 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p27507607_122130_Gen eric.zip	N/A

Table A-130 MFT Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p26798713_122130_Gen eric.zip	N/A
N/A	p26437061_122130_Gen eric.zip	N/A
N/A	p26503442_122130_Gen eric.zip	N/A
N/A	p27578074_122130_Gen eric.zip	N/A
N/A	p26720529_122130_Gen eric.zip	N/A
N/A	p28415151_122130_Gen eric.zip	N/A
N/A	p28415157_122130_Gen eric.zip	N/A
N/A	p28423565_122130_Gen eric.zip	N/A

Table A-131 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	N/A

Table A-131 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25372894_122120_Gen eric.zip	N/A
N/A	p25030652_122120_Gen eric.zip	N/A
N/A	p26448284_122120_Gen eric.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gen eric.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A
N/A	p27758215_122120_Gen eric.zip	N/A

Table A-132 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-133 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A

Table A-134 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A

Table A-134 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-135 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A

Table A-136 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1

Table A-136 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-137 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-138 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gen eric.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071 9_Generic.zip	N/A

Table A-139 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.3.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.3.5.

Table A-140 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p27507607_122130_Gener ic.zip	N/A

Table A-141 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A
N/A	p27758215_122120_Gener ic.zip	

Table A-142 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A

Table A-142 (Cont.) MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-143 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gen eric.zip	N/A
N/A	p25378006_122120_Gen eric.zip	N/A
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A

Table A-144 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-145 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A

Table A-146 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-147 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-148 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-148 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p25030652_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071_9_Generic.zip	N/A

Table A-149 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.3.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.3.3.

Table A-150 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p27507607_122130_Generic.zip	N/A

Table A-151 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Generic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Generic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Generic.zip	N/A
N/A	p24902015_122120_Generic.zip	uptake 16.4.1 Cloud Adapters for OSB

Table A-151 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A
N/A	p27758215_122120_Gener ic.zip	

Table A-152 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A

Table A-153 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gen eric.zip	N/A
N/A	p25378006_122120_Gen eric.zip	N/A
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A

Table A-154 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-154 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-155 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-156 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-157 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499

Table A-157 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-158 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gener ic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_12130160719_ Generic.zip	N/A

Table A-159 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A

Table A-159 (Cont.) MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.3.1.

Table A-160 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p27507607_122130_Gen eric.zip	N/A

Table A-161 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	N/A
N/A	p25372894_122120_Gen eric.zip	N/A
N/A	p25030652_122120_Gen eric.zip	N/A
N/A	p26448284_122120_Gen eric.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gen eric.zip	RCA: error notification rule sends out fault url with internal host and port
Bundle Patch	p27846009_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A
N/A	p27758215_122120_Gen eric.zip	

Table A-162 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-163 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
Bundle Patch	p27846009_12212170627S OACSBundlePatch_Generi c.zip	N/A

Table A-164 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-165 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-166 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-167 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-168 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-168 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p25030652_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_12130160719_Generic.zip	N/A

Table A-169 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.2.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.2.5.

Table A-170 SOA and B2B Cluster Service Type — 12.2.1.3.0

Name	Bundle Name	Description
N/A	p27507607_122130_Generic.zip	N/A

Table A-171 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Generic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Generic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Generic.zip	N/A
N/A	p24902015_122120_Generic.zip	uptake 16.4.1 Cloud Adapters for OSB

Table A-171 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25340179_122120_Gen eric.zip	N/A
N/A	p25372894_122120_Gen eric.zip	N/A
N/A	p25030652_122120_Gen eric.zip	N/A
N/A	p26448284_122120_Gen eric.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gen eric.zip	RCA: error notification rule sends out fault url with internal host and port
N/A	p25378006_1221217062 7SOACSBundlePatch_Ge neric.zip	N/A

Table A-172 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-173 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
N/A	p25378006_12212170627S OACSBundlePatch_Generi c.zip	N/A

Table A-174 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A

Table A-174 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-175 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-176 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-177 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499

Table A-177 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Adapter Pack	p24325490_12130160419_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-178 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071_9_Generic.zip	N/A

Table A-179 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A

Table A-179 (Cont.) MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Patches Applied During Provisioning — 18.2.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.2.3.

Table A-180 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-181 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-181 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-182 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-183 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-183 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-184 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-184 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gener ic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_12130160719_Generic.zip	N/A

Table A-185 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-186 SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	N/A
N/A	p26448284_122120_Gener ic.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance
N/A	p27379937_122120_Gener ic.zip	RCA: error notification rule sends out fault url with internal host and port

Table A-186 (Cont.) SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
N/A	p25378006_12212170627SOACSBundlePatch_Generic.zip	N/A

Table A-187 MFT Cluster Service Type — 12.2.1

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Table A-188 Insight Cluster Service Type — 12.2.1

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A
N/A	p25378006_12212170627SOACSBundlePatch_Generic.zip	N/A

Patches Applied During Provisioning — 18.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.2.1.

