Deploying Avaya OneCloud CPaaS Enabled Avaya Breeze Platform

Release 3.7
Issue 1
December 2019

© 2017-2019, Avaya Inc.
All Rights Reserved.

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 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, 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 types

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.

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.

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.

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).

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.

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.

Contents

Chapter 1: Introduction ... 6
Purpose ... 6
Chapter 2: Avaya One Cloud CPaaS Avaya Breeze platform Overview ... 7
Overview ... 7
Components ... 8
Topology ... 8
Standalone configuration call flow examples ... 10
Intermingled configuration call flow example ... 11
Chapter 3: Planning ... 12
Key customer configuration information ... 12
Chapter 4: Deployment process ... 13
Prerequisites ... 13
Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform deployment checklist ... 13
Chapter 5: Avaya OneCloud CPaaS account configuration ... 15
Configuring the Avaya OneCloud™ CPaaS account ... 15
Chapter 6: System Manager administration ... 17
Avaya Breeze® platform deployment ... 17
Loading the Zang Call Connector snap-in ... 17
Installing the Zang Call Connector snap-in ... 18
Configuring Zang Call Connector attributes ... 18
Routing inbound calls ... 19
Routing outbound calls to Avaya OneCloud™ CPaaS ... 20
Chapter 7: Engagement Designer administration ... 21
Administering Engagement Designer ... 21
Chapter 8: Session Border Controller administration ... 23
Administering Avaya Aura® Session Border Controller ... 23
Chapter 9: Troubleshooting ... 26
Troubleshooting call failure ... 26
Checking log files ... 26
Workflow or snap-in is not invoked ... 27
Media APIs do not function as expected ... 27
Installing certificates for HTTPS connections to Avaya OneCloud™ CPaaS ... 28
Chapter 10: Resources ... 30
Documentation ... 30
Finding documents on the Avaya Support website ... 32
Avaya Documentation Portal navigation ... 33
Training ... 34
Support ... 35

Chapter 1: Introduction

Purpose

The document describes how to deploy Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform. It describes:

- Component requirements for different system configurations
- Basic call flows
- The differences between Avaya OneCloud™ CPaaS calls and traditional Avaya Breeze® platform SIP calls
- Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform deployment and configuration steps
- Troubleshooting a Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform deployment

This document is intended for people who install and configure Avaya Breeze® platform at a customer site.

Chapter 2: Avaya One Cloud CPaaS Avaya Breeze platform Overview

Overview

Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform description

Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform allows snap-ins and workflows to leverage the Avaya Breeze® platform Call and Media API while using Avaya OneCloud™ CPaaS for call processing rather than SIP. The Zang Call Connector snap-in facilitates communication between Avaya OneCloud™ CPaaS and Avaya Breeze® platform. Avaya OneCloud™ CPaaS and Avaya Breeze® platform communicate using HTTPS. There are two deployment configurations:

- Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform standalone configuration. There is no SIP signaling. Avaya Aura® Session Border Controller and Avaya Aura® Session Manager are not required in this configuration.
- Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform intermingled configuration. Avaya Aura® Session Border Controller and Avaya Aura® Session Manager are required for SIP signaling. SIP signaling allows for the transfer of snap-in specific information.

A single Avaya Breeze® platform instance can process either traditional SIP calls exclusively or Avaya OneCloud™ CPaaS calls exclusively. It cannot process both types of calls.

Avaya OneCloud™ CPaaS call restrictions

Compared to traditional SIP calls, Avaya OneCloud™ CPaaS calls have the following limitations:

- Sequential forking is not supported – A snap-in cannot drop a called party and then add a different party in its place.
- Parallel forking is not supported – A snap-in cannot alert multiple called parties simultaneously.
- The 2–party make call API is not supported.
- There is a restriction on the source URI schemes used for a play or a prompt & collect operation. The two schemes supported are http:// and https:// (cstore:// and file:/// are not supported).

  When providing Avaya OneCloud™ CPaaS with a media URI, it must be able to access the URIs to retrieve the media files. This can be accomplished by, for example, placing the media file on your web server. If the media file resides on Avaya Breeze® platform, your network configuration must allow an incoming http(s) request to access the file.
- Recording a call and sending digits to a call are not supported.

- When two parties are on a call, no further media operations are supported.

For more information about which APIs are supported, see the Avaya Breeze® platform SDK Javadoc.

Call Deflection sample snap-in

The Call Deflection sample snap-in is an example of how to write a Java snap-in for use with Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform. The snap-in and associated documentation are in the Avaya Breeze® platform SDK.

Components

Standalone configuration

- Avaya OneCloud™ CPaaS – Processes the media portion of the call.
- Avaya Breeze® platform, release 3.7 – Executes traditional and Avaya Engagement Designer snap-ins.
- Avaya Aura® System Manager, release 8.1.1 – Used to administer the Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform environment.

