



Deploying Avaya Analytics™ for Oceana®

Release 3.6.1
Issue 1
July 2019

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the

software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN

WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are

not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	8
Purpose	8
Intended audience	8
Oracle Restricted Use License	8
Changes in this release	9
Support for the Agent Login Logout report	9
Support for Red Hat Enterprise Linux 7.6	9
Chapter 2: Overview	10
Overview	10
Supported installation configurations	11
Deployment architecture	12
Chapter 3: Deployment process	15
Deployment process	15
Chapter 4: Planning and preconfiguration	18
Avaya Analytics™ hardware requirements	18
Disk partitioning requirements	20
Oracle patching considerations	21
Red Hat Enterprise Linux RPM packages	21
VMware configuration	25
Planning tasks	25
Chapter 5: Deploying	26
Reliable Eventing group configuration	26
Creating a Reliable Eventing group	26
Viewing the status of Reliable Eventing destinations	28
Running a maintenance test for a broker	28
Installing Oracle components	29
Prerequisites	29
Installing standalone Oracle® Database	30
Installing Primary Oracle® Database	32
Installing Standby Oracle® Database	35
Installing Oracle® RAC Database	39
Installing Oracle® Business Intelligence	52
Installing Oracle® Data Integrator	54
Installing Streams server software	57
Installing Oracle® Stream Analytics	59
Installing Oracle patches	61
Deploying Avaya Analytics™ for Oracle® Database	62
Pre-installation checks for Oracle® Database	62
Installing Avaya Analytics™ for Oracle® Database	63

Deploying Avaya Analytics™ for Oracle® Business Intelligence and Oracle® Data Integrator.....	65
Pre-installation checks for Oracle® Business Intelligence and Oracle® Data Integrator.....	65
Installing Avaya Analytics™ for Oracle® Business Intelligence and Oracle® Data Integrator...	67
Post installation steps for Oracle® Business Intelligence and Data Integrator.....	68
Post installation checks for Oracle® Business Intelligence and Oracle® Data Integrator.....	74
Configuring SSL for OBIEE weblogic server.....	76
Deploying the Avaya Analytics™ Streams server.....	81
Pre-installation checks for Avaya Analytics™ Streams server.....	81
Installing Avaya Analytics™ Streams server.....	82
Post installation checks for Avaya Analytics™ Streams server.....	83
Disabling http on port 7001.....	85
Configuring Avaya Analytics™ Streams server certificates.....	85
Post installation steps for Avaya Analytics™ Streams server.....	94
Configuring SSL for Stream server weblogic.....	97
Deploying Avaya Analytics™ for Oracle® Stream Analytics.....	102
Pre-installation checks for Oracle® Stream Analytics.....	102
Installing Avaya Analytics™ for Oracle® Stream Analytics.....	109
Post installation checks for Oracle® Stream Analytics.....	110
Post installation steps for Oracle® Stream Analytics.....	111
Starting OSA components after a restart.....	112
Disaster Recovery.....	113
Switching over the dataguard database.....	114
Configuring the SNMP environment.....	115
Configuring the Server properties file.....	115
Enabling the Routing Service Groups feature.....	116
Chapter 6: Upgrading.....	118
Upgrading Avaya Analytics™	118
Uninstalling the Oceana Input Adapter application from OSA.....	119
Stopping the OSA process.....	120
Uninstalling the Agent by Auxcode applications from OSA.....	120
Removing OSART from the existing Oracle® Stream Analytics server.....	121
OBI server upgrade.....	121
Pre-upgrade steps for OBI.....	121
Upgrading the OBI server.....	122
Post-upgrade steps for OBI.....	123
Oracle® Database Data Guard upgrade.....	125
Upgrading a standalone Oracle® Database to a Primary server installation.....	125
Database backup and restore.....	126
Prerequisites	127
Backing up Avaya Analytics™ database schemas.....	127
Restoring Avaya Analytics™ database schemas.....	128
Backup and Restore of Oracle® Business Intelligence reports.....	129
Creating a new folder in OBIEE.....	129

- Editing a dashboard for custom artifacts..... 130
- Taking a backup of custom artifacts..... 130
- Restoring custom artifacts..... 131
- Chapter 7: Documentation..... 132**
 - Finding documents on the Avaya Support website..... 133
 - Avaya Documentation Portal navigation..... 133
- Chapter 8: Training..... 135**
- Chapter 9: Support..... 137**
 - Using the Avaya InSite Knowledge Base..... 137

Chapter 1: Introduction

Purpose

This document provides information about how to prepare, install, and configure Avaya Analytics™.

Intended audience

This document is intended for anyone who wants to deploy and use Avaya Analytics™. This document assumes that the user has expert knowledge of Linux operating systems, and of the Oracle® components used in an Avaya Analytics™ solution. Avaya recommends that all Avaya Analytics™ solutions have a trained Oracle® database administrator (DBA).

Oracle Restricted Use License

Avaya Analytics™ uses certain embedded Oracle programs. The Oracle programs included in Avaya Analytics™ are subject to a restricted use license and can be used solely in conjunction with Avaya Analytics™.

In Customer environments with administrative practices for functions such as: backup, security, authentication and similar operational aspects, the Customer's administrator may access an Oracle database embedded in Avaya Analytics™ for the sole purpose of configuring the embedded database for use solely with Avaya Analytics™. Customer (or its administrator) may not add or make changes to the Oracle database schemas, metadata or data models other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables.

With regards to visual tools, including but not limited to Data Visualization and Stream Analytics, Customer will be permitted to access and administer the tools solely within the scope of Avaya Analytics™. The foregoing is meant to allow Customer access to metadata for visual tools; however, in the case of Avaya Analytics™ that distributes Oracle Database Enterprise Edition, Customer may not access or change the database schema other than through and/or as an extension of the functionality of Avaya Analytics™, including but not limited to: incorporating implementation reference data, dimensional and fact tables solely related to Avaya Analytics™.

Customer is fully responsible and liable to Avaya, its affiliates, and Oracle for any damages or losses caused by any unauthorized use of any of the Oracle programs embedded in Avaya Analytics™.

Changes in this release

Avaya Analytics™ Release 3.6.1 includes the following changes:

Support for the Agent Login Logout report

Avaya Analytics™ provides the Agent Login Logout report. With this report, you can view the login and logout information of agents, such as the login and logout time, total login duration, and the attributes associated with agents when they log in to the reporting interval.

Support for Red Hat Enterprise Linux 7.6

The current release of Avaya Analytics™ supports new deployments on Red Hat Enterprise Linux (RHEL) 7.6.

Chapter 2: Overview

Overview

The Avaya Analytics™ framework:

- Provides reporting for end-to-end customer journey on multichannel sources. Using reports, supervisors can analyze current trends in the contact center and enhance the performance of agents.
- Provides enterprises the ability to receive events from a collection of event sources and process those events to derive and present business measures.
- Leverages an Oracle stack to deliver the ingestion, event processing, publishing, and historical presentation layers to customers.

Key features

The following table lists the key features of Avaya Analytics™:

Feature	Description
Historical reporting	Provides multichannel reporting data on contact center performance to track trends and improve the overall performance.
Supervisor historical reporting	Provides supervisor reporting using the Avaya Analytics™ platform in Avaya Oceana® Solution Supervisor user interface (UI). With this reporting, contact center supervisors can manage resources.
Custom reports	Enables users to create their own custom reports. Custom reports are customizable and access controlled.
Rich visualization features	Provides rich visualization features on reports and dashboards using a Business Intelligence Presentation layer.

* Note:

The Avaya Analytics™ Streams server provides producers and measures to Avaya Workspaces for use in real-time reporting dashboards.

- For information about how to configure communication between the Avaya Analytics™ Streams server and Avaya Workspaces, see *Administering Avaya Workspaces for Oceana®*.
- For information about how to view real-time reporting dashboards, see *Using Avaya Workspaces for Oceana®*.

Supported installation configurations

All Avaya Analytics™ solutions must include the following components:

- Oracle® Database
- Oracle® Business Intelligence (OBI)
- Oracle® Data Integrator (ODI)
- Avaya Analytics™ Streams Server
- Oracle® Stream Analytics (OSA)

Important:

- In all supported installation configurations, Oracle® Data Integrator must be installed on the same server as Oracle® Business Intelligence. If you are upgrading from a previous version of Avaya Analytics™, you must ensure that you install Oracle® Data Integrator on the same server as Oracle® Business Intelligence.
- If you are upgrading from a previous version of Avaya Analytics™, you must install the Avaya Analytics™ Streams Server on a server with a newly installed operating system. For example, if you want to install the Avaya Analytics™ Streams Server on the old Oracle® Business Activity Monitor (BAM) server, you must install a new operating system first.

Avaya Analytics™ supports deploying Oracle® Database using one of the following methods:

- Single Instance (SI): One instance of Oracle® Database runs on one virtual server.
- Real Application Cluster (RAC): Allows you to run more than one instance of Oracle® Database on multiple servers. Oracle® RAC Database is a clustered version of Oracle® Database, and this configuration supports load balancing and High Availability (HA).
- Oracle Data Guard: One instance of Oracle® Database runs on two virtual servers, a Primary server and a Standby server. You can use the Oracle Data Guard feature for disaster recovery. This allows you to recover after a complete outage occurs at your primary data center. For more information about disaster recovery, see [Disaster Recovery](#) on page 113.

In a High Availability solution, deploying Oracle® Database in a HA configuration is optional. Avaya Analytics™ supports deploying Single Instance Oracle® Database while deploying Avaya Oceana® Solution and other Avaya Analytics™ components in a HA configuration. If you deploy Oracle® Stream Analytics High Availability (HA), your solution must include 2 virtual OSA servers.

Important:

If you deploy Oracle® RAC Database in your Avaya Analytics™ solution, Oracle Data Guard is not supported.

You can deploy Avaya Oceana® Solution and Avaya Analytics™ in an Amazon Web Services (AWS) environment. For more information about AWS deployments, see *Deploying Avaya Oceana® Solution on Amazon Web Services*.

Deployment architecture

The following diagram depicts the architecture for the deployment of a typical Avaya Analytics™ solution.

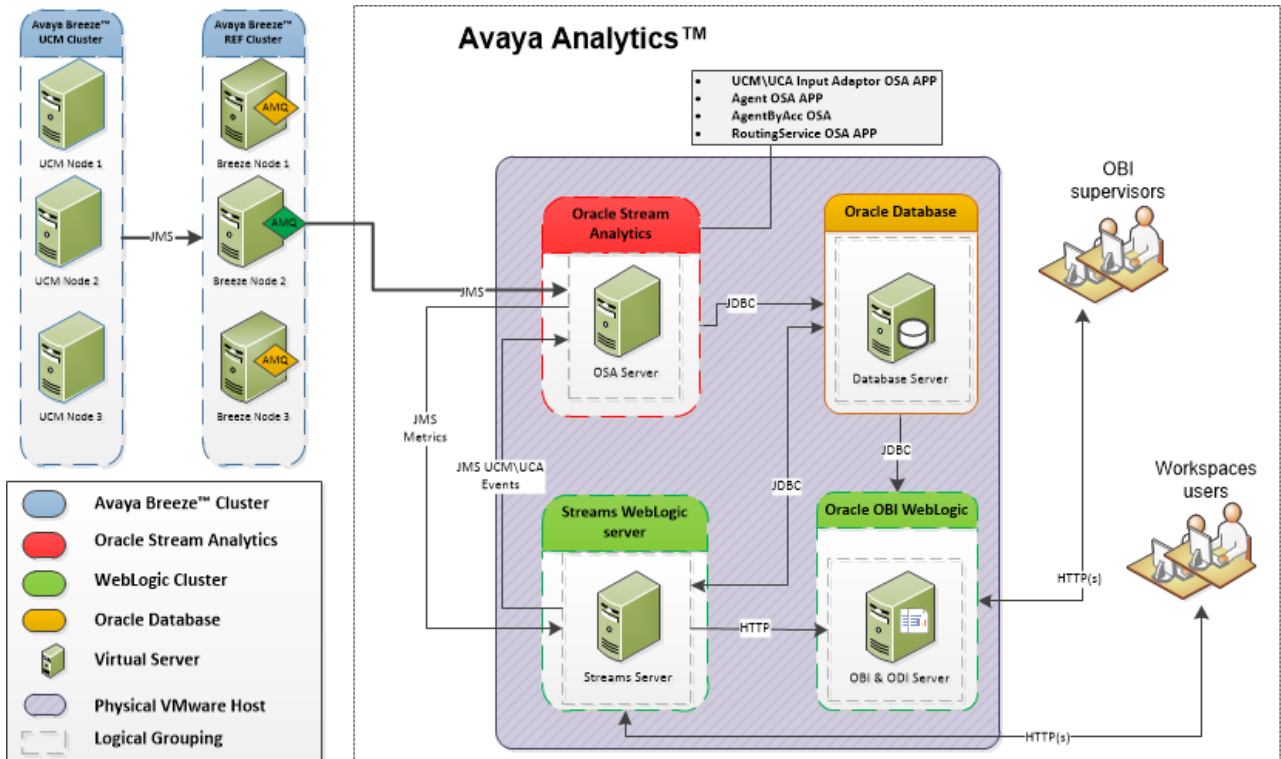


Figure 1: Avaya Analytics™ solution with single instance database

The following diagram depicts the architecture for the deployment of a typical Avaya Analytics™ solution when you install Oracle® RAC Database. Avaya Analytics™ supports 2 Oracle® RAC Database instances, each running on separate host servers to ensure that there is no single point of failure for your database.

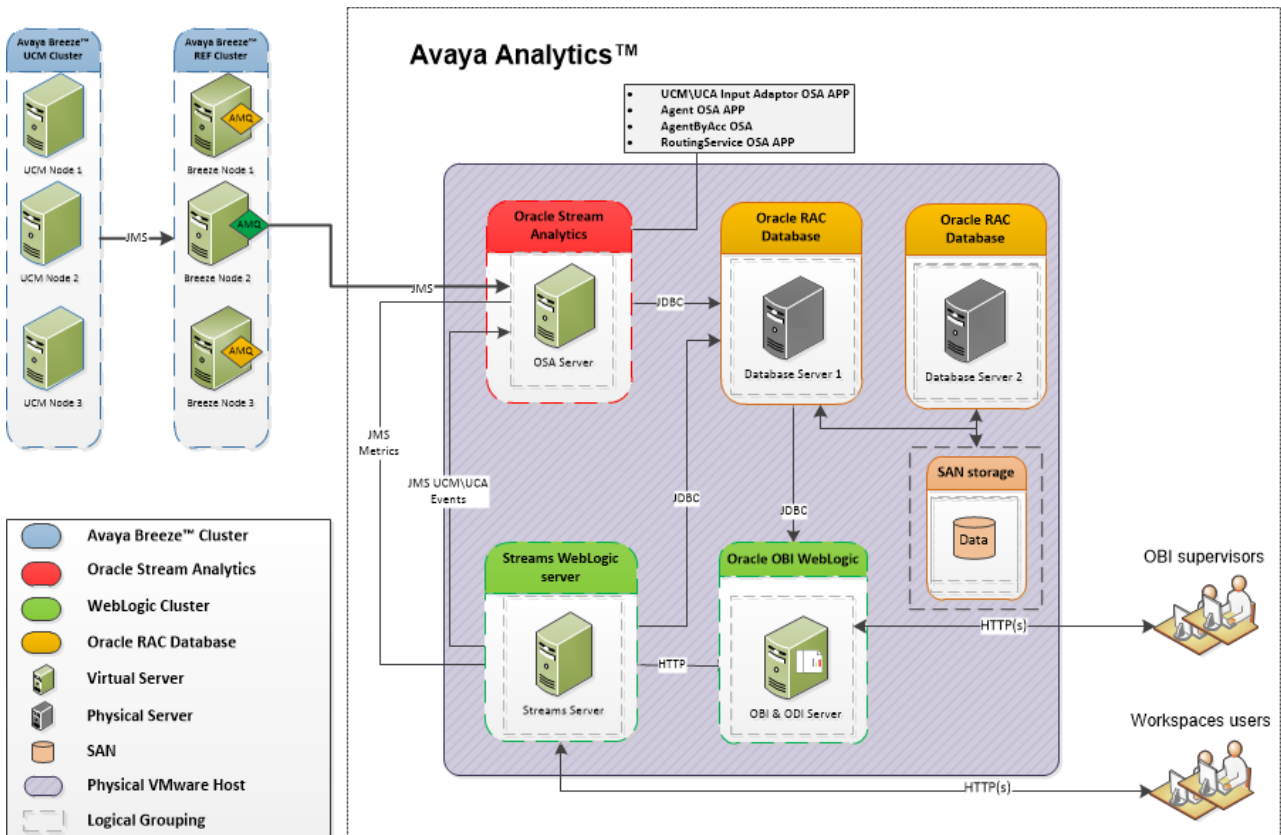


Figure 2: Avaya Analytics™ solution with RAC database

The following diagram depicts the architecture for the deployment of a typical Avaya Analytics™ solution when you configure Oracle Data Guard. Avaya Analytics™ supports Primary and Standby Oracle® Database instances, each running on separate host servers to ensure that there is no single point of failure for your database.

! Important:

You must also have a complete secondary solution deployed at the DR site. This includes installing both Avaya Oceana® Solution and Avaya Analytics™ at the DR site.

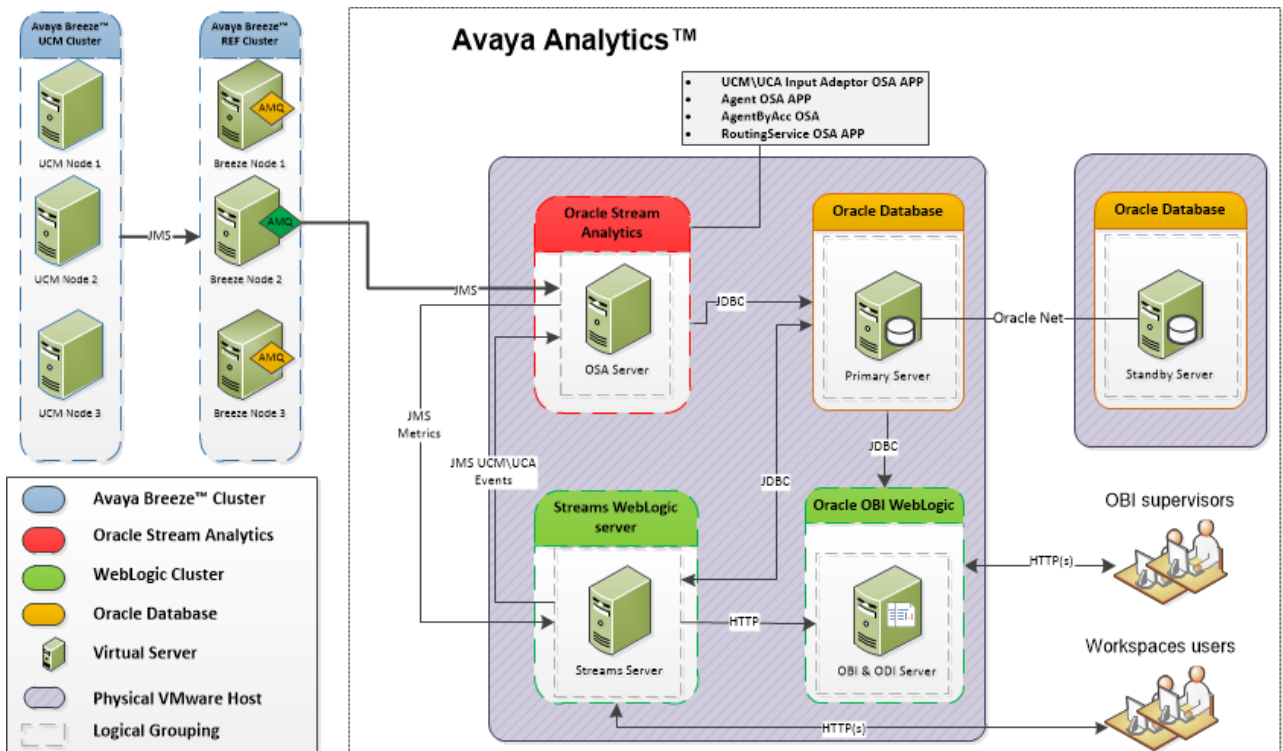


Figure 3: Avaya Analytics™ solution with Oracle Data Guard

Chapter 3: Deployment process

Deployment process

This work flow shows the sequence of tasks that you must perform, in sequential order, to deploy Avaya Analytics™.

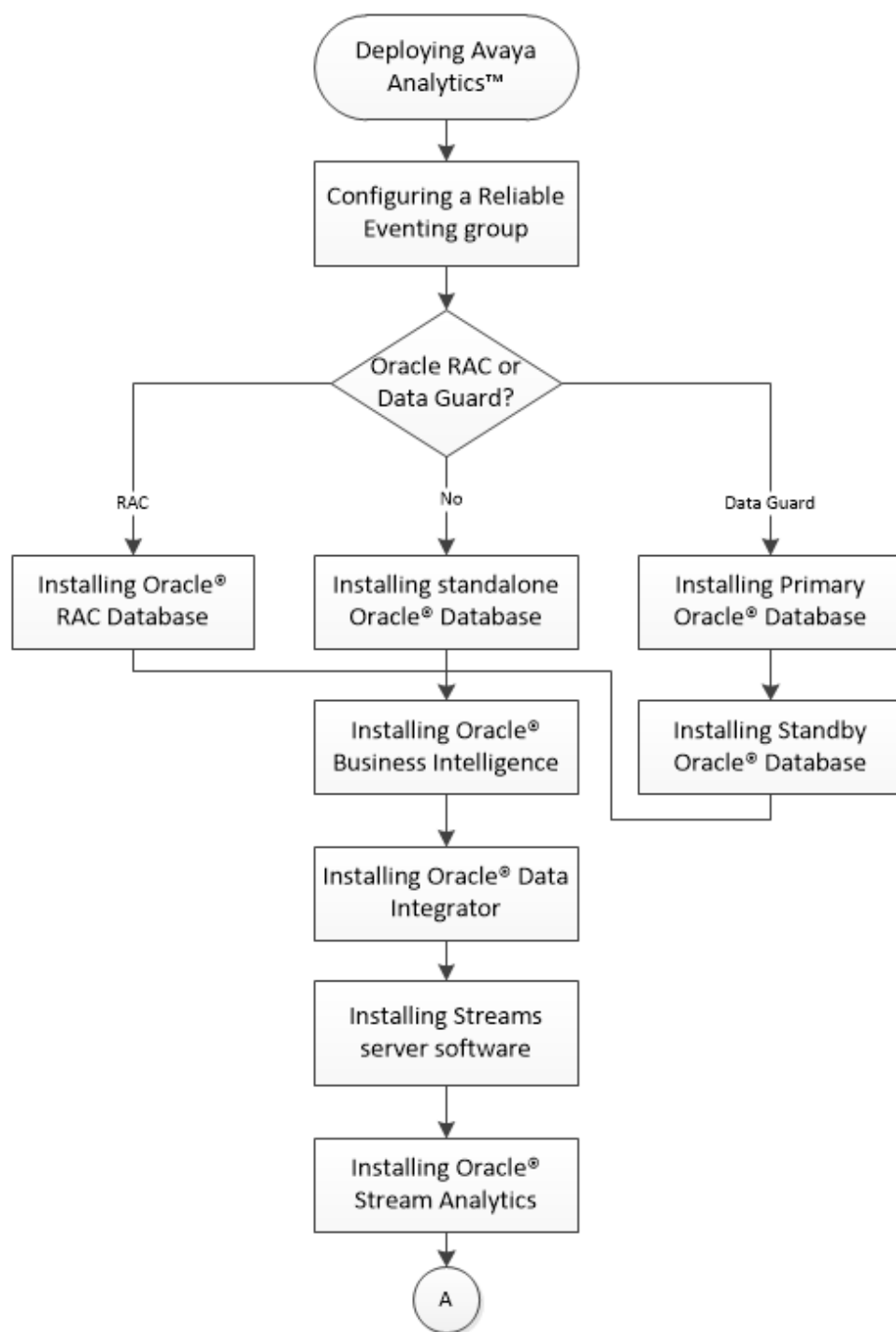


Figure 4: Avaya Analytics™ deployment

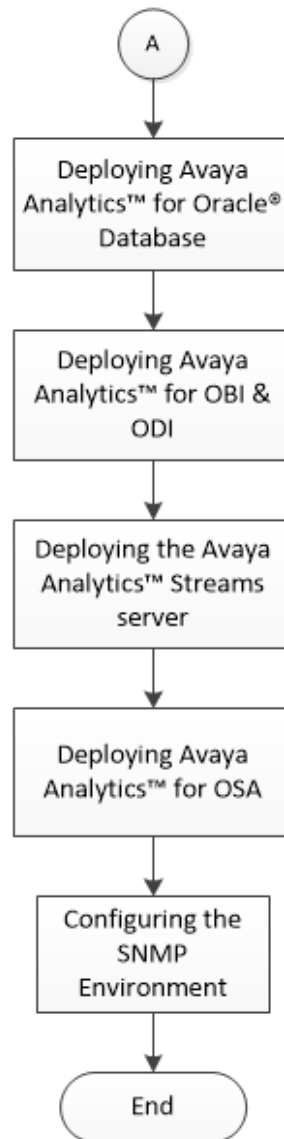


Figure 5: Avaya Analytics™ deployment continued

Chapter 4: Planning and preconfiguration

Avaya Analytics™ hardware requirements

The following table provides information about the memory, disk, and vCPU requirements for each component of Avaya Analytics™. Install each of these components on a separate VMware virtual guest.

Component	Platform	Requirement	Avaya Oceana® Solution					
			4500 Agents	2000 Agents	1000 Agents	500 Agents	250 Agents	100 Agents
Oracle® Stream Analytics	- VMware ESXi - Red Hat Enterprise Linux - Oracle software	Number of virtual servers	1 ^{Note 1}	1 ^{Note 1}	1 ^{Note 1}	1 ^{Note 1}	1 ^{Note 1}	1 ^{Note 1}
		Memory/server	96 GB	72 GB	56 GB	36 GB	26 GB	18 GB
		Minimum disk size/server	500 GB	500 GB	300 GB	300 GB	300 GB	300 GB
		vCPU's/server	16	16	8	8	8	6
		IOPS/server	300	200	100	100	50	50
Avaya Analytics™ Streams server	- VMware ESXi - Red Hat Enterprise Linux - Oracle software	Number of virtual servers	1	1	1	1	1	1
		Memory/server	30	30	16	16	16	10
		Minimum disk size/server	500	500	400	400	400	400
		vCPU's/server	8	8	8	8	6	4
		IOPS/server	300	200	100	100	50	50
Oracle® Business Intelligence and Oracle® Data Integrator	- VMware ESXi - Red Hat Enterprise Linux - Oracle software	Number of virtual servers	1	1	1	1	1	1
		Memory/server	48 GB	32 GB	24 GB	16 GB	16 GB	10 GB
		Minimum disk size/server	500 GB	500 GB	300 GB	300 GB	300 GB	300 GB
		vCPU's/server	8	8	8	8	4	3
		IOPS/server	300	200	100	100	50	50

Table continues...

Component	Platform	Requirement	Avaya Oceana® Solution					
			4500 Agents	2000 Agents	1000 Agents	500 Agents	250 Agents	100 Agents
Oracle® Database - no RAC	• VMware ESXi • Red Hat Enterprise Linux • Oracle software	Number of virtual servers	1	1	1	1	1	1
		Memory/server	48 GB	32 GB	24 GB	16 GB	16 GB	12 GB
		Minimum disk size/server	1500 GB	1500 GB	1000 GB	500 GB	500 GB	500 GB
		vCPU's/server	8	8	8	8	4	3
		IOPS/server	300	300	200	200	100	100
Oracle® RAC Database	• VMware ESXi • Red Hat Enterprise Linux • Oracle software	Number of virtual servers	2	2	2	2	2	2
		Memory/server	48 GB	32 GB	24 GB	16 GB	16 GB	12 GB
		Minimum disk size/server	500 GB	500 GB	500 GB	500 GB	500 GB	500 GB
		vCPU's/server	8	8	8	8	4	3
		IOPS/server	200	150	100	100	50	50
Oracle® Database - SAN-based shared storage Note 2	• VMware ESXi • Red Hat Enterprise Linux • Oracle software • SAN storage required	Minimum disk size/server	1500 GB	1500 GB	1000 GB	500 GB	500 GB	500 GB
		IOPS/server	300	300	200	200	100	100
Note 1 If you deploy Oracle® Stream Analytics High Availability (HA), your solution must include 2 virtual OSA servers.								
Note 2 When you deploy Oracle® RAC Database, you must use SAN storage. Identify the SAN storage requirements for your solution, and configure storage based on those requirements.								
Note 3 The minimum CPU speed based on Intel® Xeon® E5-2697 processor is 2.60 GHz.								