Table A-189 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1

Table A-189 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A

Table A-190 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A

Table A-191 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-191 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071_9_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071_9_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071_9_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071_9_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071_9_ Generic.zip	N/A

Table A-192 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-193 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gen eric.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071 9_Generic.zip	N/A

Table A-194 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-195 SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility

Table A-195 (Cont.) SOA and B2B Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	N/A
N/A	p25372894_122120_Gen eric.zip	N/A
N/A	p25030652_122120_Gen eric.zip	N/A
N/A	p26448284_122120_Gen eric.zip	Global settings was not persisted correctly for osb 12.2.1.2 instance. Newly added patch in 18.1.5.
N/A	p27379937_122120_Gen eric.zip	RCA: error notification rule sends out fault url with internal host and port. Newly added patch in 18.1.5.

Table A-196 Insight Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A

Table A-197 MFT Cluster Service Type — 12.2.1.2.0

Name	Bundle Name	Description
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Patches Applied During Provisioning — 18.1.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.1.5.

Table A-198 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-199 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A

Table A-199 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p24485566_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071_9_Generic.zip	N/A

Table A-200 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-201 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-201 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-202 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Gen eric.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071 9_Generic.zip	N/A

Table A-203 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-204 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A
N/A	p25030652_122120_Gener ic.zip	
N/A	p26448284_122120_Gener ic.zip	
N/A	p27379937_122120_Gener ic.zip	

Table A-205 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p27379937_122120_Gener ic.zip	N/A
N/A	p25378006_122120_Gener ic.zip	N/A

Table A-206 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A

Patches Applied During Provisioning — 18.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.1.3.

Table A-207 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-208 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1

Table A-208 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gener eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A

Table A-209 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-210 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS

Table A-210 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-211 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A

Table A-211 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071_9_Generic.zip	N/A

Table A-212 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-213 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Generic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Generic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Generic.zip	N/A
N/A	p24902015_122120_Generic.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Generic.zip	N/A
N/A	p25372894_122120_Generic.zip	N/A

Table A-214 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p25033100_122120_Generic.zip	N/A
N/A	p25378006_122120_Generic.zip	N/A

Table A-214 (Cont.) Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24654879_122120_Gener ic.zip	N/A

Table A-215 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24708363_122120_Gen eric.zip	N/A
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Patches Applied During Provisioning — 18.1.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 18.1.1.

Table A-216 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-217 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A

Table A-218 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-219 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - Bundle Patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 21473608 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - MERGE REQUEST ON TOP OF SOA BP 12.1.3.0.160419 FOR BUGS 20845360 21918757

Table A-220 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-220 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p25030652_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p17217722_121300_Generic.zip	N/A
Included Support for SHA2 in SMIME toolkit Patch	p25030652_1213016071_9_Generic.zip	N/A

Table A-221 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW BREAKING FOR ADMIN SERVER ACCESS IN SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-222 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Generic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Generic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Generic.zip	N/A
N/A	p24902015_122120_Generic.zip	uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Generic.zip	N/A
N/A	p25372894_122120_Generic.zip	N/A

Table A-223 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p25033100_122120_Generic.zip	N/A

Table A-223 (Cont.) Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p25378006_122120_Gener ic.zip	N/A
N/A	p24654879_122120_Gener ic.zip	N/A

Table A-224 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24708363_122120_Gen eric.zip	N/A
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Patches Applied During Provisioning — 17.4.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.4.5.

Table A-225 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-225 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A

Table A-226 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-227 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A

Table A-227 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A

Table A-228 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Generic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Generic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Generic.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Generic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_12130160419_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-229 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-229 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p17217722_121300_Gener eric.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_1213016071 9_Generic.zip	N/A

Table A-230 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-231 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	Uptake 16.4.1 Cloud Adapters for OSB

Table A-231 (Cont.) B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A

Table A-232 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Table A-233 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24708363_122120_Gen eric.zip	N/A
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Patches Applied During Provisioning — 17.4.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.4.3.

Table A-234 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1

Table A-234 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23756692_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071_9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071_9_Generic.zip	N/A

Table A-235 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A

Table A-236 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-236 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-237 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-238 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p17217722_121300_Gener ic.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-239 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-240 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gener ic.zip	SOA BP for WLS 12.2.1.2.1 compatibility

Table A-240 (Cont.) B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p24901339_122120_Gener ic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gener ic.zip	N/A
N/A	p24902015_122120_Gener ic.zip	Uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gener ic.zip	N/A
N/A	p25372894_122120_Gener ic.zip	N/A

Table A-241 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Table A-242 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24708363_122120_Gen eric.zip	N/A
N/A	p25177003_122120_Gen eric.zip	N/A
N/A	p25909495_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Patches Applied During Provisioning — 17.4.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.4.1.