Intermingled configuration

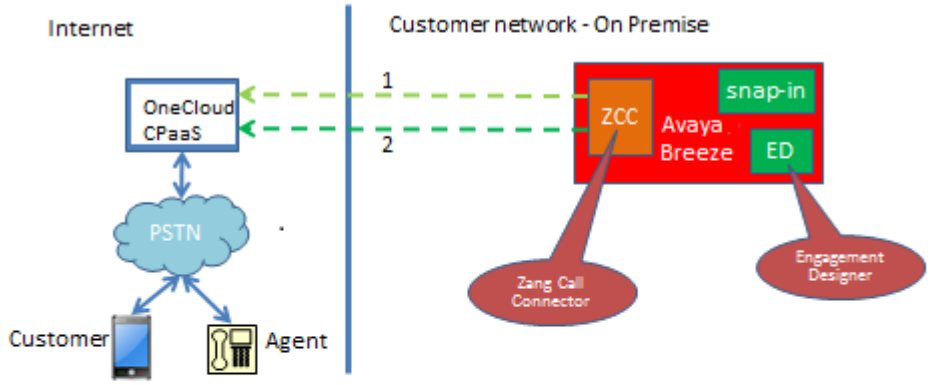
- Avaya OneCloud™ CPaaS – Processes the media portion of the call.
- Avaya Breeze® platform, release 3.7 – Executes traditional and Avaya Engagement Designer snap-ins.
- Avaya Aura® System Manager, release 8.1.1 – Used to administer the Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform environment.
- Avaya Aura® Session Manager, releases 6.3.8, 6.3.9, 7.0, 7.0.1, 7.1, 8.0 and later releases.
- Avaya Aura® Session Border Controller, release 7.1 and later releases.
- Avaya Aura® Communication Manager, release 6.3.17 and later releases.

Topology

Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform can be deployed in either of two configurations.

Standalone configuration

With the standalone configuration there is no SIP signaling. Therefore Avaya Aura® Session Manager and Avaya Aura® Session Border Controller are not required.



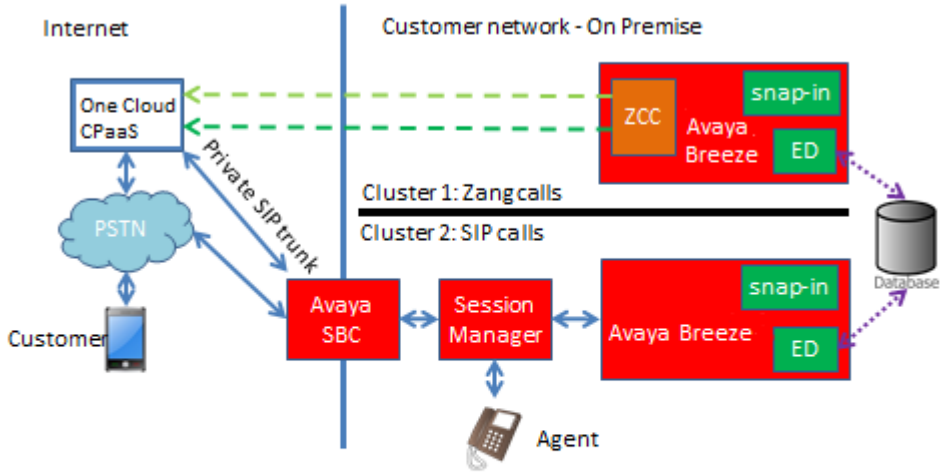
The two arrows, labeled 1 and 2, illustrate the two types of connections used by the Zang Call Connector (ZCC) to either send information to Avaya OneCloud™ CPaaS or receive information from Avaya OneCloud™ CPaaS. The Zang Call Connector uses HTTPS to send (POST) information to Avaya OneCloud™ CPaaS, and it uses HTTPS (GET) long-polling to receive information from Avaya OneCloud™ CPaaS. The long-polling construct removes the need to open special ports, or in other ways adjust your network to handle incoming information from Avaya OneCloud™ CPaaS conveyed in HTTPS POST requests.

Note that while the Agent in the above picture is connected to the PSTN, the agent could just as well be located inside the Customer network (for example, 1800-xxx-xxx, which routes to an agent) -- as long as the dialed number is addressable through the PSTN.

In this configuration the **Default call provider for Make Call** cluster attribute should be set to ZangCallConnector on the target cluster if the workflow or snap-in initiates outbound calls. For additional information, see Routing outbound calls to Avaya OneCloud CPaaS on page 20.

Intermingled configuration

With the intermingled configuration a private SIP trunk is used to transfer snap-in specific information. In an intermingled configuration, a workflow or snap-in for an incoming call to Avaya OneCloud™ CPaaS can store information about the call that can later be retrieved by another workflow when the call is extended to an agent. Therefore Avaya Aura® Session Manager and Avaya Aura® Session Border Controller are required.



In this configuration the **Default call provider for Make Call** cluster attribute can be set to ZangCallConnector or SIP on the target cluster. When the attribute is set to SIP, an Avaya Breeze® platform initiated call will traverse the Session Manager, the Session Border Controller, and go to the PSTN. When the attribute is set to ZangCallConnector, Avaya OneCloud™ CPaaS will send the call to the PSTN for an Avaya Breeze® platform initiated call.