 Note:

- The current release of Avaya Analytics™ supports VMware ESXi 6.0, 6.5, and 6.7.
- The current release of Avaya Analytics™ supports new deployments on Red Hat Enterprise Linux 7.4, 7.5, or 7.6.

Disk partitioning requirements

This section describes the hard disk drive partitioning requirements for Red Hat Enterprise Linux (RHEL) Release 7.4, 7.5, or 7.6 servers in an Avaya Analytics™ solution. The current release of Avaya Analytics™ supports new deployments on RHEL 7.4, 7.5, or 7.6 only.

Each RHEL server in an Avaya Analytics™ solution requires swap space. Linux servers use swap space when the amount of physical memory (RAM) is full. The swap space requirement for Oracle® Database and Streams servers is higher than the other servers in the solution.

The temporary directory for each RHEL server in an Avaya Analytics™ solution requires 10 GB of space. During the installation, files are extracted to the temporary directory. The directory must have sufficient space for the Java Runtime Environment (JRE) included in the installation, and for an uncompressed copy of the JRE that is expanded into the temporary directory. The files are deleted from the temporary directory after the installation completes.

The installation wrappers for Oracle software use the /home directory as the default location. As a result, you must assign most of the disk space to this location.

The following table outlines the minimum hard disk drive partitioning requirements for each server in an Avaya Analytics™ solution:

Table 1: Minimum disk partitioning requirements for Oracle® Database and Streams servers

Partition	Space
/	25 GB
/boot	1 GB
/home	Remaining Disk Space
/tmp	10 GB
swap	16 GB

Table 2: Minimum disk partitioning requirements for Oracle® Business Intelligence (OBI) and Oracle® Stream Analytics (OSA) servers

Partition	Space
/	25 GB
/boot	1 GB
/home	Remaining Disk Space
/tmp	10 GB
swap	2 GB

Oracle patching considerations

You must install all required patches when installing Oracle components. The Avaya Analytics™ install scripts automatically install the patches at the end of the Avaya Analytics™ software installation. However, you must ensure that the patches are available on each server. Download patches for the following Oracle components, available from the Avaya Support website at <http://support.avaya.com/>.

- Oracle® Database
- Oracle® Business Intelligence (OBI)
- Oracle® Data Integrator (ODI)
- Avaya Analytics™ Streams server (WebLogic Server)
- Oracle® Stream Analytics (OSA)

You must refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Red Hat Enterprise Linux RPM packages

You must ensure that required Red Hat Package Manager (RPM) packages are installed before you install Oracle software. If the required RPM packages listed in the below table are not installed, the install fails. You must also install all of the dependencies required for the RPM packages listed.

Oracle component	Required RPM packages
Oracle® Database	binutils chrony compat-libcap1 compat-libstdc++-33 gcc gcc-c++ glibc glibc-devel ksh libgcc libstdc++ libstdc++-devel libaio libaio-devel libXext libX11 libxcb libXi libXtst make net-snmp perl psmisc sysstat unzip rng-tools

Table continues...

Oracle component	Required RPM packages
Oracle® RAC Database	binutils compat-libcap1 compat-libstdc++-33 compat-libstdc++-33.i686 gcc gcc-c++ glibc glibc.i686 glibc-devel glibc-devel.i686 ksh libgcc libgcc.i686 libstdc++ libstdc++.i686 libstdc++-devel libstdc++-devel.i686 libaio libaio.i686 libaio-devel libaio-devel.i686 libXext libXext.i686 libXtst libXtst.i686 libX11 libX11.i686 libXau libXau.i686 libxcb libxcb.i686 libXi libXi.i686 make net-snmp sysstat unixODBC unixODBC-devel rng-tools
Oracle® Business Intelligence	binutils chrony compat-libcap1 compat-libstdc++-33 gcc gcc-c++ glibc glibc-devel ksh libgcc libstdc++ libstdc++-devel libaio libaio-devel make net-snmp sysstat unzip numactl numactl-devel rng-tools

Table continues...

Oracle component	Required RPM packages
Oracle® Data Integrator	chrony libXtst net-snmp unzip
Avaya Analytics™ Streams server	binutils chrony compat-libcap1 compat-libstdc++-33 gcc gcc-c++ glibc glibc-devel ksh libgcc libstdc++ libstdc++-devel libaio libaio-devel make net-snmp sysstat unzip numactl numactl-devel rng-tools net-tools psmisc
Oracle® Stream Analytics	binutils chrony compat-libcap1 compat-libstdc++-33 gcc gcc-c++ glibc glibc-devel ksh libgcc libstdc++ libstdc++-devel libaio libaio-devel make net-snmp sysstat unzip numactl numactl-devel rng-tools

VMware configuration

VMware feature	Supported on active Avaya Analytics™ servers	Supported on Avaya Analytics™ servers during maintenance window
Cloning	No	Yes
Distributed Power management (DPM)	No	No
Distributed Resource Scheduler (DRS)	No	No
Distributed Switch	No	No
Fault Tolerance	No	No
High Availability (HA)	No	No
Snapshot	No	Yes
Storage DRS	No	No
Storage Thin Provisioning	No	No
Storage vMotion	No	Yes
Suspend & Resume	No	NA
vMotion	No	Yes

Planning tasks

- Read *Avaya Oceana® Solution Description*.
- Perform all of the tasks described in *Deploying Avaya Oceana® Solution*.
- Ensure that the time on all servers in the Avaya Oceana® Solution is synchronized. Avaya Analytics™ uses chrony daemon to synchronize the time on Avaya Analytics™ servers.

Chapter 5: Deploying

Reliable Eventing group configuration

Reliable Eventing Framework provides a mechanism for delivering messages. The Reliable Eventing Framework adopts Apache ActiveMQ that provides a rich set of capabilities such as reliability, asynchronous events, inter-node, and inter-cluster.

Reliable Eventing Framework provides the following features:

- Enables delivery of events across servers and clusters.
- Guarantees event delivery with event persistence, acknowledgement, and durable subscriptions.
- Master/Slave high availability with replicated persistent messages.

Configure Reliable Eventing groups using Avaya Breeze® platform.

Creating a Reliable Eventing group

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Reliable Eventing Administration > Dashboard**.
2. On the Reliable Eventing Groups page, click **New**.
3. On the Reliable Eventing Group Editor page, enter the following details:
 - **Cluster**: Select Avaya Oceana® Cluster 1.
 - **Group Name**: Assign a name to the Reliable Eventing group.
 - **Description**: Enter a brief description.
 - **Type**: Select **HA** or **Standalone**.
 - If you select **HA**, you must select at least three Avaya Breeze® platform nodes or brokers. For example, the three Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.
 - If you select **Standalone**, you must select at least one Avaya Breeze® platform node or broker.
4. In the **Unassigned Brokers** table, click **+** to assign the Avaya Breeze® platform nodes or brokers to the Reliable Eventing group.

5. Click the Associated clusters tab:

- In the **Unassigned associated clusters** table, click the **+** icon to add an associated cluster.
- In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.

6. Click **Commit**.

The **Status** column shows one of the following:

- Green check mark (✓) : Indicates that the status of the broker is up and running for subscription and event transfers.
- Red cross mark (✗): Indicates that the status of the broker is down.

7. To view the status of the brokers, click the green check mark.

- Administration
- Cluster
- Administration
- Service Management
- Reliable Eventing
- Administration
- Dashboard**
- Destination Status
- Configuration
- System Tools and Monitoring

Broker Status

aocdc2c1n1

ActiveMQ

Attribute Name	Value
Status	Attached
NodeRole	slave
Slave	true
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

Details

aocdc2c1n2

ActiveMQ

Attribute Name	Value
Status	Attached
NodeRole	slave
Slave	true
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

Details

aocdc2c1n3

ActiveMQ

Attribute Name	Value
Status	2 slave nodes attached.
NodeRole	master
Slave	false
Uptime	2 hours 11 minutes
Persistent	true

Details

Zookeeper

Details

Viewing the status of Reliable Eventing destinations

Procedure

1. On System Manager, click **Elements > Avaya Breeze® > Reliable Eventing Administration > Destination Status**.

The system displays Broker Destination Status Page.

2. In the **Group** field, select the **Reliable Eventing group**.

The system displays the destination status.

Broker Destination Status Page

This page allows you to see destinations status.

Group: **ReffB** ▼

Reliable Eventing Destinations

Delete/Purge

32 Items Filter: Enable

☐	Destination Name	Type	Enqueued Messages	Dequeued Messages	Dispatched Messages	Pending Messages	InFlight Messages	Expired Messages	Consumers Count
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.USER	QUEUE	1111	1111	1111	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.FORWARD_NOTIFICATION	QUEUE	444	444	444	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.DISPOSITION_CODE	QUEUE	555	555	555	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.EXTERNAL_CONVERSATION_INTERACTION	QUEUE	666	666	666	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.CONVERSATION_INTERACTION	QUEUE	444	444	444	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.WORK_REQUEST	QUEUE	555	555	555	0	0	0	1
☐	VTConsumerAnalytics.IA_IP.VirtualTopic.OCEANA_LIVE.CONTACT	QUEUE	666	666	666	0	0	0	1

Select : All, None Page 2 of 2

Running a maintenance test for a broker

Procedure

1. On System Manager, click **Elements > Avaya Breeze® > System Tools and Monitoring > Maintenance Tests**.
2. In the **Select Avaya Breeze to test** field, click the Avaya Breeze® platform instance that you want to test.
3. Select the **Test Reliable Eventing Framework** check box.
4. Click **Execute Selected Tests**.

Avaya Breeze® platform displays one of the following statuses:

- **Failure** when Reliable Eventing is down. That is, publishing and receiving messages by Reliable Eventing is failing.
- **Success** when Reliable Eventing is functional. That is, publishing and receiving messages by Reliable Eventing is working.

Installing Oracle components

This section describes how to install each of the Oracle components required for Avaya Analytics™.

Prerequisites

- Configure a yum repository on the RHEL server where you are installing the Oracle software.

The installation fails if you do not configure a repository. For more information on the required RPM packages, see [Red Hat Enterprise Linux RPM packages](#) on page 21.

- Install Oracle JDK 1.8 on the server.

You must also ensure that Oracle JDK 1.8 is selected as the active Java version. Run the following command as the root user:

```
/usr/sbin/alternatives --config java
```

The active Java version is highlighted with an asterisk. Ensure that Oracle JDK 1.8 is selected as the Java version by typing the corresponding number and pressing Enter. For example:

```
[root@aocdc1odb2 ~]# /usr/sbin/alternatives --config java
There are 2 programs which provide 'java'.

  Selection    Command
-----
*   1          java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.144-0.b01.el7_4.x86_64/jre/bin/java)
+   2          /usr/java/jdk1.8.0_144/jre/bin/java

Enter to keep the current selection[+], or type selection number: [ ]
```

- Confirm Linux server entropy availability. Oracle software requires the entropy available on the virtual machine to be high. Perform the following steps to confirm entropy availability on each RHEL server in your Avaya Analytics™ solution:

1. Run the following command to check entropy availability:

```
cat /proc/sys/kernel/random/entropy_avail
```

2. If the entropy value is less than 1000, run the following command as the root user:

```
rngd -r /dev/urandom -o /dev/random -b
```

3. Confirm the entropy value now exceeds 1000. You must also check the entropy value after a server reboot.

Important:

The **rngd** command requires **rng-tools** rpm. You can start **rngd** using the following command, run as the root user:

```
systemctl start rngd
```

Installing standalone Oracle® Database

About this task

Install Oracle® Database on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. Use this procedure to deploy a Single Instance of Oracle® Database as a standalone server installation.

The following table lists the requirements for Oracle® Database installation:

Requirement	Description
Java	jdk1.8.x.x.x
DB installation scripts	db.zip
Oracle® Database software	linuxamd64_12102_database_1of2.zip
	linuxamd64_12102_database_2of2.zip

Procedure

1. Unzip the AvayaAnalytics_x.x.x.x_Build_xx.zip file.

The db.zip file is available in the Oracle_Installers/Nodal folder.

2. Copy the db.zip file to the database server using an scp or ftp tool.
3. SSH to the database server as the root user.
4. Create the /var/tmp/Analytics/ directory.
5. Run the following command to unzip the db.zip file to the /var/tmp/Analytics directory:

```
unzip -d /var/tmp/Analytics db.zip
```

Example of the directory structure contents:

- /var/tmp/Analytics/parameters.conf

6. Copy the following files to the /var/tmp/Analytics/ directory:

- linuxamd64_12102_database_1of2.zip
- linuxamd64_12102_database_2of2.zip

7. Make the following changes to the /var/tmp/Analytics/parameters.conf file based on the information relevant to your server:

```
#### SYSTEM common settings ####
DOMAIN=domain.com           #CHANGE THIS TO THE DOMAIN NAME ONLY I.E
DOMAIN.COM
NTP_HOST=127.0.0.1          #CHANGE THIS TO THE NTP IP OR HOSTNAME IF NTP
NOT_ALREADY_CONFIGURED
JAVA_HOME=/usr/java/latest  #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION

#### Oracle DB Parameters ####
DB_HOSTNAME=localhost       #CHANGE THIS TO THE HOSTNAME
ONLY (NOT THE FQDN)
DB_HOST_IP_ADDR=127.0.0.1   #CHANGE THIS TO THE IP OF
```

```

YOUR SERVER
DB_LSNR_PORT=1521
#CHANGE THIS TO LISTENER PORT OF YOUR DATABASE
DB_NAME_SERVER=127.0.0.1                #CHANGE THIS TO THE IP/
HOSTNAME OF YOUR DNS SERVER

#### This variable is required to set the ORACLE_SID environment variable for
user .bash_profile
ORACLE_DB_SID=orcl                      #CHANGE THIS TO SID OF YOUR
DATABASE

#### This variable is required to set the DB_UNIQUE_NAME parameter for Primary,
it should be unique within the enterprise
ORACLE_DB_UNIQUE_NAME=orcl             #CHANGE THIS TO THE UNIQUE NAME OF
YOUR DATABASE

#### This variable is required to set the type of installation STANDALONE,
PRIMARY or STANDBY
#### STANDALONE - Installation standalone DB on server (no Data Guard, no RAC)
#### PRIMARY - Installation PRIMARY DB on server for Data Guard setup
#### STANDBY - Installation STANDBY DB on server for Data Guard setup
ORACLE_DB_INSTALLATION_TYPE=STANDALONE #YOU MUST ENSURE THIS IS SET TO
STANDALONE

#### This variable is only used when upgrading STANDALONE to PRIMARY Data Guard
(YES/NO)
ORACLE_DATAGUARD_UPGRADE=NO            #YOU MUST ENSURE THIS
IS SET TO NO

```

8. From the `/var/tmp/Analytics/db` directory, make the following script executable and run the following command as the root user.

```
sh root.sh
```

When prompted to enter the password for the Oracle user: "Enter password for oracle:", enter the password.

9. After the script completes, review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the script.
10. Reboot the database server.
11. After the server starts, SSH to the Oracle® Database server and switch to the root user.
12. From the `/var/tmp/Analytics/db` directory, run the following command as the root user to begin the installation process:

```
sh oracle_db_install.sh
```

You must confirm that you have edited the `parameters.conf` file, and you must enter the Oracle user password during the installation.

13. After successful installation, review the output of the script to ensure that no failures or errors occurred during the installation process.

Post installation checks for Oracle® Database

About this task

Perform the following post installation checks for Oracle® Database, if required. This procedure describes checks to perform after the install, and how to manually start or stop the database. After you install Oracle® Database, the database is running.

! Important:

Ensure that you use the Oracle user account.

Procedure

1. Run the following command to set the paths required to run **sqlplus**:

```
. ~/.bash_profile
```

* Note:

This command returns no output.

2. Run the following commands to manually start the database, if required:

- **sqlplus / as sysdba**
- **STARTUP**

The output must indicate that the database is mounted. You can exit the sqlplus shell by typing **quit**.

3. Run the following command to check whether the listener has started:

```
lsnrctl status
```

4. Run the following command to start the listener, if required:

```
lsnrctl start
```

Installing Primary Oracle® Database

About this task

Install Oracle® Database on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. Use this procedure to deploy a Single Instance of Oracle® Database as a Primary server installation in an Oracle Data Guard configuration.

Oracle Data Guard has three protection mode options: Max Availability, Max Performance or Max Protection. You can select your preferred mode using the `parameters.conf` file. Max Availability mode is set by default. The value for the Oracle Data Guard protection mode parameter must match on the Primary and Standby server. Choose your Oracle Data Guard protection mode option based on your solution requirements:

- **Max Availability:** Redo logs are transmitted from the Primary server and written and acknowledged by the Standby server before a commit is complete. In the event of a failure on the Primary server there is zero data loss when you switch over to the Standby server. If the

Standby server cannot be reached at any time, the system reverts to Max Performance behavior until connectivity is restored.

- **Max Performance:** Redo logs are transmitted from the Primary server to the Standby server but the commit is complete on the Primary server before the redo log is written to the disk on the Standby server. In the event of a failure on the Primary server, transactions can be lost when you switch over to the Standby server.
- **Max Protection:** Redo logs are transmitted from the Primary server and written and acknowledged by the Standby server before a commit is complete. In the event of a failure on the Primary server there is zero data loss when you switch over to the Standby server. If the Standby server cannot be reached, the Primary server stops processing transactions until the Standby server is functional once again.

For more detailed information about Oracle Data Guard protection modes, refer to Oracle documentation.

The following table lists the requirements for Oracle® Database installation:

Requirement	Description
Java	jdk1.8.x.x.x
DB installation scripts	db.zip
Oracle® Database software	linuxamd64_12102_database_1of2.zip linuxamd64_12102_database_2of2.zip

Procedure

1. Unzip the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.

The `db.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `db.zip` file to the database server using an scp or ftp tool.
3. SSH to the database server as the root user.
4. Create the `/var/tmp/Analytics/` directory.
5. Run the following command to unzip the `db.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics db.zip
```

Example of the directory structure contents:

- `/var/tmp/Analytics/parameters.conf`

6. Copy the following files to the `/var/tmp/Analytics/` directory:
 - `linuxamd64_12102_database_1of2.zip`
 - `linuxamd64_12102_database_2of2.zip`
7. Make the following changes to the `/var/tmp/Analytics/parameters.conf` file based on the information relevant to your server:

```
#### SYSTEM common settings ####
DOMAIN=domain.com                #CHANGE THIS TO THE DOMAIN NAME ONLY I.E
DOMAIN.COM
NTP_HOST=127.0.0.1               #CHANGE THIS TO THE NTP IP OR HOSTNAME IF NTP
```

```

NOT ALREADY CONFIGURED
JAVA_HOME=/usr/java/latest           #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION

#### Oracle DB Parameters ####
DB_HOSTNAME=localhost                 #CHANGE THIS TO THE HOSTNAME
ONLY (NOT THE FQDN)
DB_HOST_IP_ADDR=127.0.0.1             #CHANGE THIS TO THE IP OF
YOUR SERVER
DB_LISTENER_PORT=1521
#CHANGE THIS TO LISTENER PORT OF YOUR DATABASE
DB_NAME_SERVER=127.0.0.1              #CHANGE THIS TO THE IP/
HOSTNAME OF YOUR DNS SERVER

#### This variable is required to set the ORACLE_SID environment variable for
user .bash_profile
ORACLE_DB_SID=orcl                    #CHANGE THIS TO SID OF YOUR
DATABASE

#### This variable is required to set the DB_UNIQUE_NAME parameter for Primary,
it should be unique within the enterprise
ORACLE_DB_UNIQUE_NAME=orcl            #CHANGE THIS TO THE UNIQUE NAME OF
YOUR DATABASE

#### Oracle Data Guard Parameters
DB_PRIMARY_HOST_IP_ADDR=127.0.0.1     #CHANGE THIS TO THE IP OF
YOUR PRIMARY SERVER
DB_PRIMARY_LISTENER_PORT=1521         #CHANGE THIS
TO THE PORT OF YOUR PRIMARY SERVER

#### This variable is required to set the type of installation STANDALONE,
PRIMARY or STANDBY
#### STANDALONE - Installation standalone DB on server (no Data Guard, no RAC)
#### PRIMARY - Installation PRIMARY DB on server for Data Guard setup
#### STANDBY - Installation STANDBY DB on server for Data Guard setup

ORACLE_DB_INSTALLATION_TYPE=PRIMARY   #YOU MUST ENSURE THIS IS SET TO PRIMARY

#### This variable is only used when upgrading STANDALONE to PRIMARY Data Guard
(YES/NO)
ORACLE_DATAGUARD_UPGRADE=NO           #YOU MUST ENSURE THIS
IS SET TO NO

####DG protection mode. Possible values: MAXAVAILABILITY, MAXPERFORMANCE,
MAXPROTECTION
DATAGUARD_MODE=MAXAVAILABILITY        #CHANGE TO THE REQUIRED MODE

```

8. From the `/var/tmp/Analytics/db` directory, make the following script executable and run the following command as the root user.

```
sh root.sh
```

9. Review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the command.
10. Reboot the database server.
11. After the server starts, SSH to the Oracle® Database server and switch to the root user.
12. From the `/var/tmp/Analytics/db` directory, run the following command as the root user to begin the installation process:

```
sh oracle_db_install.sh
```

You must confirm that you have edited the `parameters.conf` file, and you must enter the Oracle user password during the installation.

13. After successful installation, review the output of the script to ensure that no failures or errors occurred during the installation process.

Post installation checks for Oracle® Database

About this task

Perform the following post installation checks for Oracle® Database, if required. This procedure describes checks to perform after the install, and how to manually start or stop the database. After you install Oracle® Database, the database is running.

Important:

Ensure that you use the Oracle user account.

Procedure

1. Run the following command to set the paths required to run **sqlplus**:

```
. ~/.bash_profile
```

Note:

This command returns no output.

2. Run the following commands to manually start the database, if required:

- **sqlplus / as sysdba**
- **STARTUP**

The output must indicate that the database is mounted. You can exit the sqlplus shell by typing **quit**.

3. Run the following command to check whether the listener has started:

```
lsnrctl status
```

4. Run the following command to start the listener, if required:

```
lsnrctl start
```

Installing Standby Oracle® Database

Before you begin

- Install the Primary Oracle® Database, and ensure that the Primary Oracle® Database is running.

About this task

Install Oracle® Database on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. Use this procedure to deploy a Single Instance of Oracle® Database as a Standby server installation in an Oracle Data Guard configuration.

Oracle Data Guard has three protection mode options: Max Availability, Max Performance or Max Protection. You can select your preferred mode using the `parameters.conf` file. Max Availability mode is set by default. The value for the Oracle Data Guard protection mode parameter must match on the Primary and Standby server. Choose your Oracle Data Guard protection mode option based on your solution requirements:

- **Max Availability:** Redo logs are transmitted from the Primary server and written and acknowledged by the Standby server before a commit is complete. In the event of a failure on the Primary server there is zero data loss when you switch over to the Standby server. If the Standby server cannot be reached at any time, the system reverts to Max Performance behavior until connectivity is restored.
- **Max Performance:** Redo logs are transmitted from the Primary server to the Standby server but the commit is complete on the Primary server before the redo log is written to the disk on the Standby server. In the event of a failure on the Primary server, transactions can be lost when you switch over to the Standby server.
- **Max Protection:** Redo logs are transmitted from the Primary server and written and acknowledged by the Standby server before a commit is complete. In the event of a failure on the Primary server there is zero data loss when you switch over to the Standby server. If the Standby server cannot be reached, the Primary server stops processing transactions until the Standby server is functional once again.

For more detailed information about Oracle Data Guard protection modes, refer to Oracle documentation.

The following table lists the requirements for Oracle® Database installation:

Requirement	Description
Java	jdk1.8.x.x.x
DB installation scripts	db.zip
Oracle® Database software	linuxamd64_12102_database_1of2.zip linuxamd64_12102_database_2of2.zip

Procedure

1. Unzip the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.

The `db.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `db.zip` file to the database server using an scp or ftp tool.
3. SSH to the database server as the root user.
4. Create the `/var/tmp/Analytics/` directory.
5. Run the following command to unzip the `db.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics db.zip
```

Example of the directory structure contents:

- `/var/tmp/Analytics/parameters.conf`

6. Copy the following files to the `/var/tmp/Analytics/` directory:

- `linuxamd64_12102_database_1of2.zip`
- `linuxamd64_12102_database_2of2.zip`

7. Make the following changes to the `/var/tmp/Analytics/parameters.conf` file based on the information relevant to your server:

```
#### SYSTEM common settings ####
DOMAIN=domain.com                #CHANGE THIS TO THE DOMAIN NAME ONLY I.E
DOMAIN.COM
NTP_HOST=127.0.0.1                #CHANGE THIS TO THE NTP IP OR HOSTNAME IF NTP
NOT_ALREADY_CONFIGURED
JAVA_HOME=/usr/java/latest       #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION

#### Oracle DB Parameters ####
DB_HOSTNAME=localhost            #CHANGE THIS TO THE HOSTNAME
ONLY (NOT THE FQDN)
DB_HOST_IP_ADDR=127.0.0.1        #CHANGE THIS TO THE IP OF
YOUR SERVER
DB_LISTENER_PORT=1521
#CHANGE THIS TO LISTENER PORT OF YOUR DATABASE
DB_NAMESERVER=127.0.0.1         #CHANGE THIS TO THE IP/
HOSTNAME OF YOUR DNS SERVER

#### This variable is required to set the ORACLE_SID environment variable for
user .bash_profile
ORACLE_DB_SID=orcl              #CHANGE THIS TO SID OF YOUR
DATABASE

#### This variable is required to set the DB_UNIQUE_NAME parameter for Primary,
it should be unique within the enterprise
ORACLE_DB_UNIQUE_NAME=orcl      #CHANGE THIS TO THE UNIQUE NAME OF
YOUR DATABASE

#### This variable is required to set the DB_UNIQUE_NAME parameter for Standby,
it should be unique within the enterprise
ORACLE_DB_STBY_UNIQUE_NAME=orcl_stby #CHANGE THIS TO THE UNIQUE NAME
OF YOUR STANDBY DATABASE

#### This variable is required to set the DB_UNIQUE_NAME parameter for additional
DB running on stb host, it should be unique within the enterprise
ORACLE_DB_RCU_UNIQUE_NAME=orclrcu  #CHANGE THIS TO THE UNIQUE NAME OF
YOUR RCU DATABASE

#### Oracle Data Guard Parameters
DB_PRIMARY_HOST_IP_ADDR=127.0.0.1 #CHANGE THIS TO THE IP OF YOUR PRIMARY
SERVER
DB_PRIMARY_LISTENER_PORT=1521     #CHANGE THIS TO THE PORT OF YOUR
PRIMARY SERVER
DB_STBY_HOST_IP_ADDR=127.0.0.1    #CHANGE THIS TO THE IP OF YOUR STANDBY
SERVER
DB_STBY_LISTENER_PORT=1521        #CHANGE THIS TO THE PORT OF
YOUR STANDBY SERVER

#### This variable is required to set the type of installation STANDALONE,
PRIMARY or STANDBY
#### STANDALONE - Installation standalone DB on server (no Data Guard, no RAC)
#### PRIMARY - Installation PRIMARY DB on server for Data Guard setup
#### STANDBY - Installation STANDBY DB on server for Data Guard setup

ORACLE_DB_INSTALLATION_TYPE=STANDBY #YOU MUST ENSURE THIS IS SET TO STANDBY
```

```
#### This variable is only used when upgrading STANDALONE to PRIMARY Data Guard
(YES/NO)
ORACLE_DATAGUARD_UPGRADE=NO                                #YOU MUST ENSURE THIS
IS SET TO NO

####DG protection mode. Possible values: MAXAVAILABILITY, MAXPERFORMANCE,
MAXPROTECTION
DATAGUARD_MODE=MAXAVAILABILITY    #CHANGE TO THE REQUIRED MODE
```

8. From the `/var/tmp/Analytics/db` directory, make the following script executable and run the following command as the root user.

```
sh root.sh
```

When prompted to enter the password for the Oracle user: "Enter password for oracle:", enter the password.

9. After the script completes, review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the script.
10. Reboot the database server.
11. After the server starts, SSH to the Oracle® Database server and switch to the root user.
12. From the `/var/tmp/Analytics/db` directory, run the following command as the root user to begin the installation process:

```
sh oracle_db_install.sh
```

You must confirm that you have edited the `parameters.conf` file, and you must enter the Oracle user password and the Primary server SYS user password during the installation.

13. After the Standby server software installation, respond to the Repository Creation Utility (RCU) prompts.

 Note:

The `ORACLE_DB_RCU_UNIQUE_NAME` parameter in the `parameters.conf` file contains the SID for the newly installed database.

14. After successful installation, review the output of the script to ensure that no failures or errors occurred during the installation process.

Post installation checks for Standby Oracle® Database

About this task

Perform the following checks after installing Standby Oracle® Database. This procedure describes checks to perform after the install to ensure that both database instances are running.

 Important:

Ensure that you use the Oracle user account.