Table A-243 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-244 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A

Table A-244 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A

Table A-245 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A

Table A-246 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Generic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Generic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Generic.zip	[APIM] - API Manager DB schema changes in 12.1.3

Table A-246 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Core Template	p20225320_121300_Generic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041_9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041_9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-247 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Generic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Generic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p17217722_121300_Generic.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_12130160719_Generic.zip	N/A

Table A-248 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-249 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	Uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	N/A
N/A	p25372894_122120_Gen eric.zip	N/A

Table A-250 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A
N/A	p24654879_122120_Gen eric.zip	N/A

Table A-251 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p24708363_122120_Gen eric.zip	N/A
N/A	p25177003_122120_Gen eric.zip	N/A

Table A-251 (Cont.) MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
N/A	p25909495_122120_Gener eric.zip	N/A
N/A	p24654879_122120_Gener eric.zip	N/A

Patches Applied During Provisioning — 17.3.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.3.5.

Table A-252 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-253 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1

Table A-253 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-254 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-255 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS

Table A-255 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-256 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-256 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p17217722_121300_Gener ic.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-257 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-258 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p25033100_122120_Gen eric.zip	MAA: CCW breaking for Admin Server access in SOACS
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	Uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	

Table A-259 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A

Table A-260 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p24708363_122120_Gener ic.zip	N/A
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Patches Applied During Provisioning — 17.3.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.3.3.

Table A-261 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_12130160719_ Generic.zip	N/A

Table A-262 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-263 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-264 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-265 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-265 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p17217722_121300_Gener ic.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_12130160719_Generic.zip	N/A

Table A-266 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-267 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p26248598_122120_Gen eric.zip	SOA BP for WLS 12.2.1.2.1 compatibility
N/A	p25033100_122120_Gen eric.zip	MAA: CCW breaking for Admin Server access in SOACS
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Gen eric.zip	N/A
N/A	p24902015_122120_Gen eric.zip	Uptake 16.4.1 Cloud Adapters for OSB
N/A	p25340179_122120_Gen eric.zip	N/A

Table A-268 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A

Table A-269 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p24708363_122120_Gener ic.zip	N/A
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Patches Applied During Provisioning — 17.3.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.3.1.

Table A-270 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-271 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-271 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-272 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p22117696_1213016071 9_Generic.zip	N/A

Table A-273 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-274 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-274 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22117696_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p17217722_121300_Generic.zip	Included support for SHA2 in SMIME toolkit patch
Bundle Patch/Adapter Pack	p25030652_12130160719_Generic.zip	N/A

Table A-275 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Generic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-276 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p25033100_122120_Generic.zip	MAA: CCW breaking for Admin Server access in SOACS
N/A	p25378006_122120_Generic.zip	N/A
N/A	p24901339_122120_Generic.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p25636477_122120_Generic.zip	N/A
N/A	p24902015_122120_Generic.zip	Uptake 16.4.1 Cloud Adapters for OSB

Table A-277 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Generic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Generic.zip	N/A

Table A-278 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p24708363_122120_Gener ic.zip	N/A
N/A	p25177003_122120_Gener ic.zip	N/A
N/A	p25909495_122120_Gener ic.zip	N/A

Patches Applied During Provisioning — 17.2.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.2.5.

Table A-279 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-280 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-280 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-281 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-282 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gener ic.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener ic.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_12130160419_ Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-283 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-284 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gen eric.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-285 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gen eric.zip	N/A

Table A-286 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p25033100_122120_Gen eric.zip	MAA: CCW breaking for Admin Server access in SOACS
N/A	p24708363_122120_Gen eric.zip	STRESS:MFT:java.sql.SQLException on purge command execution
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p24902015_122120_Gen eric.zip	Uptake 16.4.1 Cloud Adapters for OSB

Patches Applied During Provisioning — 17.2.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.2.1.

Table A-287 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A

Table A-287 (Cont.) SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-288 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-289 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-289 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-290 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-291 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p25030652_12130160719_ Generic.zip	N/A

Table A-292 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-293 Insight Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p25378006_122120_Gener ic.zip	N/A

Table A-294 B2B with SOA and OSB – 12.2.1.2

Name	Bundle Name	Description
N/A	p25033100_122120_Gen eric.zip	MAA: CCW breaking for Admin Server access in SOACS
N/A	p24708363_122120_Gen eric.zip	STRESS:MFT:java.sql.SQLException on purge command execution
N/A	p24901339_122120_Gen eric.zip	Uptaking 16.4.1 ICS SDK for SOA
N/A	p24902015_122120_Gen eric.zip	Uptake 16.4.1 Cloud Adapters for OSB

Patches Applied During Provisioning — 17.1.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 17.1.3.