Standalone configuration call flow examples

Example of an Avaya Breeze® platform initiated call to a customer

Use case: Avaya Breeze® platform calls a customer and plays an announcement, then hangs up.

1. An Avaya Engagement Designer workflow or snap-in initiates a one-party call.
2. The request is forwarded to the Zang Call Connector.
3. The Zang Call Connector sends the request over HTTPS to Avaya OneCloud™ CPaaS, which makes the call to the customer over the PSTN.
4. The customer answers and Avaya OneCloud™ CPaaS provides the answer event to the Zang Call Connector in a long-poll response.
5. The workflow or snap-in is advised of the answer and plays an announcement. The announcement follows the same path as the initial call request to the customer.

Example of an incoming call to Avaya OneCloud™ CPaaS that is extended to an agent

Use case: A customer dials an Avaya OneCloud™ CPaaS number that is extended to an agent.

1. The customer dials an Avaya OneCloud™ CPaaS number. (This number has been administered on www.zang.io to advise the Zang Call Connector of incoming calls.)
2. Avaya OneCloud™ CPaaS conveys the incoming call event to the Zang Call Connector in a long-poll response.
3. The event is forwarded to a snap-in or an Avaya Engagement Designer workflow, which adds an agent (for example, “3035551212”) to the call.
4. The request to dial the agent is forwarded to the Zang Call Connector.
5. The Zang Call Connector sends the request over HTTPS to Avaya OneCloud™ CPaaS, which makes the call to the agent over the PSTN.
6. The agent answers and Avaya OneCloud™ CPaaS provides the answer event to the Zang Call Connector in a long-poll response.
7. The workflow or snap-in is advised of the answer. The customer and agent are now talking.

Intermingled configuration call flow example

Example of an incoming call to Avaya OneCloud™ CPaaS that is extended to an agent

Use case: The customer dials an Avaya OneCloud™ CPaaS number, which is extended to an agent. The workflow associated with the agent retrieves information about the Avaya OneCloud™ CPaaS call.

1. The customer dials an Avaya OneCloud™ CPaaS number, which advises Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform of the call.
2. The invoked workflow, or snap-in, retrieves the Universal Call ID (UCID) associated with the call and uses that identifier to store information about the call in a database (for example, cluster DB, Context Store, or other database) .
3. The workflow adds an agent to the call in a SIP format, for example, 3035551212@company.com.

   The domain name informs Avaya OneCloud™ CPaaS to send the call over the private SIP trunk. The UCID is present in the User-to-User: header in the SIP message.
4. The SIP call arrives at the Session Border Controller. It is forwarded to Session Manager and then to Avaya Breeze® platform.
5. A workflow retrieves the UCID and is able to look up information stored on the Avaya OneCloud™ CPaaS side to gain more context about the call.

Chapter 3: Planning

Key customer configuration information

Record the following information for use during the deployment.

Information to record	Notes
Avaya OneCloud™ CPaaS Account SID	
Avaya OneCloud™ CPaaS Auth Token	
Avaya OneCloud™ CPaaS Base URL	https://api.zang.io
Avaya OneCloud™ CPaaS Long Polling Base URL	https://pubsub.zang.io
Supplier Id	Provided by Avaya.
Avaya OneCloud™ CPaaS Account phone number	
For an intermingled deployment, you will also require the following information.	
Avaya Aura® Session Border Controller IP address	
Avaya OneCloud™ CPaaS server IP address	Currently the address is 72.9.136.235.
SIP Transport type	Only TCP is supported by Avaya OneCloud™ CPaaS for Avaya Breeze® platform.

Chapter 4: Deployment process

Prerequisites

Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform requires an account in Avaya OneCloud™ CPaaS. Purchase a phone number and request access to all call features, for example, call alerting, answer notification, etc. See www.zang.io for instructions on how to create and manage a Avaya OneCloud™ CPaaS account. Record the Account SID, Auth Token and phone number to use when administering the Zang Call Connector.

Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform deployment checklist

There are two types of deployment for Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform: standalone and intermingled. Complete the steps that are appropriate to your deployment.

#	Action	Reference/Notes	✔
1	Deploy and configure Avaya Breeze® platform.	Avaya Breeze platform deployment on page 17	
2	Configure your Avaya OneCloud™ CPaaS account for Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Configuring the Avaya OneCloud CPaaS account on page 15	
3	Download the Zang Call Connector from PLDS.		
4	Load and install the Zang Call Connector.	Loading the Zang Call Connector snap-in on page 17 Installing the Zang Call Connector snap-in on page 18	
5	Configure Zang Call Connector attributes.	Configuring Zang Call Connector attributes on page 18	

Table continues…

#	Action	Reference/Notes	✔
6	Configure Avaya Breeze® platform to intercept calls to your Avaya OneCloud™ CPaaS phone number.	Routing inbound calls on page 19	
7	Configure Avaya Breeze® platform initiated calls to use Avaya OneCloud™ CPaaS.	Routing outbound calls to Avaya OneCloud CPaaS on page 20 Required only if your workflow or snap-in initiates outbound calls, and you want those outbound calls to use Avaya OneCloud™ CPaaS instead of SIP.	
8	Configure Engagement Designer to launch Workflow Definitions (WFDs) in a Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform environment.	Administering Engagement Designer on page 21 Required only if you use Engagement Designer WFDs.	
9	Configure Avaya Aura® Session Border Controller.	Administering Avaya Aura Session Border Controller on page 23 Required only for the intermingled configuration.	

