Avaya Session Border Controller for Enterprise 7.2 Release Notes

Release 7.2
Issue 1
June 2017

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 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 Web site:
http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site:
http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Contents:

Overview

This document provides information about the new features/enhancements in ASBCE Release 7.2, and the known issues for this release.

Documentation

No.	Title	Link
1	Avaya Session Border Controller for Enterprise Overview and Specification	https://downloads.avaya.com/css/P8/documents/101040310
2	Deploying Avaya Session Border Controller for Enterprise	https://downloads.avaya.com/css/P8/documents/101040278
3	Deploying Avaya Session Border Controller in Virtualized Environment	https://downloads.avaya.com/css/P8/documents/101040286
4	Upgrading Avaya Session Border Controller for Enterprise	https://downloads.avaya.com/css/P8/documents/101040283
5	Administering Avaya Session Border Controller for Enterprise	https://downloads.avaya.com/css/P8/documents/101040276
6	Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	https://downloads.avaya.com/css/P8/documents/101040300
7	Deploying Avaya Session Border Controller on AWS	https://downloads.avaya.com/css/P8/documents/101040293

Build Download Location

File Name	PLDS ID	MD5SUM	Remarks
sbce-7.2.0.0-18-13712.iso	SBCE0000082	598a6322a09d7054698217c832bd41c3	ISO image for fresh install on hardware
sbce-7.2.0.0-18-13712.ova	SBCE0000083	8bda66c7951eb541d39abfb4c897e69f	OVA for fresh Installation on VMWare
sbce-7.2.0.0-18-13712-8781e5b3d8fd34dec216994d3a87524f.tar.gz	SBCE0000084	8781e5b3d8fd34dec216994d3a87524f	Upgrade package for upgrade from 7.1.x release
sbce-7.2.0.0-18-13712-8781e5b3d8fd34dec216994d3a87524f.tar.gz.asc	SBCE0000085	608116f7b294ed82bfb7fbe345279759	Signature files to be used for upgrade from 7.1 SP1&above to 7.2 release
sbce-7.2.0.0-18-13712.qcow2	SBCE0000086	99f345f59c7376a646fddae7c70b7fd5	KVM image for fresh

			installation
sbce-7.2.0.0-18-13712-hotfix-06012017.tar.gz	SBCE0000087	811b959df17e947a183c12279a09800c	Patch to be installed post fresh install or Upgrade
sbce-7.2.0.0-18-13712-aws-001.ova	SBCE0000088	779690db167f16d82211709b60c6a1fd	OVA image, to be converted to AMI for ASBCE7.2 installation on AWS
AVAYA-SBCE-MIBP_v112.mib	SBCE0000089	e562fb234eab733f8861802cf86dc310	MIB File for ASBCE7.2
sbce-7.2.0.0-18-13712_8e6d80f0da2965bfffea4ff9d0d201a9.img	SBCE0000090	8e6d80f0da2965bfffea4ff9d0d201a9	Image file for creating USB Installer for fresh install on hardware

New Features and Enhancements

CDR Statistics and Reporting

CDRs contain information about each call processed by ASBCE. A CDR is generated for each leg of the call in a half call model known as split CDR. Partial CDR is generated on call establishment and complete CDR on call termination. Media statistics provide ASBCE's view of RTP feedback quality.

- Media statistics are collected from RTP and RTCP Sender/Receiver report based on the RTCP Extended Report Framework (RFC 3611).Media statistics are embedded in CDR and available at end of the call.
- CDR over RADIUS
  ASBCE 7.2 supports RADIUS interface to send CDRs to an adjunct - 3rd party RADIUS Server.
- CDR – Local storage and SFTP
  In case RADIUS interface does not exist or the RADIUS interface is down, CDRs are saved on ASBCE locally. ASBCE provides an SFTP interface to push CDR files to 3rd party adjunct server. If FTP server is down, ASBCE has local storage up to 35% of archive partition.
- Statistics:
  Indicates the real time call traffic or load on the system and provides ability to network administrator to understand ASBCE's current usage. Statistics are collected :
  - Per System
  - Per Server/Subscriber Flow
  - Per Policy groups
  - Per URI groups

- Measurements/ Periodic Statistics
  Periodic statistics are statistics data collected per interval:
  - Per System
  - Per Server/Subscriber Flow
  - Per Policy groups
  - Per URI groups

AWS support

ASBCE 7.2 supports deployments in Amazon Web Services (AWS)

Signal-only Encryption

Through enablement of Signal-only encryption license, ASBCE GUI allows signaling encryption (TLS) configurations, but media encryption (SRTP) is not allowed.