Table A-295 SOA Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS

Table A-296 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-297 Service Bus Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-298 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-299 SOA and Service Bus Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS

Table A-300 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1

Table A-300 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-301 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
DB Schema	p20311552_121300_Gen eric.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gen eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-302 SOA and B2B Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gen eric.zip	MAA: CCW breaking for administration server access in SOACS

Table A-303 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A
Support for SHA2 in SMIME Toolkit Patch	p17217722_121300_Gener ic.zip	Included support for SHA2 in SMIME toolkit patch

Table A-304 MFT Cluster Service Type – 12.2.1.2

Name	Bundle Name	Description
CCW Patch	p25033100_122120_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
N/A	p24708363_122120_Gener ic.zip	STRESS:MFT:java.sql.SQLExce ption on purge command execution

Table A-305 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
CCW Patch	p25033100_121300_Gener ic.zip	MAA: CCW breaking for administration server access in SOACS
Bundle Patch 6	p23116819_121300_Gener ic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Patches Applied During Provisioning — 16.4.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 16.4.5.

Table A-306 SOA Cluster Service Type – 12.2.1

Name	Bundle Name	Description
Insight	p24818744_122100_Gen eric.zip	N/A
Insight	p24334160_122100_Gen eric.zip	Merge request on top of 12.2.1.0.0 for bugs 21918757 and 24322910
Insight	p23526422_122100_Gen eric.zip	Change logging of message in CallbackHandler from WARNING to FINE
Insight	p22978098_122100_Gen eric.zip	SOA patch: Indicators configured on response payload coming from a DB adapter do not work
Insight	p23708639_122100_Gen eric.zip	Tracking API changes for Insight
Adapter Pack	p22682253_122100_Gen eric.zip	[SOA] - Enabling cloud adapters
Adapter Pack	p22698114_122100_Gen eric.zip	[OSB] - UI SDK JARs for the cloud adapter pack

Table A-307 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-308 Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p24818744_122100_Gener ic.zip	N/A
Insight	p24343598_122100_Gener ic.zip	OSB agent template should point to the right procmon-client JAR
Insight	p22978098_122100_Gener ic.zip	SOA Patch: Indicators configured on Response payload coming from a DB ADapter do not work
Insight	p23708639_122100_Gener ic.zip	Tracking API Changes For Insight
Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] - Enabling cloud adapters
Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] - UI SDK JARs for the cloud adapter pack

Table A-309 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A
Bundle Patch/Adapter Pack	p23756692_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_ Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_ Generic.zip	N/A

Table A-310 SOA and Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p24818744_122100_Gener ic.zip	N/A
Insight	p24334160_122100_Gener ic.zip	Merge request on top of 12.2.1.0.0 for bugs 21918757 and 24322910

Table A-310 (Cont.) SOA and Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p23526422_122100_Gener ic.zip	Change logging of message in CallbackHandler from WARNING to FINE
Insight	p22978098_122100_Gener ic.zip	SOA Patch: Indicators configured on Response payload coming from a DB Adapter do not work
Insight	p23708639_122100_Gener ic.zip	Tracking API Changes For Insight
Insight	p24343598_122100_Gener ic.zip	OSB agent template should point to the right procmon-client JAR
Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] - Enabling cloud adapters
Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] - UI SDK JARs for the cloud adapter pack

Table A-311 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gen eric.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gen eric.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gen eric.zip	N/A
Bundle Patch/Adapter Pack	p23756692_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_1213016071 9_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_1213016071 9_Generic.zip	N/A

Table A-312 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] - bundle patch 12.1.3.0.160419
Bundle Patch 12.1.3.0.1 (ID:151209.1205)	p22364187_121300_Gen eric.zip	[OSB] - OSB bundle patch 12.1.3.0.1

Table A-312 (Cont.) API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
DB Schema	p20311552_121300_Gener eric.zip	[APIM] - API Manager DB schema changes in 12.1.3
Core Template	p20225320_121300_Gener eric.zip	[APIM] - API Manager for OSB 12.1.3.0.0
Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] - Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-313 SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p24818744_122100_Gener ic.zip	N/A
Insight	p24334160_122100_Gener ic.zip	Merge request on top of 12.2.1.0.0 for bugs 21918757 and 24322910
Insight	p23526422_122100_Gener ic.zip	Change logging of message in CallbackHandler from WARNING to FINE
Insight	p22978098_122100_Gener ic.zip	SOA Patch: Indicators configured on Response payload coming from a DB Adapter do not work
Insight	p23708639_122100_Gener ic.zip	Tracking API Changes For Insight
Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] - Enabling cloud adapters
Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] - UI SDK JARs for the cloud adapter pack

Table A-314 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p20780464_121301_Gener ic.zip	[SOA] - Cloud adapter pack SOA+OSB for 12.1.3.0.0 SOA BP1
Bundle Patch/Adapter Pack	p22364187_121300_Gener ic.zip	[OSB] - OSB Bundle Patch 12.1.3.0.1
Bundle Patch/Adapter Pack	p23116819_121300_Gener ic.zip	N/A

Table A-314 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p23756692_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24347304_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p23057550_12130160719_Generic.zip	N/A
Bundle Patch/Adapter Pack	p24485566_12130160719_Generic.zip	N/A
Support for SHA2 in SMIME Toolkit Patch	p17217722_121300_Generic.zip	N/A