Chapter 5: Avaya OneCloud CPaaS account configuration

Configuring the Avaya OneCloud™ CPaaS account

Before you begin

You must have an Avaya OneCloud™ CPaaS account and have purchased a phone number.

Procedure

1. Log on to the Avaya OneCloud™ CPaaS website: `https://www.zang.io`.
2. Sign in to your Avaya OneCloud™ CPaaS account.
3. Select the Zang Cloud application.
4. From the Zang Cloud menu bar, select **NUMBERS** > **MANAGE NUMBERS**.
5. Beside the phone number you purchased, click **Voice**.
6. On the **voice** tab, for the Voice Request Url, enter `https://pubsub.zang.io/<account SID>/calls/incoming.xml`.
7. From the drop-down menu, select **POST**.
8. Click **Save**.

Note:

The following steps are optional and are required only for the intermingled configuration.

9. From the Zang Cloud menu bar, select **SIP** > **DOMAINS**.
10. Click **Create SIP Domain**.
11. On the **General Settings** tab, enter a domain name.
12. Click **Create Domain**.
13. From the Zang Cloud menu bar, select **SIP** > **IP ACCESS CONTROL LISTS**.
14. On the **IP Access Lists** tab, click **Create Access List**.
15. Enter a name for the IP Access List and click **Create list**.
16. Click **Add IP Address**.

17. Enter a name and IP address for the Avaya Aura® Session Border Controller and click **Create IP Address**.

    This IP address must match the IP address you select for the Signaling Interface when you administer the Avaya Aura® Session Border Controller.

    Note:

    It is not necessary to configure a Credential List.

Chapter 6: System Manager administration

Avaya Breeze® platform deployment

Install and configure Avaya Breeze® platform based on the instructions in *Deploying Avaya Breeze® platform*. If you are deploying Avaya Breeze® platform exclusively for use with Avaya OneCloud™ CPaaS, you can skip the following deployment steps:

- Do not create or verify the SIP Entity Link.
- Do not administer routing of inbound or outbound ISDN calls for Communication Manager.
- Do not deploy Avaya Aura® Media Server.
- Do not administer SIP high availability.

Loading the Zang Call Connector snap-in

About this task

This task describes how to load the Zang Call Connector snap-in to System Manager.

Before you begin

Download the Zang Call Connector snap-in from PLDS to a location accessible to System Manager.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Click **LOAD**.
3. In the Load Service window, depending on the browser used, click **Browse** or **Choose File**, and browse to your snap-in file location.
4. Browse and select the Zang Call Connector snap-in (`.svar`) file, and then click **Open**.
5. In the Load Service window, click **LOAD**.
6. On the Accept End User License Agreement page, click **Accept** to accept the agreement.

   When the snap-in is loaded, the **Service Management** > **Services** page displays the **State** of the snap-in as **Loaded**.

Installing the Zang Call Connector snap-in

About this task

Use this task to install the Zang Call Connector snap-in to a specific cluster. Certificates for HTTPS connections to Avaya OneCloud™ CPaaS install automatically when you install the Zang Call Connector Snap-in.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Select the ZangCallConnector snap-in.
3. Click **Install**.
4. Select the cluster where you want the snap-in to reside, and click **Commit**.
5. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

   Installed with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.
6. To track the progress of a snap-in installation, on the Server Administration page, click the **Service Install Status** for an Avaya Breeze® platform server.

   The Service Status page displays the installation status of all the snap-ins installed on that server.
7. **(Optional)** Designate the Preferred Version.

   If you want to designate the snap-in as the preferred version, do the following:

   a. Verify that the snap-in is in the installed state on System Manager by clicking **Elements** > **Avaya Breeze** > **Service Management** > **Services**.

   b. From the **All Services** list, select the version of the snap-in you want to mark as Preferred.

   c. Click **Set Preferred Version**.

   d. Select the cluster for which you want this to be the preferred version, and click **Commit**.