Procedure

1. Run the following command to set the paths required to run `sqlplus`:

```
. ~/.bash_profile
```

*** Note:**

This command returns no output.

2. Run the following command to check whether the listener has started:

```
lsnrctl status
```

3. Run the following command to start the listener, if required:

```
lsnrctl start
```

4. Ensure that you can ping both instances of Oracle® Database using the following commands:

- `tnsping orcl`
- `tnsping orcl_stby`

5. Ensure that you can connect to both instances of Oracle® Database using sqlplus:

- `sqlplus sys/welcome1@orcl as sysdba`
- `sqlplus sys/welcome1@orcl_stby as sysdba`

6. Confirm that Data Guard configuration is successful using the following command:

- `dgmgrl sys/welcome1@orcl`
- `SHOW CONFIGURATION`

Ensure that the result is successful.

Next steps

For more information about Oracle® Database switchover testing, see *Avaya Oceana® Solution Disaster Recovery*.

Installing Oracle® RAC Database

Before you begin

- Ensure that you have performed all of the required preconfiguration on the server.

About this task

Install Oracle® RAC Database on Red Hat Enterprise Linux (RHEL) servers, for use with Avaya Analytics™.

The following table lists the requirements for Oracle® RAC Database installation:

Requirement	Description
Java	jdk1.8.x.x.x

Table continues...

Requirement	Description
ASMLib rpm	oracleasm-lib-2.0.4-1.el6.x86_64.rpm oracleasm-support-2.1.8-1.el6.x86_64.rpm
DB installation scripts	rac_db.zip
Oracle Grid infrastructure software	V46095-01_1of2.zip V46095-01_2of2.zip
Oracle® Database software	V46096-01_1of2.zip V46096-01_2of2.zip
2 network interface cards (NICs) on each node in the cluster	All nodes must have a minimum of 2 NICs configured on 2 different LANs, which must support multicast. One network is used for external communication, and the other network must be reserved for communication between Oracle® RAC Database nodes only.
SAN attached to all servers	For ASM configuration, you must attach block devices to all servers in the cluster.
DNS configuration	Single Client Access Name (SCAN) - this provides a single name for clients to access any Oracle® Database running in a cluster. In an Avaya Analytics™ solution, this is the name of the Database server used for the Database connection. The name must resolve to at least N+1 IP addresses on a public LAN (where N = number of nodes in the cluster).

Procedure

1. Unzip the AvayaAnalytics_x.x.x.x_Build_xx.zip file.
The rac_db.zip file is available in the Oracle_Installers folder.
2. SSH to the database server as the root user.
3. Create the /var/tmp/Analytics/ directory.
4. Run the following command to unzip the rac_db.zip file to the /var/tmp/Analytics directory:

```
unzip -d /var/tmp/Analytics rac_db.zip
```
5. Copy the following files to the directory:
 - V46095-01_1of2.zip
 - V46095-01_2of2.zip
 - V46096-01_1of2.zip
 - V46096-01_2of2.zip
6. Check that all nodes have 2 NICs configured on 2 different LANs. You can use the **ifconfig** command to check your networking configuration. The following is an example of the required configuration, with a private IP address assigned to the second NIC:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001 inet
192.168.0.1 netmask 255.255.255.0 broadcast 192.168.255.255

edge0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1400 inet
192.168.1.1 netmask 255.255.255.0 broadcast 192.168.255.255
```

7. Configure the `/etc/hosts` file with IP addresses for use by the cluster on both nodes. The following is an example of the required configuration:

```
#Public
192.168.0.1 myracnode01 myracnode01.myrachostedzone.net
192.168.0.2 myracnode02 myracnode02.myrachostedzone.net

#Private
192.168.1.1 myrac01priv myrac01priv.myrachostedzone.net
192.168.1.2 myrac02priv myrac02priv.myrachostedzone.net

#Virtual
192.168.2.3 myrac01vip myrac02vip.myrachostedzone.net
192.168.2.4 myrac02vip myrac01vip.myrachostedzone.net
```

8. Verify that the SCAN resolves to multiple IP addresses. The name must resolve to at least N+1 IP addresses, for example in an Avaya Analytics™ solution with 2 nodes, the SCAN must resolve to 3 IP addresses. You can use the `nslookup` command to check your DNS configuration. The following is an example of the required configuration:

```
nslookup myracscan

Server: 192.168.1.47
Address: 192.168.1.47#53

Name: myracscan.myrachostedzone.net
Address: 192.168.1.10

Name: myracscan.myrachostedzone.net
Address: 192.168.1.11

Name: myracscan.myrachostedzone.net
Address: 192.168.1.12
```

9. Edit the `/etc/selinux/config` file and set `SELINUX=disabled`. You must perform this step on both nodes and as the root user.
10. Stop and disable the firewall using the following command. You must perform this step on both nodes and as the root user.

```
systemctl stop firewalld

systemctl disable firewalld
```

11. Create the following users and groups using the following commands. You must perform this step on both nodes and as the root user.

```
groupadd -g 54321 oinstall

groupadd -g 54322 dba

groupadd -g 54323 oper

useradd -u 54321 oracle
```

```

passwd oracle

usermod -g oinstall oracle

usermod -a -G dba oracle

usermod -a -G oper oracle

mkdir -p /u01/app/12.1.0/grid_1

chown -R oracle:oinstall /u01

chmod -R 775 /u01

```

12. Edit the `/etc/sysctl.conf` file, making the following changes on both nodes and as the root user:

```

fs.file-max = 6815744
kernel.sem = 250 32000 100 128
kernel.shmmni = 4096
kernel.shmall = 1073741824
kernel.shmmax = 4398046511104
net.core.rmem_default = 262144
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 1048576
fs.aio-max-nr = 1048576
net.ipv4.ip_local_port_range = 9000 65500

```

Apply kernel changes using the following command:

```
sysctl -p
```

13. Edit the `/etc/security/limits.conf` file, making the following changes on both nodes and as the root user:

```

oracle soft nfile 16384
oracle hard nfile 65536
oracle soft nproc 16384
oracle hard nproc 16384
oracle soft stack 10240
oracle hard stack 32768

```

14. You must disable avahi-daemon on both nodes. Run the following command as the root user:

```
systemctl stop avahi-daemon
```

```
systemctl stop avahi-daemon
```

15. Edit the `/etc/sysconfig/network` file by adding the following line. You must perform this step on both nodes and as the root user.

```
NOZEROCONF=yes
```

16. Configure Oracle Automatic Storage Management (ASM). To create partitions, run the following command on Node 1 as the root user:

```
fdisk /dev/sdb
```

Answer the prompts in the following sequence: "n", "p", "1", "return", "return" and "w". Repeat this step for all disks used for ASM installation.

17. Reboot Node 1.

18. After Node 1 starts, to configure ASM on-boot properties, run the following commands on both nodes and as the root user:

```
oracleasm configure -i

Configuring the Oracle ASM library driver.

This will configure the on-boot properties of the Oracle ASM library
driver. The following questions will determine whether the driver is
loaded on boot and what permissions it will have. The current values
will be shown in brackets ('[]'). Hitting <ENTER> without typing an
answer will keep that current value. Ctrl-C will abort.

Default user to own the driver interface [oracle]: oracle
Default group to own the driver interface [oinstall]: oinstall
Scan for Oracle ASM disks on boot (y/n) [y]: y
Writing Oracle ASM library driver configuration: done
```

19. Run the following command on Node 1 as the root user:

```
oracleasm createdisk DISK1 /dev/sdb1
Writing disk header: done
Instantiating disk: done
```

Reboot both nodes.

20. After both nodes start, you can run the following command to list the disks on both nodes:

```
oracleasm scandisks
Reloading disk partitions: done
Cleaning any stale ASM disks...
Scanning system for ASM disks...

oracleasm listdisks
DISK1
```

21. Run the following command to change owner and access rights to the /var/tmp/Analytics directory:

```
chown oracle:oinstall -Rf /var/tmp/Analytics
chmod 775 -Rf /var/tmp/Analytics
```

22. Make the following changes to the /var/tmp/Analytics/parameters.conf file and the /var/tmp/Analytics/rac/source/ .rsp files:

```
parameters.conf file:
ORACLE_HOSTNAME=Node1
SCAN_NAME=myracscan
RAC_NODE_1=Node1           #The hostname of NODE 1
RAC_NODE_2=Node2           #The hostname of NODE 2
CLUSTER_NODES_IPS=rac1:rac1-vip, rac2:rac2-vip           #replace rac1-vip and rac2-
vip with the hostname from the virtual section of the hosts file (for example
myrac01vip or myrac02vip)

# PUBLIC INTERFACE_NAME, PUBLIC_SUBNET are mandatory, it is used for connection
to the RAC from other applications, change default value 255.255.255.255
# PUBLIC_INTERFACE_NAME=eth0
```

```
# PUBLIC_SUBNET=192.168.1.0
PUBLIC_INTERFACE_NAME=
PUBLIC_SUBNET=255.255.255.255
# PRIVATE_INTERFACE_NAME, PRIVATE_SUBNET are mandatory, it is used for cluster
operations, change default value 255.255.255.255
# PRIVATE_INTERFACE_NAME=eth1
# PRIVATE_SUBNET=192.168.2.0
PRIVATE_INTERFACE_NAME=
PRIVATE_SUBNET=255.255.255.255
# All other network interfaces must be listed as comma separated values (no blank
spaces), if any exists
# NOT_USED_INTERFACE_NAMES=eth2,eth3
# NOT_USED_SUBNETS=192.168.10.0,192.168.20.0
NOT_USED_INTERFACE_NAMES=
NOT_USED_SUBNETS=
```

The following table shows the parameter dependencies between the parameters.conf and .rsp files in the /var/tmp/Analytics/rac/source directory.

parameters.conf	grid.rsp	db.rsp	dbca.rsp
SCAN_PORT=1521	oracle.install.crs.config .gpnscanPort		
SCAN_NAME=rac-scan	oracle.install.crs.config .gpnscanName		
RAC_NODE_2=rac2		oracle.install.db.CLUSTER_NODES	NODELIST
RAC_NODE_1=rac1		oracle.install.db.CLUSTER_NODES	NODELIST
ORACLE_USER=oracle			
ORACLE_SERVICE=oracle			GDBNAME, SID
ORACLE_INVENTORY_LOCATION=/u01/app/oraInventory	INVENTORY_LOCATION	INVENTORY_LOCATION	
ORACLE_HOSTNAME=rac1	ORACLE_HOSTNAME	ORACLE_HOSTNAME	
ORACLE_GRID_RESPONSE_FILE=/var/tmp/Analytics/rac/source/grid.rsp			
ORACLE_GRID_HOME=/u01/app/12.1.0/grid_1	ORACLE_HOME		
ORACLE_DUMP_DIR=/var/tmp/Analytics			

Table continues...

parameters.conf	grid.rsp	db.rsp	dbca.rsp
ORACLE_DBCA_RESPONSE_FILE=/var/tmp/Analytics/rac/source/dbca.rsp			
ORACLE_DB_RESPONSE_FILE=/var/tmp/Analytics/rac/source/db.rsp			
ORACLE_DB_HOME=/u01/app/oracle/product/12.1.0/dbhome_1		ORACLE_HOME	
ORACLE_BASE=/u01/app/oracle	ORACLE_BASE	ORACLE_BASE	
ORACLE_ASM_RESPONSE_FILE=/var/tmp/Analytics/rac/source/asm_password.rsp			
ORACLE_ASM_DISKS=DISK1	oracle.install.asm.diskGroup.disks		
JAVA_HOME=/usr/java/latest			
CLUSTER_NODES_IPS=rac1:rac1	oracle.install.crs.config.clusterNodes		
CLUSTER_NAME=rac	oracle.install.crs.config.clusterName		
ASM_DISKS=/dev/oracleasm/disks/DISK1	oracle.install.asm.diskGroup.disks		
* additional changes in .rsp files	oracle.install.asm.diskGroup.name=DATA oracle.install.crs.config.networkInterfaceList needs to be modified as described earlier		SERVICEUSERPASSWORD = Admin123 DISKGROUPNAME=DATA

23. From the `/var/tmp/Analytics/rac` directory, run the following command to begin the installation process:

```
./rac_install.sh
```

The system prompts you to enter the Oracle user password during the installation.

24. During the install, you must perform cluster verification. Review the `/var/tmp/Analytics/rac/cluster_verification.log` for errors and warnings. Continue with the install by entering `y`.

25. During the install, you must then perform root actions. When prompted, open new sessions as the root user and follow the system prompts. You must run the following commands at this point:
 - a. On Node1, run `/u01/app/oraInventory/orainstRoot.sh`. Wait for the script to finish before proceeding.
 - b. On Node1 and Node2, run `/u01/app/12.1.0/grid_1/root.sh`. Wait for the script to finish before proceeding.
 - c. Run any other commands when prompted.
26. After the script finishes, type `y` to continue with the DBCA utility.
27. A message appears when the install is complete. After successful installation, review the output of the script to ensure that no failures or errors occurred during the installation process.

Post installation checks for Oracle® RAC Database

The following is the list of post installation checks for Oracle® RAC Database.

- Run the following commands as the root user on both nodes to check the status of the cluster:

```
. oraenv
```

When prompted, type `+ASM1` or `+ASM2`, depending on the node you are running the command on.

```
crsctl status res -t
```

Verify that all resources have a status of 'ONLINE', for example:

```
[root@myracnode01 ~]# . oraenv
ORACLE_SID = [root] ? +ASM1
The Oracle base has been set to /u01/app/oracle
[root@myracnode01 ~]# crsctl status res -t
```

Name	Target	State	Server	State details	
Local Resources					
ora.DATADG.dg	ONLINE	ONLINE	myracnode01	STABLE	
	ONLINE	ONLINE	myracnode02	STABLE	
ora.LISTENER.lsnr	ONLINE	ONLINE	myracnode01	STABLE	
	ONLINE	ONLINE	myracnode02	STABLE	
ora.asm	ONLINE	ONLINE	myracnode01	Started, STABLE	
	ONLINE	ONLINE	myracnode02	Started, STABLE	
ora.net1.network	ONLINE	ONLINE	myracnode01	STABLE	
	ONLINE	ONLINE	myracnode02	STABLE	
ora.ons	ONLINE	ONLINE	myracnode01	STABLE	
	ONLINE	ONLINE	myracnode02	STABLE	
Cluster Resources					
ora.LISTENER_SCAN1.lsnr	1	ONLINE	ONLINE	myracnode01	STABLE
ora.LISTENER_SCAN2.lsnr	1	ONLINE	ONLINE	myracnode01	STABLE
ora.LISTENER_SCAN3.lsnr	1	ONLINE	ONLINE	myracnode01	STABLE
ora.MGMTLSNR	1	ONLINE	ONLINE	myracnode01	169.254.50.205 192.168.16.43, STABLE
ora.cvu	1	ONLINE	ONLINE	myracnode01	STABLE
ora.mgmtldb	1	ONLINE	ONLINE	myracnode01	Open, STABLE
ora.myracnode01.vip	1	ONLINE	ONLINE	myracnode01	STABLE
ora.myracnode02.vip	1	ONLINE	ONLINE	myracnode02	STABLE
ora.oc4j	1	ONLINE	ONLINE	myracnode01	STABLE
ora.orcl.db	1	ONLINE	ONLINE	myracnode01	Open, STABLE
	2	ONLINE	ONLINE	myracnode02	Open, STABLE
ora.scan1.vip	1	ONLINE	ONLINE	myracnode01	STABLE
ora.scan2.vip	1	ONLINE	ONLINE	myracnode01	STABLE
ora.scan3.vip	1	ONLINE	ONLINE	myracnode01	STABLE

- Run the following commands as the Oracle user on Node 1 to check the listener status:

```
. oraenv
```

When prompted, type `orcl1`

```
srvctl status listener
```

Verify that the LISTENER is enabled and running, for example:

```
[oracle@myracnode01 ~]$ . oraenv
ORACLE_SID = [orcl1] ? orcl1
The Oracle base remains unchanged with value /u01/app/oracle
[oracle@myracnode01 ~]$ srvctl status listener
Listener LISTENER is enabled
Listener LISTENER is running on node(s): myracnode02,myracnode01
[oracle@myracnode01 ~]$
```

- Run the following commands as the Oracle user on Node 1 to check the database:

```
$ . oraenv
```

When prompted, type `orcl1`

If prompted for the ORACLE_HOME parameter, the correct path is ORACLE_GRID_HOME as set in the parameters.conf file.

```
$ sqlplus sys/Admin123@orcl as sysdba
```

```
SQL> select instance_name from gv$instance
```

Verify that the following output appears:

```
INSTANCE_NAME
-----
orcl1
orcl2
```

Testing a failover

About this task

This procedure describes how to test a failover after installing both RAC nodes. Completing this procedure proves that when Node 1 stops, all resources move to Node 2. Perform this procedure as the root user.

Procedure

1. On Node 1, run the following command:

```
crsctl stop crs
```

2. On Node 2, run the following command:

```
crsctl status res -t
```

Verify that all resources are now on Node 2 only.

3. On Node 1, run the following command:

```
crsctl start crs
```

4. On Node 2, run the following command:

```
crsctl stop crs
```

5. Verify that all resources are now on Node 1 only.

Stopping Oracle® RAC Database

Before you begin

Before you stop Oracle® RAC Database, ensure that there are no applications accessing the database.

About this task

This procedure describes how to stop Oracle® RAC Database.

Procedure

1. As the Oracle user, use the following commands to set the environment variable:

```
$ . oraenv
```

If prompted for the ORACLE_HOME parameter, the correct path is ORACLE_DB_HOME as set in the parameters.conf file.

```
ORACLE_SID = [oracle] ? orcl
```

2. Stop the listener on both nodes, and check the listener status using the following commands:

```
$ srvctl stop listener
```

```
$ srvctl status listener
```

Verify that LISTENER is not running.

3. Shut down RAC on both nodes, and check the status, using the following commands:

```
$ srvctl stop database -d orcl
```

```
$ srvctl status database -d orcl
```

Note:

In the example command above, 'orcl' is the SID of the database.

Verify that both instances are not running.

4. Shut down the ASM instances on both nodes which access the database, using the following commands:

```
$ srvctl stop asm -n rac1 -f
```

```
$ srvctl stop asm -n rac2 -f
```

```
$ srvctl status asm -n rac1
ASM is not running on rac1
```

```
$ srvctl status asm -n rac2
ASM is not running on rac2
```

5. Run the following command to stop applications:

```
$ srvctl stop nodeapps -f
```

Verify that the following output appears after you run the **srvctl status** command:

```
$ srvctl status nodeapps
VIP rac1-vip is enabled
VIP rac1-vip is not running
VIP rac2-vip is enabled
VIP rac2-vip is not running
Network is enabled
Network is not running on node: rac1
Network is not running on node: rac2
ONS is enabled
ONS daemon is not running on node: rac1
ONS daemon is not running on node: rac2
```

6. Shut down Oracle Clusterware. Oracle Clusterware is run by Cluster Ready Services (CRS). Use the following command to stop all CRS related processes. You must run this command as the root user on both nodes:

```
# . oraenv
```

```
ORACLE_SID = [root] ? +ASM1
```

If prompted for the ORACLE_HOME parameter, the correct path is ORACLE_GRID_HOME as set in the parameters.conf file.

```
# crsctl stop crs
```

Starting Oracle® RAC Database

About this task

This procedure describes how to start Oracle® RAC Database.

Procedure

1. Start Oracle Clusterware. Oracle Clusterware is run by Cluster Ready Services (CRS). CRS starts automatically when the node starts up. If the CRS does not start automatically, run the following commands as the root user:

```
# . oraenv
```

```
ORACLE_SID = [root] ? +ASM1
```

If prompted for the ORACLE_HOME parameter, the correct path is ORACLE_GRID_HOME as set in the parameters.conf file.

```
# crsctl start crs
```

2. You must run the remaining commands in this procedure as the Oracle user. As the Oracle user, use the following commands to set the environment variable:

```
$ . oraenv
```

If prompted for the ORACLE_HOME parameter, the correct path is ORACLE_DB_HOME as set in the parameters.conf file.

```
ORACLE_SID = [oracle] ? orcl1
```

3. Run the following command to start applications:

```
$ srvctl start nodeapps
```

Verify that the following output appears after you run the **srvctl status** command:

```
$ srvctl status nodeapps
VIP rac1-vip is enabled
VIP rac1-vip is running on node: rac1
VIP rac2-vip is enabled
VIP rac2-vip is running on node: rac2
Network is enabled
Network is running on node: rac1
Network is running on node: rac2
ONS is enabled
ONS daemon is running on node: rac1
ONS daemon is running on node: rac2
```

4. Start the ASM instances on both nodes which access the database, using the following commands:

```
$ srvctl start asm -n rac1
$ srvctl status asm -n rac1
ASM is running on rac1

$ srvctl start asm -n rac2
$ srvctl status asm -n rac2
ASM is running on rac2
```

5. Start RAC on both nodes, and check the status, using the following commands:

```
$ srvctl start database -d orcl
```

```
$ srvctl status database -d orcl
```

 Note:

In the example command above, 'orcl' is the SID of the database.

Verify that both instances are running.

6. Start the listener on both nodes, and check the listener status using the following commands:

```
$ srvctl start listener
```

```
$ srvctl status listener
```

Verify that LISTENER is running on both nodes.

Installing Oracle® Business Intelligence

About this task

Install Oracle® Business Intelligence on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™.

The following table lists the requirements for Oracle® Business Intelligence:

Requirement	Description
Java	jdk1.8.x.x.x
OBI installation scripts	obiee.zip
Oracle® Fusion Middleware software	fmw_12.2.1.3.0_infrastructure_Disk1_1of1.zip
Oracle® Business Intelligence software	fmw_12.2.1.3.0_bi_linux64_Disk1_1of2.zip fmw_12.2.1.3.0_bi_linux64_Disk1_2of2.zip

Procedure

1. Unzip the AvayaAnalytics_x.x.x.x_Build_xx.zip file.

The obiee.zip file is available in the Oracle_Installers/Nodal folder.

2. Copy the obiee.zip file to the OBIEE server using an scp or ftp tool.
3. SSH to the OBIEE server as the root user.
4. Create the /var/tmp/Analytics/ directory.
5. Run the following command to unzip the obiee.zip file to the /var/tmp/Analytics directory:

```
unzip -d /var/tmp/Analytics obiee.zip
```

Example of the directory structure contents:

- /var/tmp/Analytics/parameters.conf

6. Copy the following files to the /var/tmp/Analytics/ directory:

- fmw_12.2.1.3.0_infrastructure_Disk1_1of1.zip
- fmw_12.2.1.3.0_bi_linux64_Disk1_1of2.zip
- fmw_12.2.1.3.0_bi_linux64_Disk1_2of2.zip

7. Make the following changes to the /var/tmp/Analytics/parameters.conf file:

```
DOMAIN=domain.com                #CHANGE THIS TO THE DOMAIN NAME
ONLY I.E DOMAIN.COM
NTP_HOST=localhost                #CHANGE THIS TO THE NTP IP OR
HOSTNAME
JAVA_HOME=/usr/java/latest       #CHANGE THIS TO POINT AT THE JAVA
HOME_LOCATION
#### OBIEE Parameters ####
OBI_HOSTNAME=localhost           #CHANGE THIS TO THE HOSTNAME
```

```

ONLY (NOT THE FQDN)
OBI_HOST_IP_ADDR=127.0.0.1           #CHANGE THIS TO THE IP OF YOUR
SERVER                               #CHANGE THIS TO THE IP/
OBI_NAMESERVER=localhost             #CHANGE THIS TO THE IP, PORT
HOSTNAME OF YOUR DNS SERVER          AND SID OF YOUR ORACLE DATABASE. FOR RAC DATABASE, USE THE SCAN IN PLACE OF THE IP
OBI_DB_CONNECT_STRING=192.168.119.60:1521:orcl

```

8. From the `/var/tmp/Analytics/obiee` directory, make the following script executable and run the following command as the root user:

```
sh root.sh
```

When prompted to enter the password for the Oracle user: "Enter password for oracle:", enter the password.

9. After the script completes, review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the script.
10. Verify that the host name is correctly configured in the `/etc/hosts` file.
11. Verify that the DNS server is correctly configured in the `/etc/resolv.conf` file.
12. Reboot the OBIEE server.
13. After the server starts, SSH to the server as the root user.
14. From the `/var/tmp/Analytics/obiee` directory, run the following command as the root user:

```
sh oracle_obiee_install.sh
```

You must enter the Weblogic Administrator password, the RCU schema password, and the database SYS user password during the installation.

Important:

You must ensure that the Weblogic Administrator password contains alphanumeric characters and the following special characters only: "_", "\$", "#"

15. Review the output of the script and ensure that no failures or errors have occurred during the installation process.

Post installation checks for Oracle® Business Intelligence

The following is the list of post installation checks for Oracle® Business Intelligence.

Important:

Ensure that you use the Oracle user account.

- Run the following command from the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` location to verify that all components have the RUNNING status:

```
./status.sh
```

- In your web browser, enter the following URL to access OBI analytics:

`http://<OBI_SERVER_IP>:9502/analytics`

- Run the following command to start the OBIEE server:

`./start.sh`

- Run the following command to stop the OBIEE server:

`./stop.sh`

Installing Oracle® Data Integrator

About this task

Install Oracle® Data Integrator on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. You must install Oracle® Data Integrator on the same server as Oracle® Business Intelligence, after the OBI installation.

The following table lists the requirements for Oracle® Data Integrator:

Requirement	Description
Java	jdk1.8.x.x.x
ODI installation scripts	odi.zip
Oracle® Data Integrator software	fmw_12.2.1.0.0_odi_Disk1_1of2.zip fmw_12.2.1.0.0_odi_Disk1_2of2.zip

Procedure

1. Unzip the AvayaAnalytics_x.x.x.x_Build_xx.zip file.

The `odi.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `odi.zip` file to the ODI server using an scp or ftp tool.

Oracle® Data Integrator and Oracle® Business Intelligence are installed on the same server. Therefore, you can use the IP address of the OBI server.

3. SSH to the ODI server as the root user.

4. If the installation scripts of Oracle® Business Intelligence are still present in the `/var/tmp/Analytics/` directory, perform the following steps:

- a. Create the `/var/tmp/Analytics_OBI_Installation/` directory.
- b. Run the following command to move the content of the `/var/tmp/Analytics/` directory to the `/var/tmp/Analytics_OBI_Installation/` directory:

```
mv /var/tmp/Analytics /var/tmp/Analytics_OBI_Installation
```

5. Copy the `odi.zip` file to the `/var/tmp/Analytics/` directory using an scp or ftp tool.
6. Run the following command to unzip the `odi.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics odi.zip
```

Example of the directory structure:

- /var/tmp/Analytics/parameters.conf

*** Note:**

When you unzip the `odi.zip` file, the `/var/tmp/Analytics/parameters.conf` file used when installing Oracle® Business Intelligence is overwritten. You must consider this if you need to uninstall Oracle® Business Intelligence after the file is overwritten.