Table A-315 MFT Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Bundle Patch/Adapter Pack	p22661110_122100_Generic.zip	PSR:PERF:SOACS:MFT:SFTP Server - Low throughput with large files — FILELASTMODINTERVAL
Bundle Patch/Adapter Pack	p23484802_122100_Generic.zip	Merge request on top of 12.2.1.0.0 for bugs 22698554 and 22931138
Bundle Patch/Adapter Pack	p22290181_122100_Generic.zip	N/A

Table A-316 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
Bundle Patch 6	p23116819_121300_Generic.zip	N/A
Bundle Patch 12.1.3.0.1(ID:151209.1205)	p22364187_121300_Generic.zip	[OSB] - OSB Bundle patch 12.1.3.0.1

Table A-317 Integration Analytics Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p18668213_122100_Generic.zip	Old row values are not consistent with the set default value
Insight	p23708639_122100_Generic.zip	Tracking API changes for Insight
Insight	p21922025_122100_Generic.zip	API update of many parameterized filters to a business query is very slow

Table A-317 (Cont.) Integration Analytics Cluster Service Type — 12.2.1

Name	Bundle Name	Description
Insight	p24328873_122100_Gen eric.zip	Merge request on top of 12.2.1.0.0 for bugs 21684609 and 21922843
Insight	p24818744_122100_Gen eric.zip	N/A
Insight	p23587247_122100_Gen eric.zip	N/A
BAM	p22480338_122100_Gen eric.zip	N/A
BAM	p22700969_122100_Gen eric.zip	N/A
BAM	p22986069_122100_Gen eric.zip	N/A
BAM	p22861896_122100_Gen eric.zip	N/A
BAM	p21769609_122100_Gen eric.zip	N/A
BAM	p23216407_122100_Gen eric.zip	N/A
BAM	p21436844_122100_Gen eric.zip	N/A

Patches Applied During Provisioning — 16.4.1

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 16.4.1.

Table A-318 SOA Cluster Service Type – 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p24382279_122100_Gener ic.zip	Insight OPatch For 16.4.1
12.2.1 Insight	p24334160_122100_Gener ic.zip	Merge request on top OF 12.2.1.0.0 for bugs 21918757 and 24322910
12.2.1 Insight	p23526422_122100_Gener ic.zip	Change logging of message in CallbackHandler from WARNING to FINE.
12.2.1 Insight	p22978098_122100_Gener ic.zip	SOA Patch: Indicators configured on a response payload coming from a DB Adapter do not work.
12.2.1 Insight	p23708639_122100_Gener ic.zip	Tracking API Changes For Insight

Table A-318 (Cont.) SOA Cluster Service Type – 12.2.1

Name	Bundle Name	Description
12.2.1 Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack

Table A-319 SOA Cluster Service Type – 12.1.3

Name	Bundle Name	Description
12.1.3 Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
12.1.3 Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gen eric.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
12.1.3 Adapter Pack	p24325490_1213016041 9_Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-320 Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p24382279_122100_Gen eric.zip	Insight OPatch For 16.4.1
12.2.1 Insight	p24343598_122100_Gen eric.zip	OSB agent template should point to the right PROCMON-CLIENT JAR.
12.2.1 Insight	p22978098_122100_Gen eric.zip	SOA Patch: Indicators configured on a response payload coming from a DB Adapter do not work.
12.2.1 Insight	p23708639_122100_Gen eric.zip	Tracking API Changes For Insight
12.2.1 Adapter Pack	p22682253_122100_Gen eric.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gen eric.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack

Table A-321 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
12.1.3 Adapter Pack	p24325490_12130160419_ Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-322 SOA and Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p24382279_122100_Gener ic.zip	Insight OPatch For 16.4.1
12.2.1 Insight	p24334160_122100_Gener ic.zip	Merge request on top OF 12.2.1.0.0 for bugs 21918757 24322910
12.2.1 Insight	p23526422_122100_Gener ic.zip	Change logging of message in CallbackHandler from WARNING to FINE.
12.2.1 Insight	p22978098_122100_Gener ic.zip	SOA Patch: Indicators configured on a response payload coming from a DB Adapter do not work.
12.2.1 Insight	p23708639_122100_Gener ic.zip	Tracking API Changes For Insight
12.2.1 Insight	p24343598_122100_Gener ic.zip	OSB agent template should point to the right PROCMON-CLIENT JAR.
12.2.1 Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack

Table A-323 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419

Table A-323 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
12.1.3 Adapter Pack	p24325490_12130160419_ Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 21918757

Table A-324 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Cloud Adapter Pack SOA+OSB	p20780464_121301_Gen eric.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP
12.1.3 Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gen eric.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 DB Schema	p20311552_121300_Gen eric.zip	[APIM] [12.1.3] - API manager DB schema changes in 12.1.3
12.1.3 Core Template	p20225320_121300_Gen eric.zip	[APIM] [12.1.3] - API Manager for OSB 12.1.3.0.0
12.1.3 Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p24325490_1213016041 9_Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 20845360 and 21918757

Table A-325 SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p24382279_122100_Gen eric.zip	Insight OPatch For 16.4.1
12.2.1 Insight	p24334160_122100_Gen eric.zip	Merge request on top OF 12.2.1.0.0 for bugs 21918757 and 24322910
12.2.1 Insight	p23526422_122100_Gen eric.zip	Change logging of message in CallbackHandler from WARNING to FINE.