Configuring Zang Call Connector attributes

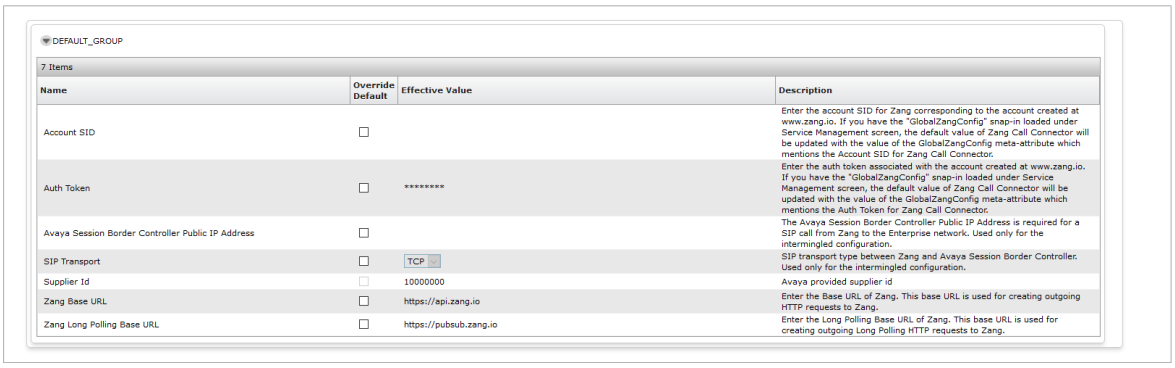
About this task

Use this task to configure attributes for the Zang Call Connector snap-in.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. Click the **Service Clusters** tab.
3. From the **Cluster** field, select the cluster on which you want to configure the snap-in attributes.
4. From the **Service** field, select the ZangCallConnector snap-in.

   The system displays all attributes that are configured at the cluster level for the snap-in.
5. For the Account SID and Auth Token attributes, enter the values from your Avaya OneCloud™ CPaaS account:
   a. Click **Override Default**.
   b. Enter a new value in the **Effective Value** field.



DEFAULT_GROUP

7 Items

Name	Override Default	Effective Value	Description
Account SID	☐		Enter the account SID for Zang corresponding to the account created at www.zang.io. If you have the "GlobalZangConfig" snap-in loaded under Service Management screen, the default value of Zang Call Connector will be updated with the value of the GlobalZangConfig meta-attribute which mentions the Account SID for Zang Call Connector.
Auth Token	☐	********	Enter the auth token associated with the account created at www.zang.io. If you have the "GlobalZangConfig" snap-in loaded under Service Management screen, the default value of Zang Call Connector will be updated with the value of the GlobalZangConfig meta-attribute which mentions the Auth Token for Zang Call Connector.
Avaya Session Border Controller Public IP Address	☐		The Avaya Session Border Controller Public IP Address is required for a SIP call from Zang to the Enterprise network. Used only for the intermingled configuration.
SIP Transport	☐	TCP	SIP transport type between Zang and Avaya Session Border Controller. Used only for the intermingled configuration.
Supplier Id		10000000	Avaya provided supplier id
Zang Base URL	☐	https://api.zang.io	Enter the Base URL of Zang. This base URL is used for creating outgoing HTTP requests to Zang.
Zang Long Polling Base URL	☐	https://pubsub.zang.io	Enter the Long Polling Base URL of Zang. This base URL is used for creating outgoing Long Polling HTTP requests to Zang.

6. Click **Commit** to save the changes.

Routing inbound calls

About this task

Complete this task to route inbound calls from Avaya OneCloud™ CPaaS to the desired snap-in.

Procedure

1. On System Manager create a Service Profile and add the snap-in to it.

   For additional information about creating a service profile, see “Creating a Service Profile” in *Administering Avaya Breeze® platform*.
2. Create a new Implicit User Profile Rule.
   a. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Implicit User Profiles**.
   b. Click **New**.

c. In the **Service Profile** field, select the Service Profile associated with the snap-in that needs to be invoked.

d. In the **Pattern** field, specify the phone number associated with your Avaya OneCloud™ CPaaS account.

   Begin the pattern with a `+1`. For example, `+17205551212`.

e. Type a description of the rule.

f. Click **Commit** to save your changes.

For additional information about creating the Implicit User Rule or assigning the Service Profile to it, see *Administering Avaya Breeze® platform*.

Routing outbound calls to Avaya OneCloud™ CPaaS

About this task

Complete this procedure only if you have a workflow or snap-in that initiates outbound calls, and you want for those outbound calls to use Avaya OneCloud™ CPaaS instead of SIP. Note that Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform does not support 2-party Make Call.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Place the cluster in Deny New Service state.
   a. Select the cluster where the Zang Call Connector is installed.
   b. From the **Cluster State** drop-down menu, select **Deny New Service**.
   c. Verify that the system displays **Denying** in the **Cluster State** column.
3. Select the cluster and click **Edit**.
4. Under Cluster Attributes, from the **Default call provider for Make Call** drop-down menu, select **ZangCallConnector**.
5. Click **Commit** to save your changes.
6. Place the cluster in Accept New Service state.
   a. Select the cluster where the Zang Call Connector is installed.
   b. From the **Cluster State** drop-down menu, select **Accept New Service**.
   c. Verify that the system displays **Accepting** in the **Cluster State** column.

Chapter 7: Engagement Designer administration

Administering Engagement Designer

About this task

In a Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform environment, the Engagement Designer snap-in is added to a service profile. The binding of an incoming call to a particular WFD is done by Engagement Designer.

Complete the following procedure to invoke Engagement Designer workflows in a Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform environment.

For additional information about installing, configuring and using Engagement Designer, see the Engagement Designer documentation.