7. Copy the following files to the `/var/tmp/Analytics/` directory using an scp or ftp tool:

- `fmw_12.2.1.0.0_odi_Disk1_1of2.zip`
- `fmw_12.2.1.0.0_odi_Disk1_2of2.zip`

8. Make the required changes to the `/var/tmp/Analytics/parameters.conf` file:

```
#### SYSTEM common settings ####
ORACLE_USER=oracle
DOMAIN=domain.com #CHANGE THIS TO THE DOMAIN NAME ONLY I.E DOMAIN.COM
NTP_HOST=localhost #CHANGE THIS TO THE NTP IP OR HOSTNAME
JAVA_HOME=/usr/java/latest #CHANGE THIS TO POINT AT THE JAVA

##### This is the location where you will have all the sotware ZIP files and the
installer
##### scripts folder and parameter file
ORACLE_DUMP_DIR=/var/tmp/Analytics

#### Oracle Software Installation directory
ORACLE_APP_DIR=/home/oracle/app

#### Oracle ODI Parameters ####
ODI_HOSTNAME=localhost #CHANGE THIS TO THE HOSTNAME ONLY (NOT THE FQDN)
ODI_HOST_IP_ADDR=127.0.0.1 #CHANGE THIS TO THE IP OF YOUR SERVER
ODI_NAMESERVER=localhost #CHANGE THIS TO THE IP/HOSTNAME OF YOUR DNS SERVER

#### This variable is required to set the ORACLE_SID environment variable for
user .bash_profile
ORACLE_DB_SID=orcl
ODI_DB_RCUI_SID="orclrcu"
ORACLE_DB_BASE=/home/oracle/app/oracle
ORACLE_DB_HOME=/home/oracle/app/oracle/product/12.1.0/dbhome_1
ORACLE_DB_INVENTORY_LOCATION=/home/oracle/oraInventory

#### This variable is required to set the type of installation
#### STANDALONE - ODI is installed on standalone DB (no Data Guard, no RAC)
#### PRIMARY - ODI is installed on PRIMARY DB for Data Guard setup
#### STANDBY - ODI is installed on STANDBY DB for Data Guard setup
INSTALLATION_TYPE=STANDALONE

#### Oracle Software Silent Installation response file location
#### It fould be in side installater folder
#### You must change oracle home if ORACLE_DB HOME changed
#ORACLE_DB_RESPONSE_FILE=${ORACLE_DUMP_DIR}/db/source/db.rsp
#ORACLE_DBCA_RESPONSE_FILE=${ORACLE_DUMP_DIR}/db/source/dbca.rsp

#### ODI HOME parameters ####
```

```

ODI_ORACLE_HOME=/home/oracle/app/oracle/Oracle_Home_ODI_Standalone
ODI_SCHEMA_PREFIX=ODI
ODI_CONNECT_STRING=127.0.0.1:1521:orcl #CHANGE THIS TO THE IP, PORT AND SID OF
YOUR ORACLE DATABASE. FOR RAC DATABASE, USE THE SCAN IN PLACE OF THE IP
# ODI JAR executable has to be the same folder where oracle_odi_install.sh is run.
ODI_JAR=${ORACLE_DUMP_DIR}/odi/fmw_12.2.1.0.0_odi.jar

# ZIPs should be placed in dump location
ODI_INSTALL_ZIP1=${ORACLE_DUMP_DIR}/fmw_12.2.1.0.0_odi_Disk1_1of2.zip
ODI_INSTALL_ZIP2=${ORACLE_DUMP_DIR}/fmw_12.2.1.0.0_odi_Disk1_2of2.zip

# Other dependent files should be placed in /odi/source
ODI_RESPONSE_FILE=${ORACLE_DUMP_DIR}/odi/source/odi.rsp
ODI_UNINSTALL_RESPONSE_FILE=${ORACLE_DUMP_DIR}/odi/source/odi_uninstall.rsp
ODI_CREATE_DOMAIN_PY=${ORACLE_DUMP_DIR}/odi/source/createOdiDomain.py
ODI_DOMAIN_PROPERTIES=${ORACLE_DUMP_DIR}/odi/source/environment.properties

#### ODI Repository Creation parameters from ex ../odi/source/rcuparam.conf ####

# Oracle DB sys password (supplied interactively)
#SYS_PWD=

# Schema password(supplied interactively). This password will be used for all
schema users of the following components:ODI,STB.
#SCHEMA_PWD=

# Supervisor password(supplied interactively): [Min Length:6, Max Length:12]
#SUPERVISOR_PWD=

# Work Repository Type: [(D) Development (Default) or (E) Execution]
WORK_REPOSITORY_TYPE=D

# Work Repository Name
WORK_REPOSITORY_NAME=WORKREP

# Work Repository Password (supplied interactively)
#WORK_REPO_PWD=

# Encryption Algorithm: [AES-128 (Default) or AES-256]
ENCRYPTION_ALGORITHM=AES-128

### Domain Creation Parameters ###
ODI_LISTEN_ADDRESS=127.0.0.1
odi_port=20910

# Middleware Home of your environment
MW_HOME=/home/oracle/app/oracle/Oracle_Home_ODI_Standalone

# The STB schema username created through RCU. Ends with _STB
# ODI Master and Work repository and Opss database connections
# are fetched from this schema
SERVICE_DB_USER=ODI_STB

# JDBC URL to the STB database
# Make sure to use the right URL format
SERVICE_DB_URL=jdbc:oracle:thin:@//127.0.0.1:1521/orcl

# Work repository name
# normally WORKREP
ODI_WORK_REPOSITORY_NAME=WORKREP

```

9. Edit the following parameters in the `AGENT_OracleDIAgent1.xml` file in the `/var/tmp/Analytics` directory:

```
<Field name="HostName" type="java.lang.String"><![CDATA[127.0.0.1]]></Field>
#UPDATE THE IP ADDRESS TO USE THE ODI SERVER IP ADDRESS
```

10. Run the following commands to change the permission and owner of all installation files to the Oracle user configured during the Oracle® Business Intelligence installation:

- `chmod 755 -Rf /var/tmp/Analytics`
- `chown oracle:oinstall -Rf /var/tmp/Analytics`

11. From the `/var/tmp/Analytics/odi/` directory, run the following command as the root user.

```
sh oracle_odi_install.sh
```

The system prompts you to enter the Oracle user password during the installation:

"Please confirm that you have edited the `parameters.conf` for ODI install, by entering `y` to continue:- "

12. Review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the command.

Installing Streams server software

Before you begin

- Ensure that Oracle® Database is running.

About this task

Install Streams server software on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. You must install WebLogic Server (WLS) software on the Avaya Analytics™ Streams server. Use the following procedure to install WLS.

The following table lists the requirements for the Streams server software install:

Requirement	Description
Java	jdk1.8.x.x.x
Streams server (WLS) installation scripts	WLS Installation Scripts
WebLogic Server installation software	fmw_12.2.1.3.0_wls_Disk1_1of1.zip

Procedure

1. Unzip the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.

The `wls.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `wls.zip` file to the Avaya Analytics™ Streams server using an scp or ftp tool.
3. SSH to the Avaya Analytics™ Streams server as the root user.
4. Create the `/var/tmp/Analytics/` directory.

5. Run the following command to unzip the `wls.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics wls.zip
```

Example of the directory structure contents:

- `/var/tmp/Analytics/parameters.conf`

6. Copy the following files to the `/var/tmp/Analytics/` directory:

- `fmw_12.2.1.3.0_wls_Disk1_1of1.zip`

7. Make the following changes to the `/var/tmp/Analytics/parameters.conf` file:

```
#### SYSTEM common settings ####
DOMAIN=domain.com           #CHANGE THIS TO THE DOMAIN NAME ONLY I.E
DOMAIN.COM
NTP_HOST=localhost          #CHANGE THIS TO THE NTP IP OR HOSTNAME
JAVA_HOME=/usr/java/latest  #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION

#### WLS Parameters ####
WLS_HOSTNAME=localhost      #CHANGE THIS TO THE HOSTNAME ONLY (NOT THE FQDN)
WLS_HOST_IP_ADDR=127.0.0.1  #CHANGE THIS TO THE IP OF YOUR SERVER
WLS_NAMESERVER=192.168.1.1  #CHANGE THIS TO THE IP/HOSTNAME OF YOUR DNS
SERVER
BASE_DOMAIN=base_domain    #CHANGE THIS TO THE YOUR DOMAIN NAME

#### Domain Creation Parameters (Python) ###

#Server Settings
SERVER1_ADDRESS=127.0.0.1    #CHANGE THIS TO THE IP OF YOUR SERVER

#Properties for AdminServer
ADMIN_LISTEN_ADDRESS=127.0.0.1 #CHANGE THIS TO THE IP OF YOUR SERVER
ADMIN_LISTEN_PORT=7001        #CHANGE THIS TO THE PORT THAT YOU NEED WLS TO
LISTEN

#Properties for enabling creation of managed domain for JMS (on standalone WLS)
MANAGED_DOMAIN_ENABLED=true
MANAGED_LISTEN_PORT=7003
```

8. If you want to change the default WLS console user, make the following changes to the `/var/tmp/Analytics/wls/source/environment.properties` file:

```
adminUser=weblogic          #CHANGE TO THE WLS WEBLOGIC CONSOLE USER
```

*** Note:**

The system prompts you for the `soaRepositoryStbPwd` database schema password during the installation. Therefore, ensure that you make a note of the value that you configured in the `environment.properties` file.

9. From the `/var/tmp/Analytics/wls` directory, run the following command as the root user:

```
sh root.sh
```

10. Review the output of the script and ensure that no errors have occurred during the configuration process. If you find any errors, correct the errors and re-run the command.
11. Reboot the Avaya Analytics™ Streams server.

12. After the Avaya Analytics™ Streams server starts, log in to the server as the root user.

Use the `hostname` command to verify that the correct hostname of the server is set.

13. Run the following commands to change the permission and owner of all installation files to the Oracle user configured during the Oracle® Database installation:

- `chmod 755 -Rf /var/tmp/Analytics/*`
- `chown -Rf oracle:oinstall /var/tmp/Analytics/*`

14. From the `/var/tmp/Analytics/wls` directory, run the following command as the root user to begin the installation process:

```
sh oracle_wls_install.sh
```

During the installation, the system prompts you to confirm that you have edited the `parameters.conf` file, and to enter the password for the WLS admin user.

15. After the installation process, verify that the WebLogic Admin server is started by browsing to the weblogic console at `http://<IP address>:7001/console`.

If the WebLogic Admin server is not started, review the output of the script, and ensure that no errors have occurred during the installation process.

16. Verify that in the `/home/oracle` directory the following folders are present:

- `oralInventory`
- `WLS_HOME`

Installing Oracle® Stream Analytics

About this task

Install Oracle® Stream Analytics on a Red Hat Enterprise Linux (RHEL) server, for use with Avaya Analytics™. For OSA High Availability (HA) deployments, install Oracle® Stream Analytics on two separate RHEL servers. The install procedure is the same for both HA servers.

The following table lists the requirements for Oracle® Stream Analytics:

Requirement	Description
Java	jdk1.8.x.x.x
OSA installation scripts	osa.zip
Oracle® Stream Analytics software	ofm_integration_osa_12.2.1.0.0_disk1.zip

Procedure

1. Unzip the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.

The `osa.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `osa.zip` file to the OSA server using an scp or ftp tool.

3. SSH to the OSA server as the root user.
4. Create the `/var/tmp/Analytics/` directory.
5. Run the following command to unzip the `osa.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics osa.zip
```

Example of the directory structure contents:

- `/var/tmp/Analytics/parameters.conf`

6. Copy the following files to the `/var/tmp/Analytics/` directory:

- `ofm_integration_osa_12.2.1.0.0_disk1.zip`

7. Make the following changes to the `/var/tmp/Analytics/parameters.conf` file:

```
DOMAIN=domain.com           #CHANGE THIS TO THE DOMAIN NAME ONLY I.E DOMAIN.COM
NTP_HOST=localhost          #CHANGE THIS TO THE NTP IP OR HOSTNAME
JAVA_HOME=/usr/java/latest  #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION

#### OSA Parameters ####
OSA_HOSTNAME=localhost      #CHANGE THIS TO THE HOSTNAME
ONLY (NOT THE FQDN)
OSA_HOST_IP_ADDR=127.0.0.1  #CHANGE THIS TO THE IP OF YOUR
SERVER                     #CHANGE THIS TO THE IP/HOSTNAME
OSA_NAMESERVER=localhost    #CHANGE THIS TO THE IP/HOSTNAME
OF YOUR DNS SERVER
```

8. **(Optional)** To change the Oracle_Home location, update the related response files located in the `/var/tmp/Analytics/osa/source` directory.
9. From the `/var/tmp/Analytics/osa/` directory, make the following script executable and run the following command as the root user:

```
sh root.sh
```

When prompted to enter the password for the Oracle user: "Enter password for oracle:", enter the password.

10. After the script completes, review the output of the script to ensure that no errors occurred during the configuration process. If you find any errors, correct the errors and re-run the script.
11. Reboot the server.
12. After the restart, SSH to the server as the root user. If it is not possible to SSH to the server as root, you must connect as a standard user and switch to the root user after connecting.
13. Ensure that the hostname of the server is set correctly using the `hostname` command.
14. Run the following command as the root user:

```
chmod 755 -Rf /var/tmp/Analytics/*
```

```
chown -Rf oracle:oinstall /var/tmp/Analytics/*
```

15. From the `/var/tmp/Analytics/osa` directory, run the following command as the root user:

```
sh oracle_osa_install.sh
```

The system prompts you to enter passwords during the installation.

16. Review the output of the script and ensure that no failures or errors have occurred during the installation process.
17. After a successful install, run the following commands as the Oracle user:

```
cd $MW_HOME/user_projects/domains/osadomain/osaserver/
nohup ./startwlevs.sh > /dev/null &
```

Post installation checks for Oracle® Stream Analytics

About this task

Perform the following post installation checks for Oracle® Stream Analytics. This procedure describes checks to perform after the install.

Procedure

Ensure that you can log in to the following web interface:

- Log in to Oracle Event Processing Visualizer as the wlevs user. The default username and password are `wlevs` and `Admin123`. Navigate to the following URL using your web browser:
`http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/`

If the web interface is accessible, continue with the Avaya Analytics™ install.

Installing Oracle patches

About this task

This procedure describes how to install Oracle patches using OPatch. You can use this procedure to install patches for all Oracle components.

Use this procedure if you need to manually install patches that were not available at the time you installed Avaya Analytics™ software. Avaya Analytics™ supports install-time patching.

The Avaya Analytics™ Release Notes contain the known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Analytics™. Read the Release Notes for the most recent instructions before you install patches.

Important:

Ensure that you use the Oracle user account when performing this procedure.

Procedure

1. Run the following script to set the environment variables:

```
ORACLE_HOME/user_projects/domains/your_domain_name/bin/
setDomainEnv.sh
```

2. Run the following command to view currently installed patches:

```
./opatch lsinventory
```

3. Create a patch folder and copy the patch zip file to the new folder. Run the following command:

```
unzip patch_file.zip
```

This command creates a new folder, with the name of the folder matching the patch number, for example 123456.

4. Run the following command to navigate to the created folder:

```
cd 123456
```

5. Run the following command:

```
ORACLE_HOME/OPatch/opatch apply
```

6. Type `Y` in response to all prompts.

OPatch checks if there are any conflicting patches, creates a backup of the old configuration for roll back, and applies the patch.

The system displays the "OPatch succeeded" message.

 Note:

To apply another patch, you must change the folder to the next patch directory created when unzipping. OPatch fails if you try to apply a patch from an incorrect folder.

To apply multiple patches at the same time, you must unzip all patches so that each path has a directory, and run the following command:

```
ORACLE_HOME/OPatch/opatch napply -id 123456,789012,345678,901234
```

Deploying Avaya Analytics™ for Oracle® Database

Pre-installation checks for Oracle® Database

About this task

Perform the following steps before installing Avaya Analytics™ for Oracle® Database. Refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Procedure

1. Log in as the Oracle user.
2. Copy the `AvayaAnalytics_x.x.x.zip` file to the target machine at any location.
3. Run the following command to unzip the deployment file:

```
unzip -d /var/tmp/Analytics/install AvayaAnalytics_x.x.x.zip
```

4. Copy the patch to `/var/tmp/Analytics/install` folder.
5. Run the following command:

```
chown -Rf oracle:oinstall
```

6. Configure the ORACLE DATABASE SECTION of the `parameters.conf` file for relevant paths and credentials. If you used default location settings during Oracle software installation, no changes in the location paths are required.

! Important:

- For solutions using Oracle® RAC Database, configure `DB_HOST` to use the SCAN.
- If you are deploying a Single Instance of Oracle® Database and you want to automatically install Oracle patches during the install, you must ensure the following line is not commented out:
#`DB_PATCH_FILE_NAME=OracleDatabasePatchesXXXX.zip`. Do not perform this step if you are installing Oracle® Database in a RAC or Data Guard configuration.

```
#####
#### ORACLE DATABASE SECTION ####
#####
#### Directory where Oracle Database 12c "database home" is located ####
DB_HOME="/home/oracle/app/oracle/product/12.1.0/dbhome_1"
#### Directory where Oracle Database 12c "Oracle Home" is installed ####
DB_ORACLE_HOME="/home/oracle/app/oracle"
#### Database Credentials ####
DB_USER="sys"
DB_HOST="192.168.1.10"
DB_SID="orcl"
```

7. Copy the Oracle® Database patches zip file to the same location as the unzipped `AvayaAnalytics_x.x.x.zip` file.

Installing Avaya Analytics™ for Oracle® Database

About this task

Use the following procedure to install Avaya Analytics™ for Oracle® Database.

! Important:

For solutions using Oracle® RAC Database, you must install Avaya Analytics™ for Oracle® Database on Node 1 only.

For solutions using Oracle® Dataguard, you must install Avaya Analytics™ for Oracle® Database on the Primary server only.

Procedure

1. Perform the following steps to configure auto-start of services:
 - a. Change to the root user using the following command:


```
sudo su -
```
 - b. Go to the directory where you unzipped the deployment scripts.
 - c. Run the following commands to set the correct permissions for the installation scripts:
 - `chown -Rf oracle:oinstall`
 - `chmod ug+w`
 - `chmod ug+x *.sh`
2. Perform the following steps as the Oracle user to configure Oracle Database Schemas:
 - a. Run the following command:


```
./installAvaya.sh
```
 - b. When the system prompts you with the `Please confirm that you have edited the parameters.conf file by entering y to continue message`, type `y`.
If you type any other string, the process is cancelled.
 - c. To install Oracle® Database from the choice of components available, type `DB` at the prompt.
 - d. To accept the End User License Agreement, type `y`.
 - e. Enter the password that is to be used as the SYS user password at the prompt.
 - f. Enter a user name for read-only access when prompted.
 - g. Enter a password for read-only access when prompted.
 - h. Enter the root password when prompted during the analytics service install.
 - i. After the installation completes, verify that the system creates the `install_db.log` and `install_db_patches.log` file in the folder containing the installer. This file contains the installation logs for Oracle® Database.
The analytics service comes into effect after the server is rebooted. You can also use the following commands to stop and start services manually:
 - `systemctl stop analytics.service`
 - `systemctl start analytics.service`

! Important:

The analytics.service applies to standalone Oracle® Database only. Do not run these commands if your solution includes Oracle® RAC Database.

Next steps

Verify patches installed successfully. Navigate to the `/home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch` directory and run the following command as the Oracle user:

```
./opatch lsinventory
```

Verify that the list of installed patches matches the list in the patch list file contained in the patch folder. There can be additional patches listed after running this command; these patches are part of the base Oracle installation.

Deploying Avaya Analytics™ for Oracle® Business Intelligence and Oracle® Data Integrator

Pre-installation checks for Oracle® Business Intelligence and Oracle® Data Integrator

About this task

Perform the steps mentioned in this procedure before installing Oracle® Business Intelligence and Oracle® Data Integrator. Refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Procedure

1. Copy the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file to the target machine at any location.
2. Log in as the Oracle user. Ensure you use the same Oracle user that installed the Oracle® software.

! Important:

Do not log in as a root user to install Oracle software. If you have logged in as an Oracle user, do not log in as root to troubleshoot issues related to Oracle user login. The root user login must be used for Operating System-specific tasks such as changing or setting kernel parameters.

3. Run the following command from the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` location to verify that all components have a status of RUNNING:

```
./status.sh
```

- Run the following command to unzip the deployment file:

```
unzip AvayaAnalytics_x.x.x.x_Build_xx.zip
```

- Configure the ORACLE BUSINESS INTELLIGENCE SECTION and ORACLE DATA INTEGRATOR SECTION of the `parameters.conf` file for relevant paths and credentials. The parameters that require changes are emphasized in the example below. If you changed the ORACLE_HOME location during install, you must also change the OBI_HOME and OBI_SERV_INST_LOC parameters to match the new path.

! Important:

For solutions using Oracle® RAC Database, configure OBI_SHARED_DB_HOST and ODI_DB_HOST to use the SCAN.

```
#####
#### ORACLE DATA INTEGRATOR SECTION ####
#####

#### Directory where ODI Weblogic domain is located ####
ODI_DOMAIN_HOME="/home/oracle/app/oracle/Oracle_Home_ODI_Standalone/user_projects/
domains/odistandaloneagent"
ODI_HOST="127.0.0.1"
ODI_PORT="20910"

#### Oracle Home for ODI ####
ODI_ORACLE_HOME="/home/oracle/app/oracle/Oracle_Home_ODI_Standalone"

#### ODI Agent Name/Instance and password ####
ODI_AGENT="OracleDIAgent1"

#### ODI Work Repository Name ####
ODI_WORKREP_NAME="WORKREP"

#### ODI_DB_Credentials ####
ODI_DB_HOST="127.0.0.1"
ODI_DB_PORT="1521"
ODI_DB_SID="orcl" when installing Avaya OBIEE software
ODI_DB_SID="orclrcu" when installing Oracle OBIEE software
ODI_DB_SID="orcl_stby" when installing or patch update of Avaya ODI software

ODI_DB_SID="orcl" .
ODI_DB_SCHEMA_PREFIX="ODI"

#####
#### ORACLE BUSINESS INTELLIGENCE SECTION ####
#####

#### Directory where OBIEE 12c is installed ####
OBI_HOME="/home/oracle/Oracle/Middleware/Oracle_Home"
OBI_HOST="127.0.0.1"
OBI_PORT="9502"

#### OBIEE Service Instance Location, normally the Weblogic domain that OBIEE is
using ####
OBI_SERV_INST_LOC="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/
domains/bi"

#### OBIEE Service Instance Name, default install uses ssi ####
OBI_SERV_INST_NAME="ssi"
```

```
#### OBIEE Credentials ####
OBI_USER="weblogic"

#### OBIEE Credentials and host information for rpd connection pool shared DB
user, do not edit the DB username or password ####
OBI_SHARED_DB_HOST="127.0.0.1"
OBI_SHARED_DB_SID="orcl"
ODI_DB_SID="orcl" when installing Avaya OBIEE software
ODI_DB_SID="orclrcu" when installing Oracle OBIEE software
ODI_DB_SID="orcl_stby" when installing or patch update of Avaya ODI software

OBI_SHARED_DB_PORT="1521"
```

6. Edit the following parameters in the AGENT_OracleDIAgent1.xml file:

```
<Field name="HostName" type="java.lang.String"><![CDATA[127.0.0.1]]></
Field>      #UPDATE THE IP ADDRESS TO USE THE ODI SERVER IP ADDRESS
```

7. Copy the Oracle® Business Intelligence patches zip file and the Oracle® Data Integrator patches zip file to the same location as the unzipped AvayaAnalytics_x.x.x.zip file.

Installing Avaya Analytics™ for Oracle® Business Intelligence and Oracle® Data Integrator

About this task

Use the following procedure to install Avaya Analytics™ for Oracle® Business Intelligence and Oracle® Data Integrator. The Avaya install script for OBIEE installs both OBI and ODI at the same time.

Procedure

1. Perform the following steps to configure auto-start of services:
 - a. Change to the root user using the following command:


```
sudo su -
```
 - b. Go to the directory where you unzipped the deployment scripts.
 - c. Run the following commands to set the correct permissions for the installation scripts:
 - `chown -Rf oracle:oinstall`
 - `chmod ug+w`
 - `chmod ug+x *.sh`
2. Make the script executable and run the following command as an Oracle user:


```
./installAvaya.sh
```
3. When the system prompts you with the Please confirm that you have edited the parameters.conf file by entering y to continue message, type y.
If you type any other string, the process is cancelled.
4. To install both OBI and ODI from the available components, type OBIEE at the prompt.

5. To accept the End User License Agreement, type `y`.
6. When prompted for the component to install, type `ALL` at the prompt. This installs both OBI and ODI.
7. Enter the password for the weblogic user on the OBIEE machine at the prompt.
8. Enter the password for the database SYS user at the prompt.
9. Enter the root password when prompted during the analytics service install.
10. After the installation completes, verify that the system creates the `install_obi.log`, `install_odi.log`, `install_obiee.patches.log` and `install_odi_patches.log` file in the folder containing the installer. These files contain the installation logs for Oracle® Business Intelligence and Oracle® Data Integrator. Ignore the following expected exceptions in the `install_odi.log` file:
 - `oracle.odi.oditools.OdiToolException`
 - `javax.persistence.RollbackException`

The analytics service comes into effect after the server is rebooted. You can also use the following commands to stop and start services manually:

- `systemctl stop analytics.service`
- `systemctl start analytics.service`

Next steps

Verify patches installed successfully. Navigate to the `Middleware/Oracle_Home/OPatch` directory and run the following command as the Oracle user:

```
./opatch lsinventory
```

Verify that the list of installed patches matches the list in the patch list file contained in the patch folder. There can be additional patches listed after running this command; these patches are part of the base Oracle installation.

Post installation steps for Oracle® Business Intelligence and Data Integrator

Configuring a secure connection to the OBIEE web interfaces

About this task

This procedure describes a generic method for creating identity certificates to secure the connection to the OBIEE web interfaces.

Important:

Run all commands for this procedure as the Oracle user, unless otherwise stated.

Before you begin

If you are using a third-party Certificate Authority, obtain a third-party root CA certificate.

Procedure

1. On the OBI server, create a directory for the certificates you are going to create. For example, run the following command to create a directory:

```
mkdir -p /home/oracle/SSL/
```

```
cd /home/oracle/SSL/
```

2. Run the following command from the newly created directory to generate a key pair, and type the correct information for your solution:

```
keytool -genkeypair -alias obiee -keyalg RSA -keysize 2048 -  
keystore obi.jks -validity 3650
```

The following is an example of the information passed:

```
Enter keystore password: password
What is your first and last name?
  [Unknown]: WFOBIEE4284V.wf.aura.com
What is the name of your organizational unit?
  [Unknown]: Analytics
What is the name of your organization?
  [Unknown]: AVAYA
What is the name of your City or Locality?
  [Unknown]: GALWAY
What is the name of your State or Province?
  [Unknown]: GALWAY
What is the two-letter country code for this unit?
  [Unknown]: IE
Is CN=WFOBIEE4284V.wf.aura.com, OU=Analytics, O=AVAYA,
L=GALWAY, ST=GALWAY, C=IE correct?
  [no]: yes
Enter key password for <obiee>
      (RETURN if same as keystore password):
Re-enter new password:
```

3. Run the following command to generate a Certificate Signing Request (CSR):

```
keytool -certreq -v -alias obiee -keyalg RSA -sigalg SHA256withRSA  
-file obi.csr -keystore obi.jks -storepass Admin123
```

4. Ensure that two files now exist in the new directory. The `obi.csr` file must be signed by a Certificate Authority (CA), the following example uses SMGR as a CA. If you are not using SMGR as a CA, skip to step 9 and use a third-party root CA certificate instead of `SystemManagerCA.pem`.

5. Perform the following steps to add an End Entity on System Manager.

- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
- b. In the left pane, under **RA Functions**, click **Add End Entity**.
- c. From the **End Entity Profile** list, select **EXTERNAL_CSR_PROFILE**.
- d. In the **Username** field, type a user name.

You must note this user name, as it is required to create a certificate from the CSR.

- e. In the **Password (or Enrollment Code)** field, type a password.

You must note this password, as it is required to create a certificate from the CSR.

- f. In the **Confirm Password** field, re-enter the password.
- g. In the **CN, Common name** field, type the FQDN of the OBI server.

 Note:

This must match the CN entered when generating the CSR.

- h. In the **Organization, Country, Organizational Unit, Locality**, and **State or Province** fields, type the same values you entered when creating the CSR.
 - i. Under **Subject Alternative Name**, in the first **DNS Name** field, type the host name of the OBI server.
 - j. Under **Subject Alternative Name**, in the second **DNS Name** field, type the FQDN of the OBI server.
 - k. Click **Add**.
6. Perform the following steps to sign the CSR file on System Manager.
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the left pane, click **Public Web**.
 - c. Click **Create Certificate from CSR**.
 - d. In the **Username** field, type the same user name you entered when adding an End Entity.
 - e. In the **Enrollment Code** field, type the same password you entered when adding an End Entity.
 - f. Copy the contents of the CSR created previously on the OBI server into the text box.
 - g. Click **OK**.
 - h. Download the new certificate as a PEM file. The file is saved as `<OBI server name>.pem`
 7. Click **Fetch CA Certificates**.
 8. Click **Download as PEM**. The file is saved as `SystemManagerCA.pem`
 9. Copy `<OBI server name>.pem` and `SystemManagerCA.pem` files to the `/home/oracle/SSL/` directory.
 10. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to import the root CA certificate into the `obi.jks` keystore:


```
keytool -import -trustcacerts -alias smgrca -file
SystemManagerCA.pem -keystore obi.jks -keypass changeit -storepass
Admin123
```
 11. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to import the signed certificate into the `obi.jks` keystore:

```
keytool -import -trustcacerts -alias obiee -file <OBI server
name>.pem -keystore obi.jks -keypass Admin123 -storepass Admin123
```

12. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to convert the JKS to p12:

```
keytool -importkeystore -srckeystore obi.jks -destkeystore obi.p12
-deststoretype pkcs12
```

13. As the root user, convert the SMGR .PEM file to a .DER file using the following command:

```
openssl x509 -outform der -in SystemManagerCA.pem -out
SystemManagerCA.der
```

14. As the root user, back up the cacerts using the following command:

```
cp /usr/java/latest/jre/lib/security/cacerts /usr/java/
latest/jre/lib/security/cacerts.orig
```

*** Note:**

The location of the cacerts folder can differ from this example.

15. As the root user, import the SMGR .DER file into the cacerts directory using the following command:

```
keytool -import -alias smgrca -keystore /usr/java/latest/jre/lib/
security/cacerts -file SystemManagerCA.der
```

*** Note:**

The default password for cacerts is `changeit`. The location of the cacerts folder can differ from this example.