Table A-325 (Cont.) SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p22978098_122100_Gener eric.zip	SOA Patch: Indicators configured on a response payload coming from a DB Adapter do not work.
12.2.1 Insight	p23708639_122100_Gener eric.zip	Tracking API Changes For Insight
12.2.1 Adapter Pack	p22682253_122100_Gener eric.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gener eric.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack

Table A-326 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Cloud Adapter Pack SOA+OSB	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_12130160419_Gener ic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for bugs 21473608 and 22568499
12.1.3 Adapter Pack	p24325490_12130160419_Gener ic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bugs 20845360 and 21918757

Table A-327 MFT Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Patch	p22661110_122100_Gener ic.zip	[MFT] [12.2.1] - PSR:PERF:SOACS:MFT:SFTP Server - Low through-put with big files - FILELASTMODINTERVAL
12.2.1 Patch	p23484802_122100_Gener ic.zip	[MFT] [12.2.1] - Merge Request on Top of 12.2.1.0.0 for bugs 22698554 and 22931138

Table A-328 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419

Table A-328 (Cont.) MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1

Table A-329 Integration Analytics Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight	p24382279_122100_Gen eric.zip	Insight OPatch For 16.4.1
12.2.1 Insight	p18668213_122100_Gen eric.zip	Old row values are not consistent with the set default value.
12.2.1 Insight	p22879420_122100_Gen eric.zip	Stress SOA Insight - Failure of the web server bridge in the graphic section of the console.
12.2.1 Insight	p23708639_122100_Gen eric.zip	Track API changes For Insight
12.2.1 Insight	p21922025_122100_Gen eric.zip	The API update of many parameterized filters to a business query is very slow.
12.2.1 Insight	p24328873_122100_Gen eric.zip	Merge request on top OF 12.2.1.0.0 for bugs 21684609 and 21922843

Patches Applied During Provisioning — 16.3.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 16.3.5.

Table A-330 SOA Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gen eric.zip	Bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work
12.2.1 Adapter Pack	p22682253_122100_Gen eric.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gen eric.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack
12.2.1 Insight Agent	p24318698_122100_Gen eric.zip	[INSIGHT_AGENT_BASE] [12.2.1] - [BASE] Insight OPatch For 16.3.5 RC2
12.2.1 Insight Agent	p22655174_122100_Gen eric.zip	[SOA] [12.2.1] - Insight Agent Patch

Table A-330 (Cont.) SOA Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight Agent	p23708639_122100_Gener eric.zip	[INSIGHT] [12.2.1] - Tracking API Changes For Insight - Bug 24007688

Table A-331 SOA Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-332 Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gener ic.zip	Bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work
12.2.1 Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack
12.2.1 Insight Agent	p24318698_122100_Gener ic.zip	[INSIGHT_AGENT_BASE] [12.2.1] - [BASE] Insight OPatch For 16.3.5 RC2
12.2.1 Insight Agent	p23327887_122100_Gener ic.zip	[SOA] [12.2.1] - Insight Agent Patch
12.2.1 Insight Agent	p23708639_122100_Gener ic.zip	[INSIGHT] [12.2.1] - Tracking API Changes For Insight - Bug 24007688

Table A-333 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419

Table A-333 (Cont.) Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-334 SOA and Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gen eric.zip	Bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work
12.2.1 Adapter Pack	p22682253_122100_Gen eric.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gen eric.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack
12.2.1 Insight Agent	p24318698_122100_Gen eric.zip	[INSIGHT_AGENT_BASE] [12.2.1] - [BASE] Insight OPatch For 16.3.5 RC2
12.2.1 Insight Agent	p22655174_122100_Gen eric.zip	[SOA] [12.2.1] - Insight Agent Patch
12.2.1 Insight Agent	p23327887_122100_Gen eric.zip	[SOA] [12.2.1] - Insight Agent Patch
12.2.1 Insight Agent	p23708639_122100_Gen eric.zip	[INSIGHT] [12.2.1] - Tracking API Changes For Insight - Bug 24007688