Procedure

1. On System Manager create a Service Profile and add the Engagement Designer snap-in to it.

   For additional information about creating a service profile, see “Creating a Service Profile” in *Administering Avaya Breeze® platform*.

2. Create a new Implicit User Rule.

   a. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Implicit User Profiles**.

   b. Click **New**.

   c. In the **Service Profile** field, select the Service Profile you created.

   d. In the **Pattern** field, specify the phone number associated with your Avaya OneCloud™ CPaaS account.

      Begin the pattern with a `+1`. For example, `+17205551212`.

   e. Type a description of the rule.

   f. Click **Commit** to save your changes.

   For additional information about creating the Implicit User Rule or assigning the Service Profile to it, see *Administering Avaya Breeze® platform*.

3. Log on to the Engagement Designer Administration Console in one of the following ways.
   - Click **Admin Console** from the Engagement Designer interface.
   - On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**. In the row for the cluster where Engagement Designer is installed, click **Select** in the Service URL column. Select **Admin Console URL**.
4. Create a new rule for the CallIntercepted event and assign a WFD to it.
   a. Click the **Routing** tab.
   b. Click **Create**.
   c. From the **Select event** menu, select the CallIntercepted/ CALL_INTERCEPT_TO_CALLED_PARTY event .
   d. From the **Select workflows** menu, select the WFD you want triggered when a call is received from your Avaya OneCloud™ CPaaS phone.

      Select the latest version of the WFD, or the version you would like to use.
   e. Enter a name for the rule and click **Add Rule**.

      A set of attributes and fields associated with the event displays.
   f. Select from the schema attribute, and function lists, and enter the values to construct a rule that specifies which WFD is triggered when a call is received from your Avaya OneCloud™ CPaaS phone number. For example, where 17205551212 is your Avaya OneCloud™ CPaaS number:
      - Select schema attribute – CallEventcallingParty.handle:string
      - Select function – is equal to
      - Enter value – +17205551212
   g. Click **Save**.

      The new rule appears in the list of rules.

Chapter 8: Session Border Controller administration

Administering Avaya Aura® Session Border Controller

About this task

Complete this procedure to administer the Avaya Aura® Session Border Controller for an intermingled system configuration. For additional information about Session Border Controller deployment and configuration, see the Avaya Aura® Session Border Controller documentation.

Before you begin

- Your session border controller must be installed and configured to run with Session Manager.
- Configure your firewall so that port 5060 is open for UDP and TCP for outgoing SIP messages.
- Open all ports for media transport.
- You will need to know your Avaya OneCloud™ CPaaS server IP address.

Procedure

1. Log in the Avaya Aura® Session Border Controller.
2. Click **Global Profiles** > **Server Interworking** and create an Interworking Profile.

   For additional information, see *Administering Avaya Session Border Controller for Enterprise*.
3. Create a Server Profile for the Avaya OneCloud™ CPaaS server.
   a. Click **Global Profiles** > **Server Configuration**.
   b. Click **Add**.
   c. Enter a **Profile Name** and click **Next**.
   d. In the **IP Address/FQDN** field, enter the Avaya OneCloud™ CPaaS server IP address.
   e. In the **Port** field, enter 5060.
   f. From the **Transport** drop-down menu, select TCP or UDP.

      TLS is not supported with Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.
   g. Click **Next**.

   h. Do not Enable Authentication. Click **Next**.
   i. Do not Enable Heartbeat. Click **Next**.
   j. Click checkboxes to **Enable DoS Protection** and **Enable Grooming**.
   k. From the **Interworking Profile** drop-down menu, select the Interworking Profile you created.
   l. Click **Finish**.

4. Create a Routing Profile.
   a. Click **Global Profiles** > **Routing**.
   b. Click **Add** above the list of Routing Profiles.
   c. Enter a **Profile Name** and click **Next**.
   d. From the **URI Group** drop-down menu, select a URI group.
   e. From the **Load Balancing** drop-down menu, select Priority.
   f. From the **Transport** drop-down menu, select TCP or UDP.
   g. Click **Add**.
   h. Enter a Priority/Weight.
   i. From the **Server Configuration** drop-down menu, select the Server Profile you created for the Avaya OneCloud™ CPaaS server.
   j. Leave the default values in all other fields.
   k. Click **Finish**.
5. Configure the public Signaling Interface.
   a. Click **Device Specific Settings** > **Signaling Interface**.
   b. Click **Add**.
   c. Enter a **Name** .
   d. From the **IP Address** drop-down menus, select the Public Network and the IP address that Avaya OneCloud™ CPaaS will use for the session border controller. This is the IP address you added to the IP Access List when you configured your Avaya OneCloud™ CPaaS account.
   e. For the **TCP Port** or **UDP Port** enter 5060.
   f. Leave all other fields blank.
   g. Click **Finish**.
6. Configure the private Signaling Interface.
   a. Click **Device Specific Settings** > **Signaling Interface**.
   b. Click **Add**.
   c. Enter a **Name** .

   d. From the **IP Address** drop-down menus, select the Private Network and the IP address the session border controller uses to route to the private network.
   e. For the **TCP Port** or **UDP Port** enter 5060.
   f. Leave all other fields blank.
   g. Click **Finish**.
7. Configure the Media Interface.
   a. Click **Device Specific Settings** > **Media Interface**.
   b. Click **Add**.
   c. Enter a **Name** .
   d. From the **IP Address** drop-down menus, select the Public Network and the IP address that Avaya OneCloud™ CPaaS will use for the session border controller. This is the IP address you added to the IP Access List when you configured your Avaya OneCloud™ CPaaS account.
   e. For the **Port Range**, enter the range of ports that will be used for media transmission.