16. On the OBI server configure nodemanager to use SSL by adding the following lines to the `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/nodemanager/nodemanager.properties` file:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=/home/oracle/SSL/obi.jks
CustomIdentityAlias=obiee
CustomIdentityPrivateKeyPassPhrase=Admin123
CustomTrustKeyStoreFileName=/home/oracle/SSL/obi.jks
```

17. On the OBI server, edit the `ORACLE_HOME/user_projects/domains/bi/bitools/bin/start.sh` file and add the lines highlighted below:

```
start.sh

#!/bin/sh

# WARNING: This file is created by the Configuration Wizard.
# Any changes to this script may be lost when adding extensions to this
configuration.

DOMAIN_HOME="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi"
export DOMAIN_HOME

export WLST_PROPERTIES="-Dweblogic.security.SSL.TrustedCAKeyStore=/home/"
```

```

oracle/SSL/obi.jks"
export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true $
{WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust $
{WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreFileName=/home/
oracle/SSL/obi.jks ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-
Dweblogic.security.CustomTrustKeyStorePassPhrase=Admin123 ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreType=JKS $
{WLST_PROPERTIES}"

/home/oracle/Oracle/Middleware/Oracle_Home/bi/modules/oracle.bi.sysman/scripts/
start.sh "$@"

```

18. On the OBI server, edit the `ORACLE_HOME/user_projects/domains/bi/bitools/bin/stop.sh` file and add the lines highlighted below:

```

stop.sh

#!/bin/sh

# WARNING: This file is created by the Configuration Wizard.
# Any changes to this script may be lost when adding extensions to this
configuration.

DOMAIN_HOME="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi"
export DOMAIN_HOME

export WLST_PROPERTIES="-Dweblogic.security.SSL.TrustedCAKeyStore=/home/
oracle/SSL/obi.jks"
export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true $
{WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust $
{WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreFileName=/home/
oracle/SSL/obi.jks ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-
Dweblogic.security.CustomTrustKeyStorePassPhrase=Admin123 ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreType=JKS $
{WLST_PROPERTIES}"

/home/oracle/Oracle/Middleware/Oracle_Home/bi/modules/oracle.bi.sysman/scripts/
stop.sh "$@"

```

19. In your web browser, open the following URL to start Weblogic Console: `http://<OBI_SERVER_IP>:9500/console`
20. In the left pane, navigate to **Environment > Servers > bi_server1**.
21. Select the **Keystores** tab.
22. Under **Identity**, in the **Custom Identity Keystore** field, type the path to the location of the identity keystore.
23. In the **Custom Identity Keystore Type** field, type `JKS`.
24. In the **Custom Identity Keystore Passphrase** field, type the password for the identity keystore.
25. Confirm the password.

26. Under **Trust**, in the **Custom Trust Keystore** field, type the path to the location of the trusted CA keystore.
27. In the **Custom Trust Keystore Type** field, type `JKS`.
28. In the **Custom Trust Keystore Passphrase** field, type the password for the trusted CA keystore.
29. Confirm the password.
30. Click **Save**.
31. Select the **SSL** tab.
32. Under **Identity**, in the **Private Key Alias** field, type the alias for the identity keystore. For example, type `obiee`.
33. In the **Private Key Passphrase** field, type the password for the identity keystore.
34. Confirm the password.
35. Click **Save**.
36. Select the **General** tab.
37. Select the **SSL Listen Port Enabled** check box.

 Important:

Ensure that the configured **SSL Listen Port** is available and not in use.

38. Restart the OBI server.

User group usage and data access control limitations

In this release of Avaya Analytics™, you can either use the Administration user for reporting or configure a reporting user.

- If you use the Administration user, you must not configure reporting users or assign them to reporting groups. Configuring multiple reporting user or groups results in the historical reports showing incorrect data.
- If you configure reporting users for data access control, you cannot use the Administration user for reporting. Multiple reporting users and multiple user groups are supported.

Applying the Avaya branding to the OBIEE interface

Procedure

1. Shut down the OBI server. From the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` directory, run the following command as the Oracle user:

`./stop.sh`
2. Copy the `bicustom.ear` file from the Deployments zip file to the following directory:

`ORACLE_HOME/user_projects/domains/bi/bidata/components/OBIPS`

3. Start the OBI server. From the the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` directory, run the following command as the Oracle user:
`./start.sh`
4. In your web browser, open the following URL to start Weblogic Console:
`http://<OBI_SERVER_IP>:9500/console`
5. Log in to Weblogic Console using your login credentials.
6. In the navigation pane, click **Environment > Servers**.
7. From the Control tab, shut down the OBI server.
8. In the navigation pane, click **Deployments > Lock and Edit**.
 If you find an existing bicustom application in the content pane, you must remove it.
9. Click **Install**.
10. Select the `bicustom.ear` file that you copied.
11. Select the **Install this deployment as an application** option.
12. Select `bi_cluster` as the target.
13. Click **Next** and select the **I will make the deployment accessible from the following location** option.
14. Click **Next** and **Finish**.
15. Confirm changes on Weblogic console in **Change Center** on top left hand side of console by clicking **Activate Changes**.
16. From the Control tab, select the check box next to the bicustom application, and then click **Start > Servicing All Requests**.
17. Shut down the OBI server. From the the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` directory, run the following command as the Oracle user:
`./stop.sh`
18. Start the OBI server. From the the `ORACLE_HOME/user_projects/domains/bi/bitools/bin` directory, run the following command as the Oracle user:
`./start.sh`

Post installation checks for Oracle® Business Intelligence and Oracle® Data Integrator

Procedure

1. From the `$ORACLE_HOME/user_projects/domains/bi/bitools/bin` directory, run the `status.sh` script.

2. Ensure that all OBI services are in a RUNNING state and that all operations completed successfully.
3. In your web browser, enter the following URL to access OBI analytics: `http://<obi server name>:9502/analytics`. Ensure that Avaya Dashboards and subject areas to report against appear.
4. You can run the following command to verify if ODI Agent is running:

```
$ODI_DOMAIN_HOME/bin/startcmd.sh "-INSTANCE=OracleDIAgent1"
OdiPingAgent "-AGENT_NAME=OracleDIAgent1"
```

If ODI Agent is not running, an error is returned. See the following successful and failed examples of the output returned after running this command.

```
*****
*****
SUCCESSFUL:
*****
*****
2018-04-04 14:00:39.715 NOTIFICATION New data source: [ODI_ODI_REPO/
*****@jdbc:oracle:thin:@//<DB_IP_ADDRESS>:1521/ORCL]
2018-04-04 14:00:40.832 NOTIFICATION Created OdiInstance instance id=1
2018-04-04 14:00:41.591 NOTIFICATION Successfully set the current thread
authentication
2018-04-04 14:00:41.598 NOTIFICATION New data source: [ODI_ODI_REPO/
*****@jdbc:oracle:thin:@//<DB_IP_ADDRESS>:1521/ORCL]
2018-04-04 14:00:41.725 NOTIFICATION New data source: [ODI_ODI_REPO/
*****@jdbc:oracle:thin:@(description=(address=(host=<DB_IP_ADDRESS>)
(protocol=tcp)(port=1521))(connect_data=(service_name=ORCL)(server=dedicated)))]
2018-04-04 14:00:41.779 NOTIFICATION Created OdiInstance instance id=2
2018-04-04 14:00:41.798 NOTIFICATION Successfully set the current thread
authentication
*****
*****
FAILURE:
*****
*****
2018-04-04 14:18:04.890 ERROR Executing: OdiPingAgent "-AGENT_NAME=OracleDIAgent1"
java.lang.RuntimeException: oracle.odi.oditools.OdiToolException: Error while
running ODI Tool OdiPingAgent
    at oracle.odi.oditools.OdiAbstractToolRunner
$3.doAction(OdiAbstractToolRunner.java:238)
    at
oracle.odi.core.persistence.dwgobject.DwgObjectTemplate.execute(DwgObjectTemplate.
java:203)
    at
oracle.odi.oditools.OdiAbstractToolRunner.executeConnectedCoreTool(OdiAbstractTool
Runner.java:228)
    at
oracle.odi.oditools.OdiAbstractToolRunner.executeCoreTool(OdiAbstractToolRunner.ja
va:133)
    at
oracle.odi.oditools.OdiAbstractToolRunner.executeTool(OdiAbstractToolRunner.java:
51)
    at oracle.odi.ToolRunner.main(ToolRunner.java:85)
Caused by: oracle.odi.oditools.OdiToolException: Error while running ODI Tool
OdiPingAgent
    at
oracle.odi.oditools.OdiAbstractToolRunner.executeTool(OdiAbstractToolRunner.java:
194)
```

```

at oracle.odi.oditools.OdiAbstractToolRunner.access
$000(OdiAbstractToolRunner.java:28)
at oracle.odi.oditools.OdiAbstractToolRunner
$3.doAction(OdiAbstractToolRunner.java:236)
... 5 more
Caused by: com.sunopsis.dwg.function.SnpsFunctionBaseException: ODI-30004: Agent
unreachable
at com.sunopsis.dwg.tools.PingAgent.actionExecute(PingAgent.java:75)
at
com.sunopsis.dwg.function.SnpsFunctionBaseRepositoryConnected.execute(SnpsFunction
BaseRepositoryConnected.java:219)
at
oracle.odi.oditools.OdiAbstractToolRunner.executeTool(OdiAbstractToolRunner.java:
190)
... 7 more

```

Configuring SSL for OBIEE weblogic server

About this task

Use this procedure to configure SSL for OBIEE weblogic server.

! Important:

Run all commands for this procedure as the Oracle user, unless otherwise stated.

Before you begin

If you are using a third-party Certificate Authority, obtain a third-party root CA certificate.

Procedure

1. On the OBI server, create a directory for the certificates you are going to create. For example, run the following command to create a directory:

```

mkdir -p /home/oracle/SSL/
cd /home/oracle/SSL/

```

2. Run the following command from the newly created directory to generate a key pair, and type the correct information for your solution:

```

keytool -genkeypair -alias obiee -keyalg RSA -keysize 2048 -
keystore obi.jks -validity 3650

```

The following is an example of the information passed:

```

Enter keystore password: password
What is your first and last name?
[Unknown]: WFOBIEE4284V.wf.aura.com
What is the name of your organizational unit?
[Unknown]: Analytics
What is the name of your organization?
[Unknown]: AVAYA
What is the name of your City or Locality?
[Unknown]: GALWAY
What is the name of your State or Province?
[Unknown]: GALWAY
What is the two-letter country code for this unit?

```

```
[Unknown]: IE
Is CN=WFOBIEE4284V.wf.aura.com, OU=Analytics, O=AVAYA,
L=GALWAY, ST=GALWAY, C=IE correct?
[no]: yes
Enter key password for <obiee>
(RETURN if same as keystore password):
Re-enter new password:
```

3. Run the following command to generate a Certificate Signing Request (CSR):

```
keytool -certreq -v -alias obiee -keyalg RSA -sigalg SHA256withRSA
-file obi.csr -keystore obi.jks -storepass Admin123
```

4. Ensure that 2 files now exist in the new directory. The `obi.csr` file must be signed by a Certificate Authority (CA), the following example uses SMGR as a CA. If you are not using SMGR as a CA, skip to step 9 and use a third-party root CA certificate instead of `SystemManagerCA.pem`.
5. Perform the following steps to add an End Entity on System Manager.

- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
- b. In the left pane, under **RA Functions**, click **Add End Entity**.
- c. From the **End Entity Profile** list, select **EXTERNAL_CSR_PROFILE**.
- d. In the **Username** field, type a user name.

You must note this user name, as it is required to create a certificate from the CSR.

- e. In the **Password (or Enrollment Code)** field, type a password.
- f. In the **Confirm Password** field, re-enter the password.
- g. In the **CN, Common name** field, type the FQDN of the OBI server.

 Note:

This must match the CN entered when generating the CSR.

- h. In the **Organization, Country, Organizational Unit, Locality, and State or Province** fields, type the same values you entered when creating the CSR.
- i. Under **Subject Alternative Name**, in the first **DNS Name** field, type the hostname of the OBI server.
- j. Under **Subject Alternative Name**, in the second **DNS Name** field, type the FQDN of the OBI server.
- k. Click **Add**.
6. Perform the following steps to sign the CSR file on System Manager.
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the left pane, click **Public Web**.

- c. Click **Create Certificate from CSR**.
 - d. In the **Username** field, type the same user name you entered when adding an End Entity.
 - e. In the **Enrollment Code** field, type the same password you entered when adding an End Entity.
 - f. Copy the contents of the CSR created previously on the OBI server into the text box.
 - g. Click **OK**.
 - h. Download the new certificate as a PEM file. The file is saved as <OBI server name>.pem
7. Click **Fetch CA Certificates**.
 8. Click **Download as PEM**. The file is saved as SystemManagerCA.pem
 9. Copy <OBI server name>.pem and SystemManagerCA.pem files to the /home/oracle/SSL/ directory in the OBI server.
 10. On the OBI server, run the following command from the /home/oracle/SSL/ directory to import the root CA certificate into the obi.jks keystore:


```
keytool -import -trustcacerts -alias smgrca -file
SystemManagerCA.pem -keystore obi.jks -keypass changeit -storepass
Admin123
```
 11. On the OBI server, run the following command from the /home/oracle/SSL/ directory to import the signed certificate into the obi.jks keystore:


```
keytool -import -trustcacerts -alias obiee -file <OBI server
name>.pem -keystore obi.jks -keypass Admin123 -storepass Admin123
```
 12. On the OBI server, run the following command from the /home/oracle/SSL/ directory to convert the JKS to p12:


```
keytool -importkeystore -srckeystore obi.jks -destkeystore obi.p12
-deststoretype pkcs12
```
 13. As the root user, convert the SMGR .PEM file to a .DER file using the following command:


```
openssl x509 -outform der -in SystemManagerCA.pem -out
SystemManagerCA.der
```
 14. As the root user, back up the cacerts using the following command:


```
cp /usr/java/latest/jre/lib/security/cacerts /usr/java/
latest/jre/lib/security/cacerts.orig
```

 **Note:**

The location of the cacerts folder can differ from this example.
 15. As the root user, import the SMGR .DER file into the cacerts directory using the following command:

```
keytool -import -alias smgrca -keystore /usr/java/latest/jre/lib/
security/cacerts -file SystemManagerCA.der
```

 Note:

The default password for cacerts is `changeit`. The location of the cacerts folder can differ from this example.

16. On the OBI server configure nodemanager to use SSL by adding the following lines to the `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/nodemanager/nodemanager.properties` file:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=/home/oracle/SSL/obi.jks
CustomIdentityAlias=obiee
CustomIdentityPrivateKeyPassPhrase=Admin123
CustomTrustKeyStoreFileName=/home/oracle/SSL/obi.jks
```

17. On the OBI server, edit the `ORACLE_HOME/user_projects/domains/bi/bitools/bin/start.sh` file and add the lines highlighted below:

```
start.sh

#!/bin/sh

# WARNING: This file is created by the Configuration Wizard.
# Any changes to this script may be lost when adding extensions to this
configuration.

DOMAIN_HOME="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi"
export DOMAIN_HOME

export WLST_PROPERTIES="-Dweblogic.security.SSL.TrustedCAKeyStore=/home/
oracle/SSL/obi.jks"
export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true $
${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust $
${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreFileName=/home/
oracle/SSL/obi.jks ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-
Dweblogic.security.CustomTrustKeyStorePassPhrase=Admin123 ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreType=JKS $
${WLST_PROPERTIES}"

/home/oracle/Oracle/Middleware/Oracle_Home/bi/modules/oracle.bi.sysman/scripts/
start.sh "$@"
```

18. On the OBI server, edit the `ORACLE_HOME/user_projects/domains/bi/bitools/bin/stop.sh` file and add the lines highlighted below:

```
stop.sh

#!/bin/sh

# WARNING: This file is created by the Configuration Wizard.
# Any changes to this script may be lost when adding extensions to this
configuration.

DOMAIN_HOME="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/bi"
export DOMAIN_HOME
```

```

export WLST_PROPERTIES="-Dweblogic.security.SSL.TrustedCAKeyStore=/home/
oracle/SSL/obi.jks"
export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true $
${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust $
${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreFileName=/home/
oracle/SSL/obi.jks ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-
Dweblogic.security.CustomTrustKeyStorePassPhrase=Admin123 ${WLST_PROPERTIES}"
export WLST_PROPERTIES="-Dweblogic.security.CustomTrustKeyStoreType=JKS $
${WLST_PROPERTIES}"

/home/oracle/Oracle/Middleware/Oracle_Home/bi/modules/oracle.bi.sysman/scripts/
stop.sh "$@"

```

19. In your web browser, open the following URL to start Weblogic Console: `http://<OBI_SERVER_IP>:7001/console`
20. In the left pane, navigate to **Environment > Servers > jms_server1** and **Environment > Servers > Admin Server**.
21. Select the **Keystores** tab.
22. Under **Identity**, in the **Custom Identity Keystore** field, type the path to the location of the identity keystore.
23. In the **Custom Identity Keystore Type** field, type `JKS`.
24. In the **Custom Identity Keystore Passphrase** field, type the password for the identity keystore.
25. Confirm the password.
26. Under **Trust**, in the **Custom Trust Keystore** field, type the path to the location of the trusted CA keystore.
27. In the **Custom Trust Keystore Type** field, type `JKS`.
28. In the **Custom Trust Keystore Passphrase** field, type the password for the trusted CA keystore.
29. Confirm the password.
30. Click **Save**.
31. Select the **SSL** tab.
32. Under **Identity**, in the **Private Key Alias** field, type the alias for the identity keystore. For example, type `obiee`.
33. In the **Private Key Passphrase** field, type the password for the identity keystore.
34. Confirm the password.
35. Click **Save**.
36. Select the **General** tab.
37. Select the **SSL Listen Port Enabled** check box.

! Important:

Ensure that the configured **SSL Listen Port** is available and not in use.

38. Restart the OBI server.

Next steps

After the configuration is complete and SSL login for weblogic console is working, configure the servers to disable the non-SSL ports. Do the following:

1. On the weblogic console, navigate to **Environment > Servers > <server name>**.
2. Click **Lock and Edit**.
3. Clear the **Listen Port Enabled** check box.
4. Select the **SSL Listen Port Enabled** check box.

*** Note:**

If you are upgrading from the current Avaya Analytics™ release which has SSL port enabled, and Admin and JMS server ports disabled, then you must enable these ports again before starting the upgrade process.

Deploying the Avaya Analytics™ Streams server

Pre-installation checks for Avaya Analytics™ Streams server

Before you begin

Copy the Kafka software .tar.gz file into the folder on the Avaya Analytics™ Streams server that you are running the installer from.

About this task

Perform this procedure before installing Avaya Analytics™ Streams server. Refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Procedure

1. Copy the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file to the target machine at any location.
2. Ensure you use the same Oracle user that installed the Oracle software.

! Important:

Do not log in as a root user to install Oracle software. If you have logged in as an Oracle user, do not log in as root to troubleshoot issues related to Oracle user login.

The root user login must be used for Operating System-specific tasks such as changing or setting kernel parameters.

3. Ensure that the Oracle software is running.
4. Run the following command to unzip the deployment file:

```
unzip AvayaAnalytics_x.x.x.x_Build_xx.zip
```

5. Configure the following parameters in the STREAMS SERVER SECTION of the `parameters.conf` file for relevant paths and credentials.

```
#####
### STREAMS SERVER SECTION ###
#####

STRM_HOST="127.0.0.1"           #CHANGE THIS TO THE IP OF YOUR SERVER
STRM_SERVER_NAME=JmsServer1    #CHANGE TO MATCH MANAGED SERVER ENTRY SET
PREVIOUSLY IN ENVIRONMENT.PROPERTIES FILE
OSA_JMS_HOSTING_PORT="7003"    #CHANGE TO MATCH MANAGED_LISTEN_PORT SET PREVIOUSLY
IN PARAMETERS.CONF FILE
```

6. Copy the WLS patches zip file to the same location as the unzipped `AvayaAnalytics_x.x.x.x.zip` file.

Installing Avaya Analytics™ Streams server

About this task

Use the following procedure to install the Avaya Analytics™ Streams server. The Avaya install script for Avaya Analytics™ Streams server installs JMS objects, OpenInterface, and Kafka at the same time.

Procedure

1. To change to the root user, type:


```
sudo su -
```
2. Navigate to the directory where you unzipped the deployment scripts.
3. To set the correct permissions for the installation scripts, type:


```
chown -Rf oracle:oinstall .
chmod ug+w .
chmod ug+x *.sh
```
4. Change to the Oracle user and run the following command:


```
./installAvaya.sh
```
5. When prompted for the component to install, type `STREAMS` at the prompt.
6. To accept the End User License Agreement, type `y`.
7. When prompted for the software to install, type `ALL` at the prompt.

8. Enter the password of the Avaya Analytics™ Streams server Weblogic user at the prompt.
9. Enter the password of the Avaya Analytics™ Streams server Redis user at the prompt.

 Note:

You are creating a new password at this prompt.

10. Enter the root password when prompted during the analytics service install.
11. After the installation completes, verify that the system creates the `install_jms.log`, `install_kafka.log`, and `install_wls.patches.log` files in the folder containing the installer. These files contain installation logs for the Avaya Analytics™ Streams server software.

The analytics service comes into effect after the server is rebooted. You can also use the following commands to stop and start services manually:

- `systemctl stop analytics.service`
- `systemctl start analytics.service`

12. Run the following command to refresh profile settings:

```
. ~/.bash_profile
```

Next steps

Verify patches installed successfully. Navigate to the `WLS_HOME/OPatch` directory and run the following command as the Oracle user:

```
./opatch lsinventory
```

Verify that the list of installed patches matches the list in the patch list file contained in the patch folder. There can be additional patches listed after running this command; these patches are part of the base Oracle installation.

Post installation checks for Avaya Analytics™ Streams server

Verifying JMS installation

About this task

Verify JMS installation using the WebLogic Admin Console.

Procedure

1. Log in to WebLogic Admin Console as the weblogic user. In your web browser, enter the following URL to access the WebLogic Admin Console: `http://<STREAMS_SERVER_IP_ADDRESS>:7001/console`
2. Click **Services > Messaging > JMS Modules** and verify the new JMS servers and their corresponding modules.

Verifying Kafka installation

About this task

Use the following procedure to verify Kafka services are started after the install.

Procedure

1. Navigate to the directory where you installed Kafka. For example, `/home/oracle/openInterface/confluent-4.0.0`.
2. Run the following command to check the status of all service:

```
./bin/confluent status
```

3. Use the following commands to manually stop or start services:

```
./bin/confluent start
```

```
./bin/confluent stop
```

! Important:

Kafka must be running before you deploy Avaya Analytics™ for Oracle® Stream Analytics.

Verifying REST OpenInterface, websocket-sender, and Redis installation

About this task

Use the following procedure to verify that REST OpenInterface, websocket-sender, and Redis are successfully installed.

Procedure

1. Navigate to the directory where you installed REST OpenInterface, `/home/oracle/openInterface/rest`. Verify that the install files are present, for example:

```
application.properties killMe.sh logback.xml open-interface-rest-api-x.x.x.x-SNAPSHOT.jar psMe.sh redis.properties rmMe.sh startMe.sh
```

2. Navigate to the directory where you installed websocket-sender, `/home/oracle/openInterface/websocket-sender`. Verify that the install files are present, for example:

```
application.properties loadTestParamsKafka.json logback.xml psMe.sh  
redis.properties startMe.sh websocket-sender-x.x.x.x-SNAPSHOT.jar
```

3. From the `/home/oracle/openInterface/redis-4.0.8` directory, run the following command to verify that Redis is running:

```
./psMe.sh
```

Disabling http on port 7001

About this task

Use this procedure to configure weblogic server to disable http on port 7001.

Procedure

1. In your web browser, open the following URL to start the WebLogic Admin Console:
`http://<STREAMS_SERVER_IP_ADDRESS>:7002/console.`
2. In the navigation pane, click **base_admin > Environment > Servers**.
3. In the Summary of Servers page, click **AdminServer**.
4. On the **General** tab, clear the **Listen Port Enabled** check box.
5. Select the **SSL Listen Port Enabled** check box.
6. Click **Save**.

Configuring Avaya Analytics™ Streams server certificates

You can use an Avaya Analytics™ script to configure security certificates for the Avaya Analytics™ Streams server. The script has 4 configuration options:

- **AUTH**: creates the keystore for Oceana Authentication for Open Interface.
- **SCRTK**: creates the Avaya Breeze® platform certificate keystore for token validation.
- **RSTCSR**: creates the REST Certificate Signing Request (CSR).
- **RSTKEY**: adds certificates to the REST keystore.

Obtaining AuthorizationService node and cluster information

About this task

Perform the following procedure to obtain information about the Avaya Breeze® platform nodes and clusters that AuthorizationService is installed on. This information is required during certificate configuration.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze® > Service Management > Services**.
2. Click **AuthorizationService**.
3. From the **Service Status** list, note the names of the nodes where the AuthorizationService is installed and the cluster information for those nodes.
4. On the System Manager web console, click **Elements > Avaya Breeze® > Cluster Administration**.

5. Expand the cluster where the AuthorizationService SVAR is installed.
6. Click on each Avaya Breeze® platform node and note their SIP Entity IP addresses.

Configuring certificates for user authentication

About this task

Use the following example procedure to configure security certificates for user authentication, using the Avaya Analytics™ Stream server configuration script. The procedure uses System Manager as the Certificate Authority (CA).

* Note:

This example procedure uses 2 Avaya Breeze® platform nodes. There can be additional Avaya Breeze® platform nodes where the **AuthorizationService** SVAR is installed, depending on your solution. If you want to use FQDN's instead of IP addresses, you must ensure that the FQDN's of the System Manager and the Avaya Breeze® platform nodes are reachable on the network.

Before you begin

If you are using a third-party Certificate Authority, obtain a third-party root CA certificate.

Procedure

1. Navigate to the location where you unzipped the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.
2. Edit the following highlighted parameters in the `parameters_certs.conf` file:

```
#####
#### STREAM ANALYTICS CERTS #####
#####
#### Certs and Keystores locations
STRM_CERTS_HOME=/home/oracle/ssl/           Location where
keystores are configured
STRM_TOKEN_TRUSTSTORE=BreezeCerts           Name of Breeze
certs keystore
#### REST System Manager Signed Certs dir
STRM_REST_CERTS_HOME=$STRM_CERTS_HOME/rest/smgr   Location where
keystores are configured

#### SMGR and BREEZE SIP addresses
SMGR_IP=127.0.0.1                               <SystemManager IP>
AUTH_BREEZE_NODE1_SIP=127.0.0.1                <Breeze_1_SIP_Entity_IP_Address>
AUTH_BREEZE_NODE2_SIP=127.0.0.1                <Breeze_2_SIP_Entity_IP_Address>
AUTH_BREEZE_NODE3_SIP=127.0.0.1                <Breeze_3_SIP_Entity_IP_Address>

#####
#####
#####
```

3. Run the following command as the Oracle user:


```
./streamCertsConfiguration.sh
```
4. When prompted for the keystore to configure, type `AUTH`.
5. Type `Y` to confirm you edited the `parameters_certs.conf` file.

6. When prompted, type a password for the new Oceana Authentication keystore.
7. The scripts prompts you for further information that is applied to your security certificates, for example:

```
Country Name (2 letter code) [XX]:IE
State or Province Name (full name) []:Galway
Locality Name (eg, city) [Default City]:Galway
Organization Name (eg, company) [Default Company Ltd]:AVAYA
Organizational Unit Name (eg, section) []:Analytics
Common Name (eg, your name or your server's hostname)
[]:<Analytics_Streams_server_FQDN>
Email Address []:
```

8. When the scripts completes, two keystores are created in the `STRM_CERTS_HOME` directory: `clientkeystore.jks` and `clienttruststore.jks`. To verify that keys exist in these keystores, run the following commands and confirm the output is similar to the following examples:

```
keytool -list -keystore /path/to/keystore/clientkeystore.jks
```

```
clientcert, 29-Jan-2019, PrivateKeyEntry,
```

```
keytool -list -keystore /path/to/keystore/clienttruststore.jks
```

```
smgr.crt, 29-Jan-2019, trustedCertEntry,
Certificate fingerprint
breeze_2, 29-Jan-2019, trustedCertEntry,
Certificate fingerprint
breeze_1, 29-Jan-2019, trustedCertEntry,
Certificate fingerprint
```

9. Perform the following steps to add the `client.crt` file, generated by the script, to System Manager.
 - a. On the System Manager web console, click **Elements > Avaya Breeze® > Configuration > Authorization**.
 - b. On the Clients tab, click **New**.
 - c. In the **New** field, enter a name.
 - d. In the **Certificate** field, browse and select the `client.crt` file that you generated earlier.
 - e. Click **Commit**.