Table A-335 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gen eric.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gen eric.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 Adapter Pack	p23115406_1213016041 9_Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p20780464_121301_Gen eric.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-336 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1
12.1.3 DB Schema	p20311552_121300_Gener ic.zip	[APIM] [12.1.3] - API manager DB schema changes in 12.1.3
12.1.3 Core Template	p20225320_121300_Gener ic.zip	[APIM] [12.1.3] - API Manager for OSB 12.1.3.0.0
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-337 SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gener ic.zip	Bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work
12.2.1 Adapter Pack	p22682253_122100_Gener ic.zip	[SOA] [12.2.1] - Enabling Cloud adapters
12.2.1 Adapter Pack	p22698114_122100_Gener ic.zip	[OSB] [12.2.1] - UI SDK JARs for Cloud adapter pack
12.2.1 Insight Agent	p24318698_122100_Gener ic.zip	[INSIGHT_AGENT_BASE] [12.2.1] - [BASE] Insight OPatch For 16.3.5 RC2
12.2.1 Insight Agent	p22655174_122100_Gener ic.zip	[SOA] [12.2.1] - Insight Agent Patch
12.2.1 Insight Agent	p23708639_122100_Gener ic.zip	[INSIGHT] [12.2.1] - Tracking API Changes For Insight - Bug 24007688

Table A-338 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Gener ic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Gener ic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1

Table A-338 (Cont.) SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Adapter Pack	p23115406_12130160419_Generic.zip	[SOA] [12.1.3] - Merge Request on Top of SOA BP 12.1.3.0.160419 for Bugs 21473608 and 22568499
12.1.3 Adapter Pack	p20780464_121301_Generic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-339 MFT Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Patch	p22661110_122100_Generic.zip	[MFT] [12.2.1] - PSR:PERF:SOACS:MFT:SFTP Server - Low thrupt w/big files - FILELASTMODINTERVAL
12.2.1 Patch	p23484802_122100_Generic.zip	[MFT] [12.2.1] - Merge Request on Top of 12.2.1.0.0 for bugs 22698554 and 22931138

Table A-340 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6	p22970958_121300_Generic.zip	[SOA] [12.1.3] - Bundle Patch 12.1.3.0.160419
12.1.3 Bundle Patch 6	p22364187_121300_Generic.zip	[OSB] [12.1.3] - [OSB] Bundle Patch 12.1.3.0.1

Table A-341 Integration Analytics Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 BAM Server	p18668213_122100_Generic.zip	[INSIGHT] [12.2.1] - Insight Server Patch
12.2.1 BAM Server	p22879420_122100_Generic.zip	[INSIGHT] [12.2.1] - STRESS SOA Insight - Failure of Web Server bridge at graphic section of Console
12.2.1 Insight Agent	p24318698_122100_Generic.zip	[INSIGHT_AGENT_BASE] [12.2.1] - [BASE] Insight OPatch For 16.3.5 RC2
12.2.1 Insight Agent	p22655174_122100_Generic.zip	[SOA] [12.2.1] - Insight Agent Patch
12.2.1 Insight Agent	p18668213_122100_Generic.zip	[INSIGHT] [12.2.1] - Insight Server Patch

Patches Applied During Provisioning — 16.3.3

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 16.3.3.

Table A-342 SOA Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gener ic.zip	Fixes bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work.
12.2.1 Adapter Pack [SOA]	p22682253_122100_Gener ic.zip	Enable cloud adapters.
12.2.1 Adapter Pack [OSB]	p22698114_122100_Gener ic.zip	UI SDK JARs for the cloud adapter pack.
12.2.1 Insight Agent	p23589303_122100_Gene ric.zip	[BASE] Insight fix for OSB HOT bug 23558099.
12.2.1 Insight Agent	p22655174_122100_Gener ic.zip	Insight agent patch

Table A-343 SOA Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bug 21473608
12.1.3 Bug 22568499	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Gener ic.zip	Bundle patch 12.1.3.0.160419
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Gener ic.zip	[OSB] Bundle patch 12.1.3.0.1

Table A-344 Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gener ic.zip	Fixes bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work.
12.2.1 Adapter Pack [SOA]	p22682253_122100_Gener ic.zip	Enable cloud adapters.
12.2.1 Adapter Pack [OSB]	p22698114_122100_Gener ic.zip	UI SDK JARs for the cloud adapter pack.
12.2.1 Insight Agent	p23589303_122100_Gene ric.zip	[BASE] Insight fix for OSB HOT bug 23558099.

Table A-344 (Cont.) Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight Agent	p23327887_122100_Gener ic.zip	Insight agent patch

Table A-345 Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Adapter Pack	p23115406_1213016041 9_Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bug 21473608
12.1.3 Bug 22568499	p20780464_121301_Gen eric.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Gen eric.zip	Bundle patch 12.1.3.0.160419
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Gen eric.zip	[OSB] Bundle patch 12.1.3.0.1

Table A-346 SOA and Service Bus Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gen eric.zip	Fixes bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work.
12.2.1 Adapter Pack [SOA]	p22682253_122100_Gen eric.zip	Enable cloud adapters.
12.2.1 Adapter Pack [OSB]	p22698114_122100_Gen eric.zip	UI SDK JARs for the cloud adapter pack.
12.2.1 Insight Agent	p23589303_122100_Gen eric.zip	[BASE] Insight fix for OSB HOT bug 23558099.
12.2.1 Insight Agent	p22655174_122100_Gen eric.zip	Insight agent patch
12.2.1 Insight Agent	p23327887_122100_Gen eric.zip	Insight agent patch