      These ports must be open on the firewall.
   f. Click **Finish**.
8. Create a Server Flow.
   a. Click **Device Specific Settings** > **End Point Flows**.
   b. On the **Server Flows** tab, click **Add**.
   c. Enter a **Flow Name** .
   d. From the **Server Configuration** drop-down menu, select the Server Profile you created for the Avaya OneCloud™ CPaaS server.
   e. For the **Transport** and **Remote Subnet** fields select or enter *****.
   f. From the **Received Interface** menu, select the public Signaling Interface you configured in this procedure.
   g. From the **Signaling Interface** menu, select the private Signaling Interface you configured in this procedure.
   h. From the **Media Interface** menu, select the Media Interface you configured in this procedure.
   i. From the **Routing Profile** menu, select the Routing Profile you configured in this procedure.
   j. Select values for the remaining fields based on your internal network configuration.
   k. Click **Finish**.

Chapter 9: Troubleshooting

Troubleshooting call failure

About this task

Take the following steps if your Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform calls are not processing.

Procedure

1. Verify that the Zang Call Connector has been administered with the correct credentials. Ensure that the Account SID and Auth Token attributes on the Zang Call Connector match those for the account on www.zang.io.
2. Verify that there are funds in your Avaya OneCloud™ CPaaS account. Navigate to the Avaya OneCloud™ CPaaS dashboard (www.zang.io) and verify that there are funds to make calls.
3. Verify that you have installed the Avaya OneCloud™ CPaaS trust certificates correctly. For additional information, see Installing certificates for HTTPS connections to Avaya OneCloud CPaaS on page 28.

   If these steps do not resolve the issue, check for alarms associated with Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.
4. On System Manager, click **Services** > **Events** > **Alarms**.
5. Look for Event IDs ZCONNFAIL and CCONNFAIL. If either event has a **Status** of Raised, contact your Avaya representative or Avaya Support for assistance.

   A **Status** of Cleared means that the issue has been resolved.

Checking log files

Procedure

1. Log onto the Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform node command line interface using the cust user account.
2. Execute the traceMsg command.
   a. Execute the command.

   b. Press `S` for start.
   c. Unselect `SIP`.
   d. Select `HTTP`.
   e. Select `Snap-ins`.
   f. Arrow down to `ZangCallConnector` and select `FINE`.
   g. Arrow down to `OK` on this and the next menu.
   h. Make a call and verify that there is snap-in and HTTP activity.
3. Examine the log files.
   a. Turn on debugging for the workflow or snap-in: `ce dlogon <snap-in name>`.
   b. Turn on debugging for the Zang Call Connector: `ce dlogon ZangCallConnector`.
   c. Make a call.
   d. Navigate to the log files directory and look at the logs for issues. For example: `ce dlogv ZangCallConnector`.
4. If the troubleshooting steps do not resolve the problem, contact your Avaya representative or Avaya Support for assistance.

Workflow or snap-in is not invoked

Condition

My Workflow or snap-in is not getting invoked when a call is made to an Avaya OneCloud™ CPaaS number.

Solution

1. Verify the implicit user configuration for your snap-in. For additional information, see Routing inbound calls on page 19.
2. For Engagement Designer workflows, verify that you have completed the required Engagement Designer administration. For additional information, see Administering Engagement Designer on page 21.

Media APIs do not function as expected

Condition

Some of the media APIs do not function exactly as they do in Avaya Aura® – for example, play URI or Text-to-speech.

Solution

1. Verify that all media operations (such as Play Announcement, Prompt and Collect, Text-to-speech, Text-to-speech and collect) have isinterruptible set to true.
2. For Engagement Designer, use Interrupt Announcement as true.
3. For Play Announcement and Prompt and Collect, verify that you are using an http/https URL only.

   For more information about the supported and available options, see the Avaya Breeze® platform SDK Javadoc.

Installing certificates for HTTPS connections to Avaya OneCloud™ CPaaS

About this task

Certificates for HTTPS connections to Avaya OneCloud™ CPaaS install automatically when you install the Zang Call Connector Snap-in. If the certificates do not install automatically, or are cleared by some other process, complete this procedure to retrieve and install the certificates.

In addition you may need to configure/install trusted certificates for your outgoing HTTPS proxy in the enterprise network. Complete the following procedure for your outgoing proxy trusted certificates.