This generates a client identifier that is used when you complete the configuration of application-properties files for REST, Kafka-interface, and websocket-sender. For example:

```
OCEANA.authenticationService.server1clientKey=6DutVilZQLi3YA_tHMFZgw
OCEANA.authenticationService.server2clientKey=6DutVilZQLi3YA_tHMFZgw
```

10. Perform the following steps to download the identity certificates for each Avaya Breeze® platform node the AuthorizationService is installed:
 - a. On the System Manager web console, click **Services > Inventory > Manage Elements**.
 - b. From the Elements list, select the Avaya Breeze® platform node to download the certificate from.

- c. From the **More Actions** list, select **Manage Identity Certificates**.
- d. From the **Service Name** list, select **Authorization** and click **Export**.

The `identity-cert.pem` file is saved to the default download location for your browser. Avaya recommends that you rename this file to `<BreezeNodeName>.pem`. For example, `AvayaBreezeNode1.pem`.

11. Save the certificates to the `STRM_CERTS_HOME` directory configured in the `parameters_certs.conf` file on the Streams server, where you store your security certificates.
12. Navigate to the location where you unzipped the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file and run the following command as the Oracle user:

```
./streamCertsConfiguration.sh
```

13. When prompted for the keystore to configure, type `SCRTK`.
14. When prompted, type a password for the new Avaya Breeze® platform certificate keystore.
15. When the scripts completes, the `BreezeCerts.jks` keystore is created in the `STRM_CERTS_HOME` directory. To verify that keys exist in this keystore, run the following commands and confirm the output is similar to the following example:

```
keytool -list -keystore /path/to/keystore/BreezeCerts
```

```
avayabreezenode2, 29-Jan-2019, trustedCertEntry,
Certificate fingerprint
avayabreezenode1, 29-Jan-2019, trustedCertEntry,
Certificate fingerprint
```

16. Navigate to the location where you unzipped the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file and run the following command as the Oracle user:

```
./streamCertsConfiguration.sh
```

17. When prompted for the keystore to configure, type `RSTCSR`.
18. When prompted, type a password for the new REST certificate keystore.
19. The scripts prompts you for further information that is applied to your security certificates, for example:

```
Enter keystore password: password
What is your first and last name?
[Unknown]: oracle44143.apclab.com
What is the name of your organizational unit?
[Unknown]: Analytics
What is the name of your organization?
[Unknown]: AVAYA
What is the name of your City or Locality?
[Unknown]: GALWAY
What is the name of your State or Province?
[Unknown]: GALWAY
What is the two-letter country code for this unit?
[Unknown]: IE
Is CN=oracle44143.apclab.com, OU=Analytics, O=AVAYA,
```

```
L=GALWAY, ST=GALWAY, C=IE correct?
[no]: yes
Enter key password for <jetty>
(RETURN if same as keystore password):
```

20. When the scripts completes, `keystore.jks` and `keystore.csr` keystores are created in the `STRM_REST_CERTS_HOME/rest/smgr/` directory. For example, the default path is `/home/oracle/ssl/rest/smgr`.

The `keystore.csr` file must be signed by a Certificate Authority (CA). The following example uses SMGR as a CA. If you are not using SMGR as a CA, skip to step 25 and use a third-party root CA certificate instead of `SystemManagerCA.pem`.

21. Perform the following steps to add an End Entity on System Manager.

- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
- b. In the left pane, under **RA Functions**, click **Add End Entity**.
- c. From the **End Entity Profile** list, select **EXTERNAL_CSR_PROFILE**.
- d. In the **Username** field, type a user name.

You must note this user name, as it is required to create a certificate from the CSR.

- e. In the **Password (or Enrollment Code)** field, type a password.

You must note this password, as it is required to create a certificate from the CSR.

- f. In the **Confirm Password** field, re-enter the password.
- g. In the **CN, Common name** field, type the FQDN of the Avaya Analytics™ Streams server.

 Note:

This must match the CN entered when generating the CSR.

- h. In the **Organization, Country, Organizational Unit, Locality**, and **State or Province** fields, type the same values you entered when creating the CSR.
- i. Under **Subject Alternative Name**, in the first **DNS Name** field, type the hostname of the Avaya Analytics™ Streams server.
- j. Under **Subject Alternative Name**, in the second **DNS Name** field, type the FQDN of the Avaya Analytics™ Streams server.
- k. Click **Add**.

22. Perform the following steps to sign the CSR file on System Manager.

- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
- b. In the left pane, click **Public Web**.
- c. Click **Create Certificate from CSR**.
- d. In the **Username** field, type the same user name you entered when adding an End Entity.

- e. In the **Enrollment Code** field, type the same password you entered when adding an End Entity.
 - f. Copy the contents of the CSR created previously on the Avaya Analytics™ Streams server into the text box.
 - g. Click **OK**.
 - h. Download the new certificate as a PEM file. The file is saved as <Streams server name>.pem.
23. Click **Fetch CA Certificates**.
 24. Click **Download as PEM**. The file is saved as SystemManagerCA.pem.
 25. Copy the <Streams server name>.pem file and the <RootCA>.pem file to the STRM_REST_CERTS_HOME directory. The <Streams server name>.pem file is a signed certificate, and if you are using SMGR as a CA the <RootCA>.pem file is SystemManagerCA.pem.
 26. Navigate to the location where you unzipped the AvayaAnalytics_x.x.x.x_Build_xx.zip file and run the following command as the Oracle user:

./streamCertsConfiguration.sh
 27. When prompted for the keystore to configure, type RSTKEY.
 28. When prompted, type the password you set for the new REST certificate keystore in step 18.
 29. When prompted, type the name for the CA file. For example, type SystemManagerCA.pem.
 30. When prompted, type the name for the Stream server PEM file. For example, type <Streams server name>.pem.
 31. When the scripts completes, the keystore.p12 keystore is created in the STRM_REST_CERTS_HOME directory. To verify that keys exist in this keystore, run the following command:

keytool -list -keystore /path/to/keystore/keystore.p12
 32. As the root user, you must perform step 32–35 to find and update the cacerts file on both the Avaya Analytics™ Streams server and the Oracle® Stream Analytics servers. For OSA High Availability deployments, perform these steps on both OSA servers. Use the following commands to find the java location and edit the cacerts in that directory:

```
$ which java
/usr/java/latest/bin/java
$ ls -l /usr/java/
total 0
lrwxrwxrwx. 1 root root 16 Apr 19 10:57 default -> /usr/java/latest
drwxr-xr-x. 9 root root 268 Jul 10 03:34 jdk1.8.0_144
drwxr-xr-x. 9 root root 268 Apr 19 10:57 jdk1.8.0_171-amd64
lrwxrwxrwx. 1 root root 28 Apr 19 10:57 latest -> /usr/java/jdk1.8.0_171-amd64
$ find /usr/java/jdk1.8.0_171-amd64 -name cacerts
/usr/java/jdk1.8.0_171-amd64/jre/lib/security/cacerts
```

*** Note:**

Java can be installed in a different location for your solution.

33. As the root user, back up the cacerts using the following command:

```
cp /usr/java/latest/jre/lib/security/cacerts /usr/java/
latest/jre/lib/security/cacerts.orig
```

34. As the root user, convert the <RootCA>.pem file to a .DER file using the following command, which uses SMGR certificates as an example:

```
openssl x509 -outform der -in SystemManagerCA.pem -out
SystemManagerCA.der
```

35. As the root user, import the <RootCA>.der file into the cacerts directory using the following command, which uses SMGR certificates as an example:

```
keytool -import -alias smgrca -keystore /usr/java/latest/jre/lib/
security/cacerts -file SystemManagerCA.der
```

*** Note:**

The default password for cacerts is `changeit`.

36. Import the <RootCA>.pem file into the Avaya Workspaces web browser. For example, import the `SystemManagerCA.pem` file.

Configuring application-properties files for REST, Kafka-interface and websocket-sender

About this task

Use the following procedure to configure application-properties files for REST, Kafka-interface and websocket-sender after configuring your security certificates.

*** Note:**

This example procedure uses 2 Avaya Breeze® platform nodes. There can be additional Avaya Breeze® platform nodes where the **AuthorizationService** SVAR is installed, depending on your solution.

Procedure

1. Navigate to the location where you unzipped the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.
2. Configure the following parameters in the `streamsApplicationsPropertiesParams.conf` file for relevant paths and credentials.

The `BREEZE_NODE_IP=127.0.0.1` field in the code points to the breeze nodes where the authentication service is installed. Ensure that you replace the IP address 127.0.0.1 with the IP address of your breeze nodes.

```
#####
#### STREAMS SERVER APPLICATION PARAMS ####
```

```
#####

#### REST, kafka-interface and websocket-sender locations####
STRM_REST_HOME=/home/oracle/openInterface/rest
STRM_KAFKAINTERFACE_HOME=/home/oracle/openInterface/kafka-interface
STRM_WEBSOCKETSENDER_HOME=/home/oracle/openInterface/websocket-sender

#Authentication Breeze Nodes SIPs
STRM_SERVER1_BREEZE_NODE1_IP=127.0.0.1
#<Breeze_1_SIP_Entity_IP_Address>
STRM_SERVER1_BREEZE_NODE2_IP=127.0.0.1
#<Breeze_2_SIP_Entity_IP_Address>
STRM_SERVER2_BREEZE_NODE1_IP=127.0.0.1
#<Breeze_1_SIP_Entity_IP_Address>
STRM_SERVER2_BREEZE_NODE2_IP=127.0.0.1
#<Breeze_2_SIP_Entity_IP_Address>

# Oceana Authentication Service
STRM_CLIENT_KEYSTORE_HOME=/home/oracle/ssl/clientkeystore.jks          #Change
to Path of
clientkeystore.jks keystore
STRM_CLIENT_TRUSTSTORE_HOME=/home/oracle/ssl/clienttruststore.jks    #Change to
Path of
clienttruststore.jks keystore
STRM_SERVER1_CLIENT_KEY=          #Change to Client identifier generated on
System Manager
STRM_SERVER2_CLIENT_KEY=          #Change to Client identifier generated on
System Manager

# Token Validation
STRM_TOKEN_TRUSTSTORE_HOME=/home/oracle/ssl/BreezeCerts              #Change to
Path of your BreezeCerts keystore
STRM_TOKEN_TRUSTSTORE_ALIAS=AvayaBreezeNode1,AvayaBreezeNode2        #Change to
Aliases
of keys in BreezeCerts keystore

# REST Keystore
STRM_REST_KEYSTORE_HOME=/home/oracle/ssl/rest/smgr/keystore.p12      #Change to
Path of
REST keystore

# Streams fqdn
STRM_REST_FQDN=localhost          #Change to Stream Server FQDN

# Streams consumer and sender websocket id
STRM_WEBSOCKET_ID=localhost127.0.0.1    #Change to Streams Server name and IP
address

#####
```

3. Run the following command as the Oracle user:

```
./updateApplicationProperties.sh
```

4. When prompted for the Oceana Authentication keystore password, type the password used to generate the `clientkeystore.jks` and `clienttruststore.jks` keystores.
5. When prompted for the REST keystore password, type the password used to generate the `keystore.p12` keystore.
6. Check the script output and verify that no errors occurred.

7. Verify that the REST, Kafka-interface and websocket-sender application-properties files are updated.

Example

See the following example of updated REST, Kafka-interface and websocket-sender application-properties files:

The TokenEndpoint=https://127.0.0.1 field in the code points to the breeze nodes where the authentication service is installed. Ensure that you replace the IP address 127.0.0.1 with the IP address of your breeze nodes.

REST application.properties:

```
# Oceana Authentication Service for Open Interface
OCEANA.authenticationService.storePwd=Admin01$
OCEANA.authenticationService.clientKeystore=/home/oracle/ssl/clientkeystore.jks
OCEANA.authenticationService.clientTruststore=/home/oracle/ssl/clienttruststore.jks
OCEANA.authenticationService.server1clientKey=K38x0GcsSXGTKP1VA7tS9Q
OCEANA.authenticationService.server1breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server1breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2clientKey=K38x0GcsSXGTKP1VA7tS9Q
OCEANA.authenticationService.server2breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.clientCert=clientcert

# Token validation
OCEANA.authenticationService.tokenValidationTrustStore=/home/oracle/ssl/BreezeCerts
OCEANA.authenticationService.smgrPemAlias=AvayaBreezeNode1,AvayaBreezeNode2

server.ssl.key-store=/home/oracle/ssl/rest/smgr/keystore.p12
server.ssl.key-store-password=Admin123

#websocket url
OCEANA.websocket.url=wss://<stream server fqdn>:8422/advrealtime/
```

Kafka-interface application.properties:

```
rest.server.fqdn=hostname.domain

OCEANA.authenticationService.storePwd=Admin01$
OCEANA.authenticationService.clientKeystore=/home/oracle/ssl/clientkeystore.jks
OCEANA.authenticationService.clientTruststore=/home/oracle/ssl/clienttruststore.jks
OCEANA.authenticationService.server1clientKey=K38x0GcsSXGTKP1VA7tS9Q
OCEANA.authenticationService.server1breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server1breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2clientKey=K38x0GcsSXGTKP1VA7tS9Q
OCEANA.authenticationService.server2breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.clientCert=clientcert
```

Websocket-sender application.properties:

```
rest.server.fqdn=hostname.domain
```

```

OCEANA.authenticationService.storePwd=Admin01$
OCEANA.authenticationService.clientKeystore=/home/oracle/ssl/clientkeystore.jks
OCEANA.authenticationService.clientTruststore=/home/oracle/ssl/clienttruststore.jks
OCEANA.authenticationService.server1clientKey=K38x0GcsSXGTP1VA7tS9Q
OCEANA.authenticationService.server1breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server1breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2clientKey=K38x0GcsSXGTP1VA7tS9Q
OCEANA.authenticationService.server2breeze1TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.server2breeze2TokenEndpoint=https://127.0.0.1:9443/
services/AuthorizationService/token
OCEANA.authenticationService.clientCert=clientcert

# Token validation
OCEANA.authenticationService.tokenValidationTrustStore=/home/oracle/ssl/BreezeCerts
OCEANA.authenticationService.smgrPemAlias=AvayaBreezeNode1,AvayaBreezeNode2

OCEANA.websocketSender.kafka.consumerid.prefix=hostname127.0.0.1

OCEANA.websocketSender.senderId=hostname127.0.0.1

OCEANA.websocketSender.server.ssl.key-store=/home/oracle/ssl/rest/smgr/keystore.p12
OCEANA.websocketSender.server.ssl.key-store-password=

OCEANA.openInterface.rest.url=https://<stream server fqdn>:8443

```

Post installation steps for Avaya Analytics™ Streams server

JVM settings on the Avaya Analytics™ Streams server

Application	Agent sizing		
	1	2	3
	25, 100 Agents	250, 500, 1000 Agents	2000, 4500 Agents
REST	0.8 GB	1.5 GB	2 GB
Kafka-interface	0.7 GB	1.5 GB	2 GB
Websocket-sender	1.5 GB	3 GB	3.5 GB
JMS	4.5 GB	9 GB	11 GB

Modifying JVM heap settings for 25-100 agents

About this task

This procedure provides instructions about how to modify JVM heap settings on the Avaya Analytics™ Streams server for the agent sizing 1 (12 GB) involving 25-100 agents.

Procedure

1. To set the JVM memory to 0.8 GB on the REST application, do the following:
 - a. Edit \$STREAMS_REST_HOME/startMe.sh.

- b. Add the Xmx parameter to the existing java command as follows:


```
nohup java -Xmx820m -jar ./open-interface-rest-api.jar &
```
2. To set the JVM memory to 0.7 GB on the Kafka-interface application, do the following:
 - a. Edit \$STREAMS_KAFKA_INTERFACE_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:


```
nohup java -Xmx717m -jar ./open-interface-kafka-interface.jar &
```
3. To set the JVM memory to 1.5 GB on the websocket-sender application, do the following:
 - a. Edit \$STREAMS_WEBSOCKET_SENDER_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:


```
nohup java ${DEBUG} -Xmx1536m -jar ./open-interface-websocket-sender.jar &
```
4. To set the JVM memory to 4.5 GB on the JMS application, do the following:
 - a. Edit \$STRM_HOME/bin/setUserOverrides.sh.
 - b. Modify the Xms and Xmx parameters as follows:


```
export USER_MEM_ARGS="-Xms4608m -Xmx4608m -Xmn4g"
```

Modifying JVM heap settings for 250-1000 agents

About this task

This procedure provides instructions about how to modify JVM heap settings on the Avaya Analytics™ Streams server for the agent sizing 2 (24 GB) involving 250-1000 agents.

Procedure

1. To set the JVM memory to 1.5 GB on the REST application, do the following:
 - a. Edit \$STREAMS_REST_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:


```
nohup java -Xmx1536m -jar ./open-interface-rest-api.jar &
```
2. To set the JVM memory to 1.5 GB on the Kafka-interface application, do the following:
 - a. Edit \$STREAMS_KAFKA_INTERFACE_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:


```
nohup java -Xmx1536m -jar ./open-interface-kafka-interface.jar &
```
3. To set the JVM memory to 3 GB on the websocket-sender application, do the following:
 - a. Edit \$STREAMS_WEBSOCKET_SENDER_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:


```
nohup java ${DEBUG} -Xmx3G -jar ./open-interface-websocket-sender.jar &
```

4. To set the JVM memory to 9 GB on the JMS application, do the following:
 - a. Edit \$STRM_HOME/bin/setUserOverrides.sh.
 - b. Modify the Xms and Xmx parameters as follows:

```
export USER_MEM_ARGS="-Xms9g -Xmx9g -Xmn4g"
```

Modifying JVM heap settings for 2000-4500 agents

About this task

This procedure provides instructions about how to modify JVM heap settings on the Avaya Analytics™ Streams server for the agent sizing 3 (30 GB) involving 2000-4500 agents.

Procedure

1. To set the JVM memory to 2 GB on the REST application, do the following:
 - a. Edit \$STREAMS_REST_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:
2. To set the JVM memory to 2 GB on the Kafka-interface application, do the following:
 - a. Edit \$STREAMS_KAFKA_INTERFACE_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:
3. To set the JVM memory to 3.5 GB on the websocket-sender application, do the following:
 - a. Edit \$STREAMS_WEBSOCKET_SENDER_HOME/startMe.sh.
 - b. Add the Xmx parameter to the existing java command as follows:
4. To set the JVM memory to 11 GB on the JMS application, do the following:
 - a. Edit \$STRM_HOME/bin/setUserOverrides.sh.
 - b. Modify the Xms and Xmx parameters as follows:

```
nohup java -Xmx2G -jar ./open-interface-rest-api.jar &
```

```
nohup java -Xmx2G -jar ./open-interface-kafka-interface.jar &
```

```
nohup java ${DEBUG} -Xmx3584m -jar ./open-interface-websocket-sender.jar &
```

```
export USER_MEM_ARGS="-Xms11g -Xmx11g -Xmn4g"
```

Starting REST, Kafka interface and websocket-sender

About this task

This procedure describes how you manually start the REST Interface, the Kafka interface, and websocket-sender on the Avaya Analytics™ Streams server.

Procedure

1. Make the scripts executable in the /home/oracle/openInterface/rest, /home/oracle/openInterface/kafka-interface, and /home/oracle/openInterface/websocket-sender directories by running the following command:

```
chmod +x *.sh
```

2. To start REST, run the following command from the `/home/oracle/openInterface/rest` directory:

```
./startMe.sh
```

3. To start Kafka, run the following command from the `/home/oracle/openInterface/kafka-interface` directory:

```
./startMe.sh
```

4. To start websocket-sender, run the following command from the `/home/oracle/openInterface/websocket-sender` directory:

```
./startMe.sh
```

5. To check if each of the processes are running, run the following command in each directory:

```
./psMe.sh
```

Checking configuration of auto-start of services

Procedure

1. Reboot the Streams server.

Wait until all the following applications start:

- Node Manager
- Weblogic AdminServer and JMS Server1
- Kafka processes such as Zookeeper, Kafka, Schema-Registry, Kafka-Rest and Connect
- Open-interface-rest
- Open-interface-kafka-interface and websocket-sender

2. Run the following commands:

```
systemctl stop analytics.service
```

```
systemctl start analytics.service
```

The application checks the auto-start feature of services of all these processes.

Configuring SSL for Stream server weblogic

About this task

Use this procedure to configure SSL for Stream server weblogic.

! Important:

Run all commands for this procedure as the Oracle user, unless otherwise stated.

Before you begin

If you are using a third-party Certificate Authority, obtain a third-party root CA certificate.

Procedure

1. On the OBI server, create a directory for the certificates you are going to create. For example, run the following command to create a directory:

```
mkdir -p /home/oracle/SSL/
cd /home/oracle/SSL/
```

2. Run the following command from the newly created directory to generate a key pair, and type the correct information for your solution:

```
keytool -genkeypair -alias obiee -keyalg RSA -keysize 2048 -
keystore obi.jks -validity 3650
```

The following is an example of the information passed:

```
Enter keystore password: password
What is your first and last name?
  [Unknown]: WFOBIEE4284V.wf.aura.com
What is the name of your organizational unit?
  [Unknown]: Analytics
What is the name of your organization?
  [Unknown]: AVAYA
What is the name of your City or Locality?
  [Unknown]: GALWAY
What is the name of your State or Province?
  [Unknown]: GALWAY
What is the two-letter country code for this unit?
  [Unknown]: IE
Is CN=WFOBIEE4284V.wf.aura.com, OU=Analytics, O=AVAYA,
L=GALWAY, ST=GALWAY, C=IE correct?
  [no]: yes
Enter key password for <obiee>
      (RETURN if same as keystore password):
Re-enter new password:
```

3. Run the following command to generate a Certificate Signing Request (CSR):

```
keytool -certreq -v -alias obiee -keyalg RSA -sigalg SHA256withRSA
-file obi.csr -keystore obi.jks -storepass Admin123
```

4. Ensure that 2 files now exist in the new directory. The `obi.csr` file must be signed by a Certificate Authority (CA), the following example uses SMGR as a CA. If you are not using SMGR as a CA, skip to step 9 and use a third-party root CA certificate instead of `SystemManagerCA.pem`.
5. Perform the following steps to add an End Entity on System Manager.
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the left pane, under **RA Functions**, click **Add End Entity**.

- c. From the **End Entity Profile** list, select **EXTERNAL_CSR_PROFILE**.
- d. In the **Username** field, type a user name.

You must note this user name, as it is required to create a certificate from the CSR.

- e. In the **Password (or Enrollment Code)** field, type a password.

You must note this password, as it is required to create a certificate from the CSR.

- f. In the **Confirm Password** field, re-enter the password.
- g. In the **CN, Common name** field, type the FQDN of the OBI server.

 Note:

This must match the CN entered when generating the CSR.

- h. In the **Organization, Country, Organizational Unit, Locality, and State or Province** fields, type the same values you entered when creating the CSR.
 - i. Under **Subject Alternative Name**, in the first **DNS Name** field, type the hostname of the OBI server.
 - j. Under **Subject Alternative Name**, in the second **DNS Name** field, type the FQDN of the OBI server.
 - k. Click **Add**.
6. Perform the following steps to sign the CSR file on System Manager.
- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the left pane, click **Public Web**.
 - c. Click **Create Certificate from CSR**.
 - d. In the **Username** field, type the same user name you entered when adding an End Entity.
 - e. In the **Enrollment Code** field, type the same password you entered when adding an End Entity.
 - f. Copy the contents of the CSR created previously on the OBI server into the text box.
 - g. Click **OK**.
 - h. Download the new certificate as a PEM file. The file is saved as `<OBI server name>.pem`
7. Click **Fetch CA Certificates**.
8. Click **Download as PEM**. The file is saved as `SystemManagerCA.pem`
9. Copy `<OBI server name>.pem` and `SystemManagerCA.pem` files to the `/home/oracle.SSL/` directory in the OBI server.
10. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to import the root CA certificate into the `obi.jks` keystore:

```
keytool -import -trustcacerts -alias smgrca -file
SystemManagerCA.pem -keystore obi.jks -keypass changeit -storepass
Admin123
```

11. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to import the signed certificate into the `obi.jks` keystore:

```
keytool -import -trustcacerts -alias obiee -file <OBI server
name>.pem -keystore obi.jks -keypass Admin123 -storepass Admin123
```

12. On the OBI server, run the following command from the `/home/oracle/SSL/` directory to convert the JKS to p12:

```
keytool -importkeystore -srckeystore obi.jks -destkeystore obi.p12
-deststoretype pkcs12
```

13. As the root user, convert the SMGR .PEM file to a .DER file using the following command:

```
openssl x509 -outform der -in SystemManagerCA.pem -out
SystemManagerCA.der
```

14. As the root user, back up the cacerts using the following command:

```
cp /usr/java/latest/jre/lib/security/cacerts /usr/java/
latest/jre/lib/security/cacerts.orig
```

 Note:

The location of the cacerts folder can differ from this example.

15. As the root user, import the SMGR .DER file into the cacerts directory using the following command:

```
keytool -import -alias smgrca -keystore /usr/java/latest/jre/lib/
security/cacerts -file SystemManagerCA.der
```

 Note:

The default password for cacerts is `changeit`. The location of the cacerts folder can differ from this example.

16. In your web browser, open the following URL to start Weblogic Console: `http://<OBI_SERVER_IP>:7001/console`
17. In the left pane, navigate to **Environment > Servers > jms_server1** and **Environment > Servers > Admin Server**.
18. Select the **Keystores** tab.
19. Under **Identity**, in the **Custom Identity Keystore** field, type the path to the location of the identity keystore.
20. In the **Custom Identity Keystore Type** field, type `JKS`.
21. In the **Custom Identity Keystore Passphrase** field, type the password for the identity keystore.

22. Confirm the password.
23. Under **Trust**, in the **Custom Trust Keystore** field, type the path to the location of the trusted CA keystore.
24. In the **Custom Trust Keystore Type** field, type `JKS`.
25. In the **Custom Trust Keystore Passphrase** field, type the password for the trusted CA keystore.
26. Confirm the password.
27. Click **Save**.
28. Select the **SSL** tab.
29. Under **Identity**, in the **Private Key Alias** field, type the alias for the identity keystore. For example, type `obiee`.
30. In the **Private Key Passphrase** field, type the password for the identity keystore.
31. Confirm the password.
32. Click **Save**.
33. Select the **General** tab.
34. Select the **SSL Listen Port Enabled** check box.

 Important:

Ensure that the configured **SSL Listen Port** is available and not in use.

35. Restart the OBI server.

Next steps

After the configuration is complete and SSL login for weblogic console is working, configure the servers to disable the non-SSL ports. Do the following:

1. On the weblogic console, navigate to **Environment > Servers > <server name>**.
2. Click **Lock and Edit**.
3. Clear the **Listen Port Enabled** check box.
4. Select the **SSL Listen Port Enabled** check box.

 Note:

If you are upgrading from the current Avaya Analytics™ release which has SSL port enabled, and Admin and JMS server ports disabled, then you must enable these ports again before starting the upgrade process.

Deploying Avaya Analytics™ for Oracle® Stream Analytics

Pre-installation checks for Oracle® Stream Analytics

Before you begin

- Ensure that certificate configuration for Avaya Breeze® platform is complete. For more information, see [Configuring Avaya Analytics certificates for Avaya Breeze platform](#) on page 106.
- Ensure that the JMS components are installed on Weblogic. There is a dependency for the OSA applications on the existence of JMS queues with certain names.
- Ensure that Confluent Kafka is installed and running on the Avaya Analytics™ Streams server. The OSA install fails if Kafka is not running. For more information about manually starting Kafka, see [Verifying Kafka installation](#) on page 84.
- Ensure that the Database components are installed on the historical reports target database. There is a dependency for the OSA applications on the existence of certain database columns.
- For OSA High Availability deployments, install Oracle® Stream Analytics on two separate RHEL servers. The install procedure is the same for both servers. For more information, see [Installing Oracle® Stream Analytics](#) on page 59.

About this task

Perform this procedure before installing Oracle® Stream Analytics. Using this procedure you must update the Oracle® Stream Analytics configuration files, and you must also log on to the Oracle Event Processing Visualizer to create a data source. Refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Important:

For OSA High Availability deployments, perform this procedure on both the primary and standby servers.

Procedure

1. Complete Step 32 through Step 35 as mentioned in [Configuring certificates for user authentication](#) on page 86.
2. Copy the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file to the target machine at any location.
3. Ensure you use the same Oracle user that installed the Oracle software.

Important:

Do not log in as a root user to install Oracle software. If you have logged in as an Oracle user, do not log in as root to troubleshoot issues related to Oracle user login. The root user login must be used for Operating System-specific tasks such as changing or setting kernel parameters.