Table A-347 SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Adapter Pack	p23115406_1213016041 9_Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bug 21473608
12.1.3 Bug 22568499	p20780464_121301_Gen eric.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP

Table A-347 (Cont.) SOA and Service Bus Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Gener eric.zip	Bundle patch 12.1.3.0.160419
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Gener eric.zip	[OSB] Bundle patch 12.1.3.0.1

Table A-348 API Manager Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 API Manager Core Template	p20225320_121300_Gener ic.zip	API Manager for OSB 12.1.3.0.0.
12.1.3 Adapter Pack	p23115406_12130160419_ Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bug 21473608.
12.1.3 Bug 22568499	p20780464_121301_Gener ic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP.
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Gener ic.zip	Bundle patch 12.1.3.0.160419.
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Gener ic.zip	[OSB] Bundle patch 12.1.3.0.1.
12.1.3 DB Schema	p20311552_121300_Gener ic.zip	API manager DB schema changes in 12.1.3.

Table A-349 SOA and B2B Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 DB Adapter Patch	p22978098_122100_Gener ic.zip	Fixes bug 22978098 - Indicators configured on response payload coming from a DB Adapter do not work.
12.2.1 Adapter Pack [SOA]	p22682253_122100_Gener ic.zip	Enable cloud adapters.
12.2.1 Adapter Pack [OSB]	p22698114_122100_Gener ic.zip	UI SDK JARs for the cloud adapter pack.
12.2.1 Insight Agent	p23589303_122100_Gene ric.zip	[BASE] Insight fix for OSB HOT bug 23558099.
12.2.1 Insight Agent	p22655174_122100_Gener ic.zip	Insight agent patch

Table A-350 SOA and B2B Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Adapter Pack	p23115406_12130160419_Generic.zip	Merge request on top of SOA BP 12.1.3.0.160419 for bug 21473608.
12.1.3 Bug 22568499	p20780464_121301_Generic.zip	Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP.
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Generic.zip	Bundle patch 12.1.3.0.160419.
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Generic.zip	[OSB] Bundle patch 12.1.3.0.1.

Table A-351 MFT Cluster Service Type — 12.1.3

Name	Bundle Name	Description
12.1.3 Bundle Patch 6 [SOA]	p22970958_121300_Generic.zip	Bundle patch 12.1.3.0.160419.
12.1.3 Bundle Patch 6 [OSB]	p22364187_121300_Generic.zip	[OSB] Bundle patch 12.1.3.0.1.

Table A-352 Integration Analytics Cluster Service Type — 12.2.1

Name	Bundle Name	Description
12.2.1 Insight Agent	p23589303_122100_Generic.zip	[BASE] Insight fix for OSB HOT bug 23558099.
12.2.1 Insight Agent	p22655174_122100_Generic.zip	Insight agent patch
12.2.1 BAM Server	p18668213_122100_Generic.zip	Insight server patch.

Patches Applied During Provisioning — 16.1.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 16.1.5.

Patch Name	Bundle Name (all paths preceded by the following path: distribution/binaries/soacs/)
Installs API Manager	p20225320_121300_Generic.zip
SOA Bundled Patch 12.1.3.0.3 (BP3)	p20900599_121300_Generic.zip
Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP3 (1 of 2)	p21473608_121303_Generic.zip
Cloud Adapter Pack SOA+OSB for 12.1.3.0.0 SOA BP1 (2 of 2)	p20780464_121300_Generic.zip

Patch Name	Bundle Name (all paths preceded by the following path: distribution/binaries/soacs/)
API manager DB schema changes in 12.1.3 (related to API Manager installation)	p20311552_121300_Generic.zip

Patches Applied During Provisioning — 15.4.5

The following patches are applied to instances when they are provisioned using Oracle SOA Cloud Service 15.4.5.

Patch Name	Bundle Name (all paths preceded by the following path: distribution/binaries/soacs/)
Cloud Adapter Pack for SOA BP1	p20780464_121300_Generic.zip
OSB Install Jar (1213)	osb_generic.jar
Cloud Adapter Patch	p21496295_121301_Generic.zip
B2B Install Jar	b2bhealthcare_generic.jar
SOA Bundle Patch 12.1.3.0.1	p19707784_121300_Generic.zip
DBClient Jar for MFT/B2B	dbclient121020.zip
API Manager Patch 12.1.3 (DB Schema)	p20311552_121300_Generic.zip
MFT Install Jar (1213)	mft_generic.jar
SOA Install Jar (1213)	soa_generic.jar
Provisioning Zip	provSoaCS-src.zip
API Manager Patch 12.1.3 for OSB	p20225320_121300_Generic.zip