Procedure

1. Download the following certificates. The certificates must be in a location accessible to System Manager.
   - https://support.cloudflare.com/hc/en-us/articles/218689638-What-are-the-root-certificate-authorities-CAs-used-with-Cloudflare-Origin-CA-. Scroll to the bottom of the page and click **cloudflare_origin_ecc.pem.**
   - https://digicert.com/digicert-root-certificates.htm baltimore-cybertrust-root.digicert.com/info/index.html. Click **Download** for the Baltimore CyberTrust Root.
   - Optionally download your outgoing HTTPS proxy trusted certificate.
2. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
3. Select the cluster where you want to administer the trusted certificates.
4. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze® Instances)** to download the trusted certificate for all the servers in the cluster.

   Note:

   The Trust Certificate that you are about to add will apply to all the Avaya Breeze® platform servers assigned to the cluster.
5. From the **Select Store Type to install trusted certificate** menu, select **WEBSPHERE**.

6. Click **Browse** to the location of your Trust Certificate, and select the certificate.
7. Click **Retrieve Certificate**, and review the details of the Trusted Certificate.
8. Click **Commit** .
9. Repeat to retrieve and commit the second trust certificate.

Chapter 10: Resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Understanding		
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Implementing		
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform.	Services and support personnel System administrators
Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform	Deploy and configure Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Services and support personnel System administrators
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel

Table continues…

Title	Use this document to:	Audience
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
Deploying Avaya Aura® System Manager	Deploy and configure Avaya Aura® System Manager in a virtualized environment using VMware.	System administrators Services and support personnel
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Use Solution Deployment Manager.	System administrators Services and support personnel
Migrating and Installing Avaya Aura® Appliance Virtualization Platform	Deploy and configure Avaya Aura® Appliance Virtualization Platform.	System administrators Services and support personnel
Deploying Avaya Session Border Controller for Enterprise	Deploy and configure Avaya Aura® Session Border Controller.	System administrators Services and support personnel
Customizing		
Getting Started with the Avaya Breeze® platform SDK	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze® platform SDK.	Programmers
Avaya Breeze® platform Snap-in Development Guide	Understand the key concepts needed to develop the different types of Avaya Breeze® platform snap-ins.	Programmers
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze® platform.	Programmers
Avaya Breeze® platform API Javadocs	Understand API classes and uses.	Programmers
Supporting		

Table continues…

Title	Use this document to:	Audience
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Using		
Quick Start to deploying the HelloWorld Snap-in	Install, configure, and test an Avaya Breeze® platform snap-in service, specifically the HelloWorld call-intercept snap-in.	Programmers System administrators
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Session Border Controller for Enterprise	Administer Avaya Aura® Session Border Controller.	System Administrators Services and support personnel

Related links

Finding documents on the Avaya Support website on page 32
Avaya Documentation Portal navigation on page 33

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 the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
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 only displays the documents for the selected category.
7. Click **Enter**.

Related links

Documentation on page 30

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, and Twitter.
- 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.

Related links

Documentation on page 30

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field, and click **Go** to search for the course.

Course code	Course title
2016W	Fundamentals of Avaya Breeze® platform
2316W	Avaya Breeze® platform Client SDK Fundamentals
2024V	Programming Avaya Breeze® platform Snap-ins using Java SDK Bootcamp
2024T	Programming Avaya Breeze® platform Snap-ins using Java SDK Online Test
20250V	Programming Avaya Breeze® platform Snap-ins using Engagement Designer
20250T	Programming Avaya Breeze® platform R3 Snap-ins using Engagement Designer Online Test
5105	Avaya Breeze® platform Implementation and Support Test
7016W	Avaya Breeze® platform Implementation and Support

Support

Platform support

Go to the Avaya Support website at www.avaya.com/Support for the most up-to-date product documentation, and product notices. Also search for release notes, service packs, and patches. 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.

Product documentation is also available on the Avaya Documentation Portal at https://documentation.avaya.com.

Developer support

Go to the Avaya DevConnect website at http://www.avaya.com/breezedeveloper to access the Avaya Breeze® platform API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Index

A

Avaya OneCloud CPaaS account 15
Avaya OneCloud CPaaS call routing 19, 20

C

call flow
- intermingled configuration 11
- standalone configuration 10

calls fail 26
collection
- delete 33
- edit name 33
- generating PDF 33
- sharing content 33

communication manager 8
configuring snap-in attributes 18
content
- publishing PDF output 33
- searching 33
- sharing 33
- watching for updates 33

D

deployment checklist 13
documentation portal 33
- finding content 33
- navigation 33

E

engagement designer 21
EULA 17

F

finding content on documentation portal 33

I

implicit user profile 21
intermingled configuration 7, 8

L

loading snap-ins
- service 17

load snap-ins 17
log files 26

M

My Docs 33

P

preferred version
- setting 18

prerequisites 13

R

release notes 35

S

searching for content 33
service packs 35
service profile 21
session border controller
- administration 23
- version support 8

session manager 8
sharing content 33
snap-in
- installation 18
- loading 17

snap-in install status 18
standalone configuration 7, 8
support 35
system manager 8

T

training 34
trust certificates 28

W

watch list 33