4. Ensure the Oracle software is running.
5. Run the following command to unzip the deployment file:

```
unzip AvayaAnalytics_x.x.x.x_Build_xx.zip
```
6. Configure the certificates as described in [Configuring Avaya Analytics certificates for Avaya Breeze platform](#) on page 106.
7. Copy the Oracle® Stream Analytics patches zip file to the same location as the unzipped AvayaAnalytics_x.x.x.x.zip file.
8. Edit the following highlighted OSA parameters in the ORACLE STREAM ANALYTICS SECTION of the parameters.conf file to point to the correct IP addresses:

```
#####
#### ORACLE STREAM ANALYTICS SECTION ####
#####

#### Oracle Home under which Oracle Stream Analytics is installed ####
OSA_ORACLE_HOME="/home/oracle/Oracle/Middleware/Oracle_Home"

#### Directory where the OSA server is installed, this is a folder under the osa
domain directory ####
OSA_SERVER_HOME="/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/
osadomain/osaserver"
#### Homes 1 and 2 only needed for cluster install ####
OSA_SERVER_HOME1="/home/oracle/Oracle/Middleware/Oracle_Home_OSA/user_projects/
domains/osacluster/osa1"
OSA_SERVER_HOME2="/home/oracle/Oracle/Middleware/Oracle_Home_OSA/user_projects/
domains/osacluster/osa2"

#### Oracle Stream Analytics Credentials and host details ####
OSA_USER="wlevs"
OSA_HOST="127.0.0.1"
OSA_PORT="9002"

#### Do not modify the OSA group value ####
OSA_GROUP="AllDomainMembers"

#### Ports 1 and 2 and groups only needed for cluster install ####
#OSA_PORT1="9002"
#OSA_PORT2="9004"
#OSA_GROUP0="AllDomainMembers"
#OSA_GROUP1="osa1"
#OSA_GROUP2="osa2"

#### Directory where Java is installed, needed for wlevsdeploy to run ####
OSA_JAVA_HOME="/usr/java/latest"

#### Weblogic JMS Server that the OSA applications are using ####
OSA_STREAMS_HOST="127.0.0.1"      #SET TO STREAMS SERVER IP ADDRESS
OSA_JMS_PORT="7003"
OSA_JMS_USER="weblogic"

#### Apache MQ Server that OSA applications are reading, items 2 and 3 are for
Ref cluster failover. Ignore them if there is no cluster ####
OSA_MQ_HOST="ssl://127.0.0.1"      #SET TO SECURITY IP ADDRESS OF BREEZE NODE 1 -
OCEANA CLUSTER 1
OSA_MQ_PORT="61617"

OSA_MQ_HOST2="ssl://0.0.0.0"      #SET TO SECURITY IP ADDRESS OF BREEZE NODE 2 -
```

```

OCEANA_CLUSTER 1
OSA_MQ_PORT2="00000"

OSA_MQ_HOST3="ssl://0.0.0.0"      #SET TO SECURITY IP ADDRESS OF BREEZE NODE 3 -
OCEANA_CLUSTER 1
OSA_MQ_PORT3="00000"

UCM REST Cluster IP ####
OSA_UCM_HOST="127.0.0.1"          #SET TO CLUSTER IP ADDRESS OF OCEANA_CLUSTER 1

#### OSA Open Interfaces enabled YES/NO####
OPEN_INTERFACES_ENABLED=YES

```

9. Edit the parameters highlighted below in the SNMP APPLICATION section:

```

#####
#OSA - SNMP APPLICATION
# DB server
OSA_DB_HOST_IP="127.0.0.1"
OSA_DB_SSH_USER="oracle"
OSA_DB_SSH_PASSWORD="oraclePwd"
OSA_DB_EM_PORT="5500"
OSA_DB_TNS_LOG_LOCATION="/home/oracle/app/oracle/diag/tnslsnr/databaseHostname/
listener/trace/"
OSA_DB_LOG_LOCATION="/home/oracle/app/oracle/diag/rdbms/orcl/orcl/trace/"
OSA_DB_LOG_FILE="alert_orcl.log"
# ODI server
OSA_ODI_HOST_IP="127.0.0.1"
OSA_ODI_SSH_USER="oracle"
OSA_ODI_SSH_PASSWORD="oraclePwd"
OSA_ODI_LOG="/home/oracle/app/oracle/Oracle_Home_ODI_Standalone/user_projects/
domains/odistandaloneagent/system_components/ODI/OracleDIAgent1/logs/oracledi/"
# OBIEE server
OSA_OBIEE_HOST_IP="127.0.0.1"
OSA_OBIEE_ADMINSERVER_PORT="9500"
OSA_OBIEE_NODEMANAGER_PORT="9506"
OSA_OBIEE_ANALYTICS_PORT="9502"
# STREAMS server
OSA_STREAMS_HOST_IP="127.0.0.1"
# SNMP destinations
OSA_TRAP_DESTINATION_HOST_IP=127.0.0.1
OSA_TRAP_DESTINATION_HOST_PORT=162
OSA_PROTOCOL_VERSION="V3"
OSA_V3_USER="snmpV3Usr"
OSA_V3_AUTH_PASSWORD="snmpV3Pwd"
OSA_V3_PRIV_PASSWORD="snmpV3Pwd"
OSA_V3_AUTH_PROTOCOL="MD5"
OSA_V3_PRIV_PROTOCOL="DES"
OSA_V3_SECURITY_LEVEL="AUTH_PRIV"
# OSA - SNMP APPLICATION #
#####

```

Important:

- For a fresh installation, ensure that you open the `server.properties.vanilla` file, search for the `DataBase.OceanaDataMart.url=jdbc:oracle:thin:@127.0.0.1:1521:orcl` line, and edit the Database connection string to replace the IP address with the IP address of your Oracle® Database server.

Configure the port number of your Oracle® Database server and also the SID(orcl) to match the one on your server.

10. Edit the following section in the `server.properties.vanilla` file:

```
#Delphi Producer Registration Service

#IP address of the Streams server
Oceana.producer.source.transactionUrl=https://127.0.0.1:8443           #CHANGE THIS
TO THE ADDRESS OF YOUR STREAMS SERVER
Oceana.producer.source.sourceName=Oceana_142_Streams
Oceana.producer.source.timeZone=GMT
Oceana.producer.source.version=3.5
Oceana.producer.source.description=Analytics for Oceana
Oceana.producer.source.location=Galway

#IP address of the OSA server
Oceana.producer.source.ipAddress=127.0.0.1           #CHANGE THIS TO THE IP OF
YOUR OSA SERVER
OCEANA.realtime.measures.source=Oceana
```

For OSA High Availability deployments, you must also edit the following parameters on the primary server:

```
HA.deployment=YES
Other.HA.Server.IP=127.0.0.1           #CHANGE THIS TO THE IP ADDRESS OF YOUR OSA
STANDBY SERVER
HA.JMS.server.IP=127.0.0.1           #CHANGE THIS TO THE IP ADDRESS OF YOUR
STREAMS SERVER
HA.JMS.server.port=7003           #CHANGE THIS TO THE PORT THAT JMS TOPICS
CONNECT TO
```

For OSA High Availability deployments, you must also edit the following parameters on the standby server:

```
HA.deployment=YES
Other.HA.Server.IP=127.0.0.1           #CHANGE THIS TO THE IP ADDRESS OF YOUR OSA
PRIMARY SERVER
HA.JMS.server.IP=127.0.0.1           #CHANGE THIS TO THE IP ADDRESS OF YOUR
STREAMS SERVER
HA.JMS.server.port=7003           #CHANGE THIS TO THE PORT THAT JMS TOPICS
CONNECT TO
```

For OSA High Availability deployments, you must ensure that the below property is the same on both the primary and secondary server.

```
Oceana.producer.source.ipAddress=127.0.0.1           #CHANGE THIS TO THE IP ADDRESS OF
THE PLANNED PRIMARY SERVER
```

11. Login to `http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/`. The default username and password are `wlevs` and `Admin123`.* **Note:**

If the web interface is not accessible, run the following commands as the Oracle user to start services:

```
cd $MW_HOME/user_projects/domains/osadomain/osaserver/
nohup ./startwlevs.sh > /dev/null &
```

12. To create a new datasource, click **osadomain > osaserver**.13. Select the **Data Sources** tab.

14. Click **Add**.
15. On the Data Sources tab, perform the following steps:
 - a. In the **Name** field, enter `StreamAnalyticsDS`.
 - b. In the **JNDI Name** field, enter `jdbc/StreamAnalyticsDS`.
 - c. In the **Global Transaction Protocol** field, select `One Phase Commit`.
16. On the Global Transaction Protocol tab, perform the following steps:
 - a. In the **Database Type** field, select `Oracle`.
 - b. In the **URL** field, enter `jdbc:oracle:thin:@your_database_host:your_database_port:SID`.
This is the database where the Historical Reports are located.

 Note:

For solutions using Oracle® RAC Database, `your_database_host` must match the Single Client Access Name (SCAN).

- c. In the **Driver Name** field, enter `oracle.jdbc.OracleDriver`.
 - d. In the **User Name** field, enter `GILA_STAGE`.
 - e. In the **Password** field, enter `Admin01$`.
 - f. In the **Use XA** field, select `True`.
17. Click **Save**.

 Note:

The `server.properties` file is updated based on the values populated in the `parameters.conf` and `server.parameters.vanilla` files.

Configuring Avaya Analytics™ certificates for Avaya Breeze® platform

About this task

The connection to Reliable Eventing Broker (ActiveMQ) includes a mutual TLS connection. It involves setting clients to present valid certificates to Reliable Eventing Broker. However, if your client is an external client other than a snap-in, these external clients need to be configured with the security certificates.

The passwords used for the keystore and the CSR/P12 certificate must match. When you download the `JKS` file from System Manager Certificate Authority (CA), it has the password `changit`. When the keystore is built, you must change the password so that it is same as the password of the certificate. You must also add the password to the `server.properties` file.

With this procedure, you can configure security certificates for user authentication using the Avaya Analytics™ OSA server configuration script. The script has the following configuration options:

- CSR: To create Certificate Signing Request (CSR).
- STORE: To add certificates to the keystore and configure the OSA server.

The procedure uses System Manager as the CA.

Before you begin

- Install OpenSSL on the OSA server if required.
- If you are using a third-party Certificate Authority (CA), obtain a third-party root CA certificate.

Procedure

1. Navigate to the location where you unzipped the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file.
2. From the unzipped folder, open the `param_cert_osa.conf` file.
3. Configure the `OSA_SERVER_HOME` and `SMGR_HOME` parameters according to the configuration of your environment.
4. Configure the following parameters according to their descriptions mentioned in the table:

Parameter	DN field	Description	Example
CITY	City or Locality	The city where your organization is legally located.	Galway
FDQN	Common Name	The fully qualified domain name of the OSA server. This must be an exact match.	To secure the <i>www.yourdomain.com</i> URL, use your CSR's common name as <i>www.yourdomain.com</i> . To get a wildcard certificate, ensure to prefix your domain name with an asterisk. For example, <i>*.domain.com</i> .
COUNTRY	Country	The two-letter ISO abbreviation for your country.	IE
ORGANIZATION	Organization Name	The exact legal name of your organization.	AVAYA
ORG_UNIT	Organizational Unit	The section of the organization.	Analytics
STATE	State or Province	The state or province where your organization is legally located. Do not use an abbreviation.	Galway

5. From the Avaya installation folder, run the following command as the `oracle` user:

```
./create_cert_osa.sh
```

6. For the first action of the script, enter the CSR.

The following three files are created in the `<BuildDirectory>/osa_certs` directory:

- `client.csr`
- `client.key`
- `SystemManagerCA.pem`

7. Do the following to create an end entity:
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the navigation pane, in the RA Functions area, click **Add End Entity**.
 - c. In the **End Entity Profile** field, select `EXTERNAL_CSR_PROFILE`.
 - d. In the **Username** field, enter a user name.
Ensure that you make a note of the user name. This user name is required for creating a certificate from the CSR.
 - e. In the **Password (or Enrollment Code)** field, enter a password.
Ensure that you make a note of the password. This password is required when creating a certificate for this server.
 - f. In the **Confirm Password** field, re-enter the password.
 - g. In the **CN, Common name** field, enter a name that matches the FQDN of the server.
This name must match the CN that you entered while generating the CSR.
 - h. In the **Organization, Country, Organizational Unit, Locality**, and **State or Province** fields, enter the appropriate value as specified while creating the CSR.
 - i. Click **Add**.
8. Do the following to create a certificate from the CSR:
 - a. Using an FTP client, export the Certificate Signing Request (CSR) file from the server.
 - b. Open the CSR file in a text editor such as Notepad.
 - c. In your web browser, enter the following URL for the System Manager installation of EJBCA.
`https://<SMGR_FQDN>/ejbca`
 - d. In the navigation pane, in the **Enroll** area, click **Create Certificate from CSR**.
 - e. In the **Username** field, enter the user name.
 - f. In the **Enrollment code** field, enter the password.
 - g. From the text editor, copy the content of the CSR file that is present between the `---BEGIN CERTIFICATE REQUEST---` and `---END CERTIFICATE REQUEST---` lines.
 - h. Paste the copied content into the list.
 - i. Click **OK**.
 - j. Download the certificate as a `pem` file with the name `<Cert_Name>.pem`.
 - k. Upload the downloaded `pem` file to the `<BuildDirectory>/osa_certs/` directory in the OSA server.
9. In the `param_crt_osa.conf` file, in the `CRT_PEM_CSR` parameter, enter `<Cert_Name>.pem`.

<Cert_Name> is the name of the certificate file that you specified while creating the certificate from the CSR.

10. Run the following command as the Oracle user:

```
./create_cert_osa.sh
```

When prompted to select an action, enter `STORE` and wait for the script execution to complete.

 Important:

Ensure that you do not delete the default OSA Keystore (evsidentity.jks). This is required to start the OSA server.

Installing Avaya Analytics™ for Oracle® Stream Analytics

Before you begin

- Ensure that the Dashboard appears when you log in to Oracle Event Processing Visualizer at `http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/`.

About this task

Use the following procedure to install Avaya Analytics™ for Oracle® Stream Analytics. This procedure also describes how to install Avaya Analytics™ for Oracle® Stream Analytics in a HA deployment.

Procedure

1. Perform the following steps to configure auto-start of services:
 - a. Change to the root user using the following command:


```
sudo su -
```
 - b. Go to the directory where you unzipped the deployment scripts.
 - c. Run the following commands to set the correct permissions for the installation scripts:
 - `chown -Rf oracle:oinstall .`
 - `chmod ug+w .`
 - `chmod ug+x *.sh`
2. Ensure that you use the Oracle user account.
3. Run the following command to install the OSA project:


```
./installAvaya.sh
```
4. When the system prompts you with the Please confirm that you have edited the parameters.conf file by entering y to continue message, type y.
If you type any other string, the process is cancelled.

5. When prompted for the component to install:
 - Type `OSA` for non-HA solutions.
 - Type `OSAHA` for HA solutions on both HA servers.
6. To accept the End User License Agreement, type `y`.
7. The system prompts you with the message: "To accept the End User License Agreement SDK terms and conditions, type `y`".
8. Enter the password for the Oracle® Stream Analytics administrator user at the prompt.
9. Enter the password of the Avaya Analytics™ Streams server Weblogic user at the prompt.
10. Enter the root password when prompted during the analytics service install.
11. After the installation completes, verify that the system creates the `install_osa.log` file in the folder containing the installer. This file contains the installation logs for Oracle® Stream Analytics.

The analytics service comes into effect after the server is rebooted. You can also use the following commands to stop and start services manually:

- `systemctl stop analytics.service`
- `systemctl start analytics.service`

Next steps

Verify patches installed successfully. Navigate to the `Middleware/Oracle_Home/OPatch` directory and run the following command as the Oracle user:

```
./opatch lsinventory
```

Verify that the list of installed patches matches the list in the patch list file contained in the patch folder. There might be additional patches listed after running this command; these patches are part of the base Oracle installation.

Post installation checks for Oracle® Stream Analytics

The system displays the new applications deployed to the OSA server in the Oracle Event Processing Visualizer. Navigate to `http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/` using your web browser.

When you log in to the OSA Dashboard, in the left pane, expand the menu and click **Deployment**. Confirm that your applications are in **RUNNING** state.

Review the status of Reliable Eventing destinations to ensure that relevant topics and queues have been created. For more information, see [Viewing the status of Reliable Eventing destinations](#) on page 28.

Post installation steps for Oracle® Stream Analytics

Modifying JVM heap settings

About this task

After install, the default heap settings for the Avaya Analytics™ OSA process are configured for a 100 agent solution. If your solution requires a higher agent capacity, you must configure heap settings and restart the OSA wlevs process. Perform this procedure as the Oracle user.

! Important:

Avaya recommends that you back up the startwlevs.sh script before performing this procedure.

Procedure

1. Ensure that the OSA server has adequate RAM to support your solution capacity.
2. Navigate to the OSA_SERVER_HOME directory.
3. Using the values in the table below, edit the startwlevs.sh script, replacing the Xms, Xmx and Xmn settings of JVM_ARGS as required for your solution. For example, to change the setting to support a 500 agent solution, set JVM_ARGS to the following highlighted values:

```
if [ $JAVA_VENDOR = "Sun" ]
then
  JVM_ARGS="-server -Xms30g -Xmx30g -Xmn12g -XX:MetaspaceSize=768m -
XX:MaxMetaspaceSize=768m -XX:+UseConcMarkSweepGC -XX:SurvivorRatio=4 -XX:-
UseAdaptiveSizePolicy -XX:CMSInitiatingOccupancyFraction=70 -XX:
+UseCMSInitiatingOccupancyOnly -XX:+UnlockDiagnosticVMOptions -XX:
+UnsyncloadClass -verbose:gc -XX:+PrintGCDateStamps -XX:+PrintGCDetails -
Xloggc:osa_server_gc.%p.log -XX:+HeapDumpOnOutOfMemoryError -
XX:HeapDumpPath=osa_server.%p.hprof"
fi
```

Table 3: Heap settings required per solution capacity

Solution capacity	OSA wlevs process heap settings		
	Xms	Xmx	Xmn
1 – 100 agents	12g	12g	7g
101 – 250 agents	18g	18g	9g
251 – 500 agents	30g	30g	12g
501 – 1000 agents	48g	48g	16g
1001 – 2000 agents	56g	56g	20g
2001 – 4500 agents	72g	72g	24g

4. Restart the OSA server by running the following commands:

```
./stopwlevs.sh
nohup ./startwlevs.sh > /dev/null &
```

Generating CSV files

About this task

If you require CSV files to be generated for Agent By Account and Routing Service historical reports, perform the following procedure. Once this procedure is performed, CSV files are generated at 15 minute intervals to the following locations:

- Routing Service
 - /home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/osadomain/osaserver/FnS/RoutingService_Details.csv
- Agent By Account
 - /home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/osadomain/osaserver/Scorecard/AgentByAccount_Details.csv

Procedure

1. Navigate to the /home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/osadomain/osaserver directory.
2. Edit the server.properties file, making the following change:

```
CSV.consumer=true
```

3. Restart the OSA server by running the following commands:

```
./stopwlevs.sh
nohup ./startwlevs.sh > /dev/null &
```

The CSV files are created when the first measures for each dimension are written to the database.

Starting OSA components after a restart

About this task

Use this procedure to start OSA after you restart the OSA server.

Procedure

Perform the following steps to start OSA:

- a. Go to the directory where you installed OSA. For example, \$Oracle_Home/user_projects/domains/<OSA_Domain_Dir>/<OSA_SERVER_NAME>.
- b. Run the following command to start OSA:

```
nohup ./startwlevs.sh > sw.out &
```

Disaster Recovery

In a solution using Oracle Data Guard, one instance of Oracle® Database runs on two virtual servers, a Primary server and a Standby server. You can use the Oracle Data Guard feature for Disaster Recovery (DR). This allows you to recover after a complete outage occurs at your primary data center. You must have a complete secondary solution deployed at the DR site. This includes installing both Avaya Oceana® Solution and Avaya Analytics™ at the DR site.

When you install the Standby server in an Oracle Data Guard configuration, a second database called “orclrcu” is created. This database is not part of the Data Guard configuration and the data contained in it is not synchronized with the database on the Primary server.

You must complete a full Avaya Analytics™ install on the DR site. There are a number of configuration items that differ when you install Avaya Analytics™ on the DR site. For example, some of the parameters in the `parameters.conf` files must point to the “orclrcu” database. You must perform the following steps when installing Avaya Analytics™ on the DR site:

1. Install the Primary and Standby Oracle® Database.
2. When you install OBI, set the `OBI_DB_CONNECT_STRING` parameter in the `parameters.conf` file to point to “orclrcu”.
3. When you install ODI, set the `ODI_CONNECT_STRING` parameter and the `SERVICE_DB_URL` parameter in the `parameters.conf` file to point to “orclrcu”.
4. Do not install Avaya Analytics™ for Oracle® Database at the DR site.
5. When you install Avaya Analytics™ for OBI, set the `OBI_SHARED_DB_HOST` parameter in the `parameters.conf` file to the IP address of the Standby Oracle® Database.
6. Set the `OBI_SHARED_DB_SID` parameter in the `parameters.conf` file to point to “orcl”. This is the SID of the Standby Oracle® Database.
7. Ensure that the latest ODI patch is installed, and then do the following in the `parameters.conf` file:
 - a. Ensure that the following parameters are set to the correct instance names:
 - `ODI_DB_SID="orcl"`
 - `ODI_DB_RCU_SID="orclrcu"`
 - b. Update the `INSTALLATION_TYPE` parameter to match the type of installation being performed:
 - For the Data Guard Primary installation type, set the parameter to `PRIMARY`.
 - For the Data Guard Standby installation type, set the parameter to `STANDBY`.

The correct configuration of this parameter ensures that the appropriate instance names are set.
8. Set the `ODI_DB_HOST` parameter in the `parameters.conf` file to the IP address of the Standby Oracle® Database.
9. When you deploy Avaya Analytics™ Streams server, you must configure the Streams server to point at the Avaya Oceana® Solution at the DR site.
10. When you deploy Avaya Analytics™ for OSA, you must configure OSA to point at the Avaya Oceana® Solution at the DR site.

11. After you deploy the complete secondary solution deployed at the DR site, the Avaya Analytics™ Streams server can be running at the DR site. The OSA server and the OBI/ODI server must not be running at the site, until you need to failover. After the Standby Oracle® Database becomes the Primary server, start OSA and OBI/ODI. Once Avaya Analytics™ at the DR site is operational, you can use the Avaya Oceana® Solution at the DR site.
12. When you install the DR site, you must perform a Database Switchover. For more information, see *Switching over the dataguard database*.
13. After successful installation of the DR site, ensure that the ODI, OBIEE, and OSA processes on the DR site is stopped.
14. Perform a database switchover using **SWITCHOVER TO orcl_stby** to switch to your primary database. After successful installation of the DR site, you must switchover the databases to their original state. For more information, see *Step 5 of Switching over the dataguard database*.

 Important:

You must take the snapshots of DR databases only after shutting down the databases. Otherwise, the DR replication breaks while attempting to revert a snapshot.

Switching over the dataguard database

About this task

Use this procedure to switch over the primary dataguard database to the secondary dataguard database.

Procedure

1. SSH to your primary database as the oracle user.
2. To establish the connection, run the following command:

```
dgmgrl sys/<your_password>@orcl
```

Where <your_password> is the SYS user password created during the database installation.

3. Confirm that the connection is successful and then run the following command:

```
SHOW CONFIGURATION VERBOSE
```

The output must have configuration status as Success.

4. To switch over from the primary database to the secondary database, run the following command:

```
SWITCHOVER TO orcl_stby
```

After the switchover, the Standby database acts as a Primary database.

5. To switch over from the secondary database to the primary database:

- a. SSH to your primary database as the oracle user.
- b. To establish the connection, run the following command:

```
dgmgrl sys/<your_password>@orcl_stby
```

- c. Confirm that the connection is successful and then run the following command:

```
SWITCHOVER TO orclna
```

The databases come back to their original states.

For more information on Oracle® Database switchover testing, see *Avaya Oceana® Solution Disaster Recovery*.

Configuring the SNMP environment

This section describes how to configure your Avaya Analytics™ solution for SNMP. SNMP configuration is optional.

The Avaya Analytics™ Management Information Base (MIB) is available in the Avaya install directory.

Configuring the Server properties file

Procedure

1. On the OSA server, navigate to the `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/osa_domain/<osa_server>` and open the `server.properties` file.
2. You must set the following values to enable SNMP. The path locations to the Oracle® Database, ODI, OBI, and Streams server are the default paths. If your solution is configured with non-default paths, you must change them. The values that you must change are highlighted below.

```
server.properties on OSA #####
#SNMP Properties

#DB server
database.host.ip=127.0.0.1
database.host.ssh.user=oracle
database.host.ssh.password=oraclePwd
database.host.ssh.port=22
database.host.em.port=5500
database.parameters.encrypted=false
database.tns.log.location=/home/oracle/app/oracle/diag/tnslsnr/dbhostname/
listener/trace/
database.log.location=/home/oracle/app/oracle/diag/rdbms/orcl/orcl/trace/
database.log.fileName=alert_orcl.log
```

```

#ODI server
odi.host.ip=127.0.0.1
odi.host.ssh.port=22
odi.host.ssh.user=oracle
odi.host.ssh.password=oraclePwd
odi.host.studio.log.location=
odi.host.agent.log.location=/home/oracle/app/oracle/Oracle_Home_ODI_Standalone/
user_projects/domains/odistandaloneagent/system_components/ODI/OracleDIAgent1/
logs/oracledi/
odi.parameters.encrypted=false

#OBIEE server
obiee.host.ip=127.0.0.1
obiee.host.adminserver.port=9500
obiee.host.nodemanager.port=9506
obiee.host.analytics.port=9502

#STREAMS server
streams.host.ip=127.0.0.1
streams.host.ssh.port=22
streams.host.ssh.user=oracle
streams.host.ssh.password=oraclePwd
streams.host.em.log.location=/home/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/streams_domain/servers/AdminServer/sysman/log/
streams.host.composer.port=7003
streams.host.adminserver.port=7001
streams.host.nodemanager.port=5556
streams.parameters.encrypted=false

#OSA server
osa.host.ip=127.0.0.1
osa.wlevs.port=9002
osa.wlevs.user=wlevs
osa.wlevs.password=wlevsPwd
osa.parameters.encrypted=false

#SNMP destinations
trap.destination.host.ip=127.0.0.1
trap.destination.host.port=162

```

Enabling the Routing Service Groups feature

About this task

By default, the Routing Service Group feature is disabled for real-time reporting to avoid breaking existing installs on upgrade. However, if the service is required, you can use this procedure to enable the feature.

For more information on Routing Service Groups, see *Administering Avaya Workspaces for Oceana®*.

Procedure

1. On Analytics Stream Server, navigate to the websocket-sender location at `/home/oracle/openInterface/websocket-sender/`
2. To confirm that the websocket-sender process is running, run the `./psMe.sh` command.

3. **(Optional)** If the websocket-sender process is running, to stop the websocket-sender process, run the `./killMe.sh` command.
4. To edit the `application.properties` file, locate the property `OCEANA.websocketSender.enableRoutingServiceGroupFilter=false`, change the property to `OCEANA.websocketSender.enableRoutingServiceGroupFilter=true`, and save the file.
5. To start the websocket-sender, run the `./startMe.sh` command.

Chapter 6: Upgrading

Upgrading Avaya Analytics™

This chapter describes how to upgrade to Avaya Analytics™ 3.6.1. Avaya Analytics™ 3.6.1 supports the following upgrade scenarios:

- Avaya Analytics™ 3.4.x to Avaya Analytics™ 3.6.1
- Avaya Analytics™ 3.5.x to Avaya Analytics™ 3.6.1

From Avaya Analytics™ 3.5, the Oracle Business Activity Monitor (BAM) server is replaced by the Avaya Analytics™ Streams server. If you are upgrading from Avaya Analytics™ 3.4.x, you must install the Avaya Analytics™ Streams server on a server with a newly installed operating system. For example, if you want to install the Avaya Analytics™ Streams server on the old Oracle® BAM server, you must install a new operating system first.

You can use the procedures in this chapter to upgrade from Avaya Analytics™ 3.4.x or 3.5.x to Avaya Analytics™ 3.6.1.

The following steps outline the procedure to upgrade your solution from Avaya Analytics™ 3.4.x to Avaya Analytics™ 3.6.1.

1. Uninstall the Oceana Input Adapter application from OSA.
See [Uninstalling the Oceana Input Adapter application from OSA](#) on page 119.
2. Stop the OSA process.
See [Stopping the OSA process](#) on page 120.
3. Remove OSART from the existing Oracle® Stream Analytics server.
See [Removing OSART from the existing Oracle® Stream Analytics server](#) on page 121.
4. Upgrade the OBI server. See [Upgrading the OBI server](#) on page 122.
5. Install the Avaya Analytics™ Streams server.
See [Installing Streams server software](#) on page 57 and [Installing Avaya Analytics Streams server](#) on page 82.
6. Install the most recent Avaya Analytics™ software using the procedures described in this guide.

The following steps outline the procedure to upgrade your solution from Avaya Analytics™ 3.5.x to Avaya Analytics™ 3.6.1.

1. Uninstall the Oceana Input Adapter application from OSA.

See [Uninstalling the Oceana Input Adapter application from OSA](#) on page 119.

2. Stop the OSA process.

See [Stopping the OSA process](#) on page 120.

3. Install the most recent Avaya Analytics™ software using the procedures described in this guide.

You do not need to install any Oracle software to upgrade from Avaya Analytics™ 3.5.x to Avaya Analytics™ 3.6.1.

 Note:

If you upgrade from Avaya Analytics™ 3.4.x or 3.5.1 to Avaya Analytics™ 3.6.1, you must install additional Oracle patches. The Avaya Analytics™ 3.6.1 install scripts automatically install the patches at the end of the Avaya Analytics™ software installation. For Oracle® RAC Database and Oracle Data Guard installations, patches are not automatically installed. You must refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

While performing Avaya Analytics™ 3.5.0.1 to Avaya Analytics™ 3.6.1 update of OSA, the `server.properties` file is preserved. If you change the IP address of Avaya Breeze® platform node or other server in the `parameters.conf` file, then the new changes is not written to OSA during update. To reflect these changes in OSA, you must delete the `server.properties` file from OSA and update `server.properties.vanilla` file in the build directory with the new settings. The install then creates a new `server.properties` file with the new settings populated from the `server.properties.vanilla` file.

Before upgrading Avaya Analytics™ Streams server, take a back up of the security certificates on the Avaya Analytics™ Streams server to a directory outside of the OpenInterface directory. For example, copy the authenticationService and Spring Security certificates to the `home/oracle/ssl` directory.

Uninstalling the Oceana Input Adapter application from OSA

About this task

If you are upgrading to Avaya Analytics™ 3.6.1 from a previous release, you must uninstall the Oceana Input Adapter application from OSA before upgrading. This stops Avaya Analytics™ receiving events from Avaya Oceana® Solution during the upgrade process.

For OSA High Availability (HA) deployments, perform these steps on both OSA servers.

Procedure

1. Login to `http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/`.
The default user name is `wlevs` and the default password is `Admin123`.
2. Click **osadomain > Deployment**.
3. From the list of deployed applications, select **OceanalInputAdptor.ReflInputAdaptor**.
4. Click **Uninstall**.

Stopping the OSA process

About this task

If you upgrade Avaya Analytics™ to 3.6.1, you must stop the OSA process before upgrading. Stopping the OSA process prevents Avaya Analytics™ from receiving the events from Avaya Oceana® Solution during the upgrade process.

For OSA High Availability (HA) deployments, you must follow these steps, first on the standby OSA server, then on the primary OSA server.

Procedure

1. Using an SSH client, connect to the OSA server.
2. Run the following command to stop the OS process:

```
killall -9 -f wlevs
```

Uninstalling the Agent by Auxcode applications from OSA

About this task

If you are upgrading to Avaya Analytics™ 3.6.1 from a previous release, you must uninstall the Agent by Auxcode Start of Day and Moving Window applications from OSA before upgrading.

Procedure

1. Login to `http://<PRIMARY_OSA_SERVER_IP>:9002/wlevs/`.
The default user name is `wlevs` and the default password is `Admin123`.
2. Click **osadomain > Deployment**.
3. From the list of deployed applications, select **agentbyauxcode.AgentByAuxcode**.
4. Click **Uninstall**.
5. From the list of deployed applications, select **agentbyauxcodemovingwindow.AgentByAuxcodeMeasures**.

6. Click **Uninstall**.

Removing OSART from the existing Oracle® Stream Analytics server

About this task

If you are upgrading to Avaya Analytics™ 3.6.1 from 3.4, you must first remove OSART from the existing OSA server. From Avaya Analytics™ 3.5, the functionality previously provided by OSART is provided by the Avaya Analytics™ Streams server.

Use the Oracle user account to perform this procedure.

Procedure

1. Navigate to the `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/osadomainRT/osaserverRT` directory.
2. Stop OSART using the following command:
`./stopwlevs.sh`
3. Confirm OSART is stopped using the following command:
`ps -ef | grep wlevs`
4. Navigate to the `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains` directory.
5. Use the `ls` command to list the directories in this location.
6. Remove the `osadomainRT` directory using the following command:
`rm -rf osadomainRT/`

OBI server upgrade

Pre-upgrade steps for OBI

About this task

Perform the following steps before the OBI server upgrade to ensure that supervisor permissions are retained after upgrade, and that they can successfully log on to OBI analytics. Roles are not automatically retained after the upgrade.

Procedure

1. Run the following command from the `/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bitools/bin` directory to stop OBI services:
`./stop.sh`
2. Create the following directories:
 - `/home/oracle/workDir`
 - `/home/oracle/exportDir`
3. Run the following command from the `/home/oracle/Oracle/Middleware/Oracle_Home/oracle_common/common/bin` directory:
`./wlst.sh`
4. Run the following command:

```
exportServiceInstance('/home/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/bi','ssi','/home/oracle/workDir','/home/
oracle/exportDir','','','false','Admin01$')
```
5. Run the following command from the `/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bitools/bin` directory to start OBI services:
`./start.sh`
6. Save the newly created `ssi.bar` file from the `/home/oracle/exportDir` directory to a local location. This is the original version of the `ssi.bar` file.
7. In your web browser, open the following URL to start Weblogic Console: `http://<OBI_SERVER_IP>:9500/console`
8. In the left pane, navigate to **<WegLogic domain> > myrealm > Migration > Export**.
 A “user_export” directory is created in the WebLogic domain. The data is exported to this directory.
9. Type the file system path in the **Export Directory on Server** box, and click **Save**.
 This creates 5 .DAT files containing all of the information from the local myrealm.
10. Save the “user_export” directory to a local location.

Upgrading the OBI server

About this task

Use the following procedure to upgrade the OBI server for Avaya Analytics™ 3.6.1. Avaya Analytics™ 3.6.1, supports OBI version 12.2.1.3.0. You must uninstall the older version of OBI before you install version 12.2.1.3.0.

Before you begin

- Stop Avaya Analytics™ services on all servers in the solution, except for the Oracle® Database server.

Procedure

1. Unzip the `obiee.zip` file from the `AvayaAnalytics_x.x.x.x_Build_xx.zip` file to the `/var/tmp/Analytics/` directory.
2. Update the required parameters in the `parameters.conf` file to match the new install. For more information about the parameters to update, see [Installing Oracle Business Intelligence](#) on page 52.
3. From the `/var/tmp/Analytics/obiee` directory, make the following script executable and run the following command:


```
sh oracle_obiee_uninstall.sh
```
4. Install the new version of OBI server. For more information about installing OBI server, see [Installing Oracle Business Intelligence](#) on page 52 and [Installing Avaya Analytics for Oracle® Business Intelligence and Oracle® Data Integrator](#) on page 67.

Next steps

Install the Avaya Analytics™ Streams server. See [Installing Streams server software](#) on page 57 and [Installing Avaya Analytics Streams server](#) on page 82.

Post-upgrade steps for OBI

About this task

Perform the following steps after the OBI server upgrade to ensure that supervisor permissions are retained after upgrade, and that they can successfully log on to OBI analytics. Roles are not automatically retained after the upgrade.

Procedure

1. Run the following command from the `/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bitools/bin` directory to stop OBI services:


```
./stop.sh
```
2. Create the following directories:
 - `/home/oracle/workDir`
 - `/home/oracle/exportDir`
3. Run the following command from the `/home/oracle/Oracle/Middleware/Oracle_Home/oracle_common/common/bin` directory:


```
./wlst.sh
```
4. Run the following command:

```
exportServiceInstance('/home/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/bi','ssi','/home/oracle/workDir','/home/
oracle/exportDir','','',false,'Admin01$')
```

5. Run the following command from the `/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bitools/bin` directory to start OBI services:


```
./start.sh
```
6. Save the newly created `ssi.bar` file from the `/home/oracle/exportDir` directory to a local location. This is the new version of the `ssi.bar` file.
7. Copy the “user_export” directory you exported before the upgrade to the new WebLogic domain. Change the directory ownership and file permissions as required for the new domain.
8. In your web browser, open the following URL to start WebLogic Console: `http://<OBI_SERVER_IP>:9500/console`
9. In the left pane, navigate to **<WegLogic domain> > myrealm > Migration > Import**.
10. Type the file path to the “user_export” directory you exported before the upgrade that you now want to import to the new domain, and click **Save**.
11. Modify the security content of the new `ssi.bar` file:
 - a. Using a file archiver utility such as 7-zip, open the new version and the old version of the `ssi.bar/authmodel/jazn/jazn-data.xml` file.
 - b. Replace all of the content in the new version of the `ssi.bar/authmodel/jazn/jazn-data.xml` file with the content from the old file, and save your changes.
12. Copy the newly edited version of the new `ssi.bar` file from the local location to a location on your OBI server. For example, copy the file to `/home/oracle/Downloads/BAR/`
13. Ensure that all OBI services are stopped.
14. Run the following command from the `/home/oracle/Oracle/Middleware/Oracle_Home/oracle_common/common/bin` directory:


```
./wlst.sh
```
15. Run the following command:


```
importServiceInstance('/home/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/bi','ssi','/home/oracle/Downloads/BAR/
ssi.bar',true,true,true,'Admin01$')
```
16. Run the following command from the `/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bitools/bin` directory to start OBI services:


```
./start.sh
```

Oracle® Database Data Guard upgrade

This section describes how to convert an existing standalone Oracle® Database to a Primary Oracle® Database for use in an Oracle Data Guard configuration. After you upgrade your standalone Oracle® Database to a Primary Oracle® Database, you must deploy a Standby Oracle® Database to complete Oracle Data Guard configuration.

Upgrading a standalone Oracle® Database to a Primary server installation

About this task

Use this procedure to upgrade an existing standalone Single Instance of Oracle® Database to a Primary server installation in an Oracle Data Guard configuration.

The following table lists the requirements for Primary Oracle® Database upgrade:

Requirement	Description
Java	jdk1.8.x.x.x
DB installation scripts	db.zip
Oracle® Database patches	Refer to the Avaya Analytics™ Release Notes for additional information about patches that are specific to your release.

Procedure

1. Unzip the Avaya Deployments zip file.

The `db.zip` file is available in the `Oracle_Installers/Nodal` folder.

2. Copy the `db.zip` file to the database server using an scp or ftp tool.
3. SSH to the database server as the root user.
4. Create the `/var/tmp/Analytics/` directory.
5. Run the following command to unzip the `db.zip` file to the `/var/tmp/Analytics` directory:

```
unzip -d /var/tmp/Analytics db.zip
```

Example of the directory structure contents:

- `/var/tmp/Analytics/parameters.conf`

6. Make the following changes to the `/var/tmp/Analytics/parameters.conf` file based on the information relevant to your server:

```
#### SYSTEM common settings ####
DOMAIN=domain.com           #CHANGE THIS TO THE DOMAIN NAME ONLY I.E
DOMAIN.COM
NTP_HOST=127.0.0.1          #CHANGE THIS TO THE NTP IP OR HOSTNAME IF NTP
NOT_ALREADY_CONFIGURED
JAVA_HOME=/usr/java/latest  #CHANGE THIS TO POINT AT THE JAVA HOME LOCATION
```

```

#### Oracle DB Parameters ####
DB_HOSTNAME=localhost                #CHANGE THIS TO THE HOSTNAME
ONLY (NOT THE FQDN)
DB_HOST_IP_ADDR=127.0.0.1            #CHANGE THIS TO THE IP OF
YOUR SERVER
DB_LISTENER_PORT=1521
#CHANGE THIS TO LISTENER PORT OF YOUR DATABASE
DB_NAMESERVER=127.0.0.1              #CHANGE THIS TO THE IP/
HOSTNAME OF YOUR DNS SERVER

#### Oracle Data Guard Parameters
DB_PRIMARY_HOST_IP_ADDR=127.0.0.1    #CHANGE THIS TO THE IP OF
YOUR PRIMARY SERVER
DB_PRIMARY_LISTENER_PORT=1521        #CHANGE THIS
TO THE PORT OF YOUR PRIMARY SERVER

#### This variable is required to set the type of installation STANDALONE,
PRIMARY or STANDBY
#### STANDALONE - Installation standalone DB on server (no Data Guard, no RAC)
#### PRIMARY - Installation PRIMARY DB on server for Data Guard setup
#### STANDBY - Installation STANDBY DB on server for Data Guard setup
ORACLE_DB_INSTALLATION_TYPE=PRIMARY #YOU MUST ENSURE THIS IS SET TO PRIMARY

#### This variable is only used when upgrading STANDALONE to PRIMARY Data Guard
(YES/NO)
ORACLE_DATAGUARD_UPGRADE=YES         #YOU MUST ENSURE THIS IS SET TO YES

```

7. Run the following commands to change the permission and owner of all installation files to the Oracle user previously configured through the `root.sh` script:

- `chmod 755 -Rf /var/tmp/Analytics/*`
- `chown -Rf oracle:oinstall /var/tmp/Analytics/*`

8. From the `/var/tmp/Analytics/db` directory, run the following command as the root user to begin the installation process:

```
sh oracle_db_install.sh
```

You must confirm that you have edited the `parameters.conf` file, and you must enter the Oracle user password during the installation.

9. After successful installation, review the output of the script to ensure that no failures or errors occurred during the installation process.

Next steps

Install the Standby Oracle® Database to complete Oracle Data Guard configuration. For more information about installing the Standby Oracle® Database, see [Installing Standby Oracle® Database](#) on page 35.

Database backup and restore

The Avaya Analytics™ solution uses Oracle® Data Pump to backup and restore from the Avaya Analytics™ database schemas.

Oracle® Data Pump technology enables very high-speed movement of data and metadata from one database to another. Oracle® Data Pump includes three parts:

- Command-line clients: expdp and impdp.
- The DBMS_DATAPUMP PL/SQL package (also known as the Data Pump API)
- The DBMS_METADATA PL/SQL package (also known as the Metadata API)

The expdp and impdp clients start the Data Pump Export utility and Data Pump Import utility. Avaya Analytics™ uses these utilities to backup and restore data.

The Avaya Analytics™ database contains the following database schemas: gila_stage and oceana_datamart. You must backup and restore each of these schemas separately, and you must back up the schemas in the following order:

1. oceana_datamart
2. gila_stage

! Important:

You must restore the database schemas in reverse order.

If you are backing up and restoring large databases, the process can take several hours.

Avaya recommends that you perform regular database backups. Regular backups allow you to recover from events such as data loss and damage due to disk failures and power outages.

Prerequisites

Procedure

- When you use expdp or impdp you must provide user credentials for connecting to the Oracle database. This user must be a member of the DBA role.

! Important:

Do not connect to the Oracle database as the SYSDBA user.

- Oracle® Data Pump reads and writes to the directory specified by the "DATA_PUMP_DIR" database parameter. Obtain this directory using the following query:

```
SELECT DIRECTORY_PATH FROM dba_directories WHERE
DIRECTORY_NAME='DATA_PUMP_DIR';
```

You must run the command as a user who is a member of the DBA role.

Backing up Avaya Analytics™ database schemas

Before you begin

Review Oracle documentation for full details about backing up the Oracle database.

About this task

You back up the database schemas using expdp. This involves passing a number of parameters to expdp, which the example below describes. This example procedure demonstrates how to back up the oceana_datamart schema.

! Important:

- Database backups using expdp must be performed during a scheduled maintenance window. You must stop all database updates while using expdp.
- The expdp command uses the “flashback_time” parameter to maintain data consistency for the backup set. Only data committed prior to the flash back time is included in the export. If the OSA server and ODI Agent are running while the export is taking place, rows inserted while the export is running are not backed up. This data is included the next time a backup is performed.

Database backups using expdp must be performed during a scheduled maintenance window. You must stop all database updates while using expdp.

Procedure

Run the expdp command. Ensure you pass the required parameters for the backup. For example:

```
expdp system/systempassword SCHEMAS="oceana_datamart"
DUMPFILE="oceana_datamart_export.dmp" REUSE_DUMPFILES='Y'
FLASHBACK_TIME=systimestamp CONTENT="ALL"
```

Example

For Avaya Analytics™ database backups, you can use the following parameters:

Parameter	Description
dbuser	The name of the oracle database user running the export.
dbuserpassword	The password associated with the dbuser.
schemas	A comma separated list of schemas to be exported. You can export gila_stage or oceana_datamart.
dumpfile	The name of the file to which data is exported.
reuse_dumpfiles	This is a flag which specifies whether dump files can be overwritten if they exist. Type Y or N.
content	This controls which information is exported. Type ALL for this procedure.
flashback_time	This parameter ensures the backup is consistent. It specifies the timestamp to which the data is frozen.

Restoring Avaya Analytics™ database schemas

Before you begin

- Review Oracle documentation for full details about restoring the Oracle database.
- Stop all OSA applications and ODI Agent.

- For each schema you want to restore, connect to the Oracle database and delete the user associated with the schema.
- For each schema you want to restore, copy the previously exported dumpfile to the Oracle® Data Pump directory. See [Backing up Avaya Analytics database schemas](#) on page 127.

About this task

You restore the database schemas using impdp. This involves passing a number of parameters to impdp, which the example below describes. This example procedure demonstrates how to restore the oceana_datamart schema.

Procedure

Run the impdp command. Ensure you pass the required parameters for the restore. For example:

```
impdp system/systempassword schemas="oceana_datamart"
dumpfile="oceana_datamart_export.dmp" CONTENT="ALL"
```

Example

For Avaya Analytics™ database restores, you can use the following parameters:

Parameter	Description
dbuser	The name of the oracle database user running the import.
dbuserpassword	The password associated with the dbuser.
schemas	A comma separated list of schemas to be imported. You can import gila_stage or oceana_datamart.
dumpfile	The name of the file to which data is imported.
content	This controls which information is exported. Type ALL for this procedure.

Next steps

Start all OSA applications and ODI Agent.

Backup and Restore of Oracle® Business Intelligence reports

Creating a new folder in OBIEE

About this task

When you create customized artifacts such as Filters, Dashboards, and Analysis in OBIEE, you must store them in a new folder in the `Shared Folders` directory. If you do not store custom created reports in a custom folder, you must archive each artifact individually.

Procedure

1. Log in to OBIEE using your user ID and password.
2. On the OBIEE Home page, click **Catalog**.
3. In the Folders pane, expand and select the `Shared Folders` directory.
4. On the toolbar, click the **New Folder** icon.
5. In the New Folder dialog box, enter an appropriate name for the folder.

All customized artifacts are stored in the new folder. You can also create subfolders for different artifact types, such as Filters, Prompts, Dashboards, and Analysis.

6. Click **OK**.

Editing a dashboard for custom artifacts

About this task

If you have custom artifacts that are not in their own custom folder, you must create a new folder in OBIEE and then drag your custom artifacts to the new custom folder. After dragging the custom artifacts, use this procedure to edit the dashboard.

Procedure

1. Log in to OBIEE using your user ID and password.
2. Edit your dashboard and identify the component with a warning symbol.
The warning symbol indicates that the component cannot be found.
3. Remove the component.
4. From the new folder that you created, drag the same component and drop it to the same place from which it was removed.
5. Save the changes and ensure that the warning symbol has disappeared.

Note:

To list a report under **Dashboards**, you must store the dashboard in a folder with the extension `_portal`. This is the reason why all dashboards in the `Dashboards` folder are stored at `/shared/Oceana Reporting & Analytics/_portal`.

Taking a backup of custom artifacts

Procedure

1. Log in to OBIEE using your user ID and password.
2. On the OBIEE Home page, click **Catalog**.
3. In the Folders pane, expand the `Shared Folders` directory.

4. Select the custom folder containing the artifacts for which you want to take a backup.
5. In the Tasks pane, click **Archive**.
6. In the Archive dialog box, select the **Keep Permissions** check box.
7. Click **OK**.

The system displays a dialog box to select where to store the catalog backup.

8. Click **Save As** to save the backup to a local folder.

Restoring custom artifacts

Procedure

1. Log in to OBIEE using your user ID and password.
2. On the OBIEE Home page, click **Catalog**.
3. In the Folders pane, expand and select the `Shared Folders` directory.
4. In the Tasks pane, click **Unarchive**.
5. In the Unarchive dialog box, perform the following steps:
 - a. In the **Archive file** field, browse and select the catalog backup that you want to restore.
 - b. In the **Replace** field, select one of the following options:
 - **All**: Replaces existing folders or objects with the same names as the folders or objects included in the archive file that you upload.
 - **Old**: Replaces folders or objects except the folders or objects that exist, unless they are older than the source.
 - **None**: Adds new folders or objects and preserves existing folders or objects.
 - **Force**: Adds and replaces all folders or objects.
 - c. In the **ACL** field, select one of the following options:
 - **Inherit**: Inherits the folder or object's permissions (ACL) from its new parent folder.
 - **Preserve**: Preserves the folder or object's permissions (ACL) as in the original, mapping accounts.
 - **Create**: Preserves the folder or object's permissions (ACL) as in the original, creating and mapping accounts.
6. Click **OK**.

Next steps

The paths do not change dynamically, so if the referenced analyses cannot find the correct path it cannot display the dashboard. To resolve this issue, you must drag the analysis into the dashboard from the shared folder, and remove the previous analyses.

Chapter 7: Documentation

Title	Use this document to:	Audience
Overview		
<i>Avaya Oceana® Solution Description</i>	Know about tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales Engineers • Business Partners • Solution Architects • Implementation Engineers
Implementing		
<i>Deploying Avaya Oceana® Solution</i>	Deploy and configure Avaya Oceana® Solution.	• Solution Architects • Implementation Engineers
<i>Deploying Avaya Workspaces for Oceana®</i>	Deploy and configure Avaya Workspaces.	• Solution Architects • Implementation Engineers
<i>Deploying Avaya Analytics™ for Oceana®</i>	Deploy and configure Avaya Analytics™.	• Solution Architects • Implementation Engineers
<i>Avaya Oceana® Solution Disaster Recovery</i>	Configure Avaya Oceana® Solution for disaster recovery.	• Solution Architects • Implementation Engineers
<i>Deploying Avaya Oceana® Solution on Amazon Web Services</i>	Deploy and configure Avaya Oceana® Solution and Avaya Analytics™ in an Amazon Web Services (AWS) environment.	• Solution Architects • Implementation Engineers
Administering		
<i>Administering Avaya Workspaces</i>	Administer Avaya Workspaces.	• Administrators • Solution Architects • Implementation Engineers
Using		
<i>Using Avaya Workspaces</i>	Use Avaya Workspaces.	Supervisors
<i>Avaya Analytics™ Data Dictionary</i>	Use historical and real-time measures in custom reports.	• Administrators • Report designer
Troubleshooting		

Table continues...

Title	Use this document to:	Audience
<i>Troubleshooting Avaya Oceana® Solution</i>	Troubleshoot issues related to Avaya Oceana® Solution.	• Administrators • Solution Architects
<i>Maintaining and Troubleshooting Avaya Analytics™ for Oceana®</i>	Troubleshoot Oracle and report issues.	• Administrators • Solution Architects • Report designer

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.

7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at <https://documentation.avaya.com>.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
 - Type a keyword in the **Search** field.
 - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.

- Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **My Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
 - Add content from various documents to a collection.
 - Save a PDF of selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

Navigate to the **My Content > Watch list** menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

 Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Chapter 8: Training

The following courses are available for the Avaya Oceana® Solution program.

Course code	Course title	Delivery Type
Fundamental - Technical Delta Courses		
21160W	Avaya Oceana® Fundamentals	Web-based Training
21140W	Avaya Oceana® and Avaya Analytics™ R 3.6 Technical Delta	Web-based Training
Implementation Courses		
74150V	Integrating Avaya Oceana®	Virtual Instructor-Led Training
74550V	Supporting Avaya Oceana®	Virtual Instructor-Led Training
74350V	Integrating and Supporting Avaya Analytics™ for Avaya Oceana®	Virtual Instructor-Led Training
Administration Courses		
24320W	Administering Avaya Oceana® Basics	Web-based Training
24300V	Administering Avaya Oceana® Channels	Virtual Instructor-Led Training
24310W	Administering Avaya Analytics™ for Avaya Oceana®	Web-based Training
End User Courses		
24020W	Using Avaya Oceana® Workspaces for Agents	Web-based Training
24040W	Using Avaya Oceana® Workspaces for Supervisors	Web-based Training
Developer Courses		
24100W	Developing Customer Applications for Avaya Oceana®	Web-based Training
24150W	24150W - Customizing the Avaya Workspaces® Framework	Web-based Training
Design Courses		
34200W	Avaya Oceana® Solutions Design Fundamentals	Web-based Training
34800W	Designing the Avaya Oceana® Solution	Web-based Training
Sales Courses		
41410W	Selling Avaya Oceana®	Web-based Training

Table continues...

Course code	Course title	Delivery Type
41490W	What's New for Sales: Avaya Oceana®	Web-based Training
41480W	The Basics of Cost Justification and Selling Oceana Using the Oceana ROI Tool	Web-based Training
41400W	Selling Avaya Analytics™ Strategy and Positioning Overview	Web-based Training
41020W	Avaya Oceana and Analytics Solutions Product Information Documents (Sales)	Web-based Training
4785W	Avaya Oceana Remote Agent Solution	Web-based Training
4789W	Avaya Oceana: The Customer Experience	Web-based Training
4794W	Avaya Oceana: The Agent Experience	Web-based Training
4795W	Avaya Oceana: The Management Experience	Web-based Training
4877W	Avaya Oceana Solution for Financial Services: Car Loan Use Case	Web-based Training

Chapter 9: Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <http://www.avaya.com/support>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
The system displays the Avaya Support page.
3. Click **Support by Product > Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

A

application properties	
Kafka	91
REST	91
websocket-sender	91
AuthorizationService information	
obtaining	85
auto-start of services	
checking configuration	97
Avaya Analytics™ overview	10
Avaya branding	73
Avaya support website support	137

B

backup custom artifacts	130
-------------------------------	---------------------

C

changes in this release	9
collection	
delete	133
edit name	133
generating PDF	133
sharing content	133
configure	
Server properties file	115
content	
publishing PDF output	133
searching	133
sharing	133
watching for updates	133
convert standalone Oracle® Database	
Data Guard	125
CSV files	
historical reports	112
customer responsibilities	8

D

database backup	126 , 127
database restore	126 , 128
dataguard database	
switch over	114
deployment architecture	12
deployment process	15
disabling	85
disaster recovery	113
disk	18
disk partitions	20
documentation portal	133

documentation portal (<i>continued</i>)	
finding content	133
navigation	133

E

edit	
dashboard	130
enabling	
Routing Service Groups	116

F

failover	
testing	48
finding content on documentation portal	133

H

hardware	18
HTTPS	
OBIEE	68

I

InSite Knowledge Base	137
install	
Oracle Stream Analytics	59
patches	61
installing	30 , 32 , 35
Oracle® Business Intelligence	52
Oracle® Data Integrator	54
installing Avaya Analytics™	63 , 82
installing steps	57
intended audience	8

J

JMS install verification	83
JVM heap size	
modifying	111
JVM settings	94

K

Kafka install verification	84
----------------------------------	--------------------

L

licensing	
Oracle Restricted Use License	8

limitations	73	RAC install	39
M		RAC install test	46
maintenance test		redis install verification	84
broker	28	related documentation	132
memory	18	Reliable Eventing group	
My Docs	133	creating	26
O		Reliable Eventing groups	26
OBI	65	Reliable Eventing status	28
post-upgrade steps	123	restore custom artifacts	131
pre-upgrade steps	121	RHEL partitioning	20
OBIEE, weblogic server	76	RPM	21
OBI server		S	
upgrade	122	searching for content	133
ODI	65	security certificates	
OPatch	21	Streams	85
openInterface install verification	84	sharing content	133
Oracle® Business Intelligence and Oracle® Data Integrator		SNMP environment	
.....	67 , 74	configuring	115
Oracle® Database	62 , 63	SSL	76 , 97
Oracle® Stream Analytics	109 , 110	standalone Oracle® Database	30
Oracle components		standalone Oracle® Database upgrade	
installing	29	Data Guard	125
Oracle RAC DB		standby Oracle® Database	35
installing	39	startup	
Oracle Restricted Use License	8	kafka	96
OSART		REST	96
removing	121	websocket-sender	96
upgrade	121	stopping	
P		OSA process	120
patching	21	stream server, weblogic	97
planning tasks	25	Streams server	81 , 82
Port 7001	85	Streams server software	57
post installation checks	110	support	137
Oracle® Business Intelligence	53	supported configurations	11
Oracle® Database	32 , 35	T	
Oracle® Stream Analytics	61	testing failovers	48
standby Oracle® Database	38	training	135
post installing checks	74	U	
pre-installation steps	81	upgrade	
pre installing steps	62 , 65	Avaya Analytics™	118
prerequisites	29	V	
primary Oracle® Database	32	vCPU	18
R		VMware configuration	25
RAC		W	
post install check	46	watch list	133
RAC DB		websocket-sender install verification	84
starting	50		
stopping	49		

Y

yum repository [21](#)