Enterprise/Remote Worker IPv6 Support

ASBCE 7.2 supports IPV6 and SDP-ANAT for Remote Workers and Enterprise. ASBCE 7.2 performs the interworking functionality between any of the following address types IPV4, IPV6, tolerant IPV4/IPV6 for SIP Signaling and Media. Management Interface IPv6 has to be in Dual-Stack Mode only. ASBCE supports both IPv6 unique-local unicast address and IPv6 global unicast address configuration, besides support for conventional IPv4 addressing on Management interface. Communication towards DNS servers, NTP server, syslog server etc. is supported over IPv6. ASBCE 7.2 supports SIP Entities & Endpoints having following levels of IP Address Family support:

- IPv4 only: V4 SIP signaling over IPv4 connections.
- IPv6 only: V6 SIP signaling over IPv6 connections.
- Tolerant IPv4: V4 and V6 SIP signaling over IPv4 connections.
- Tolerant IPv6: V6 and V4 SIP signaling over IPv6 connections.
- Interworking media address with non ANAT V4 or non ANAT V6 and SDP ANAT on the other side.
- Interwork between SDP-ANAT on both sides with different preferences
- The SDP-ANAT preference for IPV6 and IPV4 shall be as per local administration or overridden by remote preference

External Media server and Transrating

ASBCE 7.2 adds support for Transrating for audio sessions. ASBCE uses Avaya Media Server (AMS) to support transcoding and transrating. ASBCE 7.2 Release adds support for external Media Server. This allows offloading transcoding and transrating to an external server. ASBCE7.2 continues to support internal/co-resident Media Server as well. ASBCE supports load balancing between clustered/multiple Media Servers based on

- Load factor
- Round robin

AMS build 7.8.0.312 (or above version) is required with ASBCE7.2 release. ASBCE can be configured to support the following configurations using media rules and feature control flags

- Transcoding only
- Transrating only
- Transrating+Transcoding

Configurable Snapshot

This feature supports restoring of snapshots taken from one ASBCE to other ASBCE devices, attached to same EMS. The snapshots taken from one ASBCE device can be restored on other ASBCE devices with same hardware configurations/VM resources. The snapshot will contain the device configurations like, media interface, end point flows. The configuration will replicate into other device, thereby substantially reducing time for configuring new device.

RHEL7.2 Migration

Starting with ASBCE7.2, Red Hat Enterprise Linux has been migrated from 6.x to 7.2. Besides support of new features with ASBCE7.2, there is no change in user experience as a result of Linux upgrade. Starting with ASBCE7.2, rollback sequence has been changed that requires ASBCE's to be downgraded first and then the EMS. There is no change in upgrade sequence.

Dynamic Licensing

Starting with ASBCE7.2 licenses can be dynamically allocated across ASBCEs. With this option, licenses can be fully utilized across difference ASBCE devices connected to same EMS. If one of the ASBCE devices goes down, its licenses can be reallocated to another ASBCE that can now serve more sessions due to the outage. Static assignment of licenses is not required anymore.

VMware 6.0 Support

ASBCE deployments are supported on ESXI Version 6.0.

KVM Support

Starting with ASBCE deployments are supported on KVM (Linux Kernel-based Virtual Machine).

AS-SIP deployment

In a UCR/AS-SIP deployment, ASBCE's can be deployed in the core network as well as in the enclaves

- Enclave fronting ASBCE for remote workers
- Enterprise Session Border Controller (ESC) fronting ASBCE for remote workers
- ASBCEs between ESC and Soft switch: two ASBCEs fronting ESC and Soft Switch (trunk deployment)
- ASBCE fronting Soft Switch towards Trunk

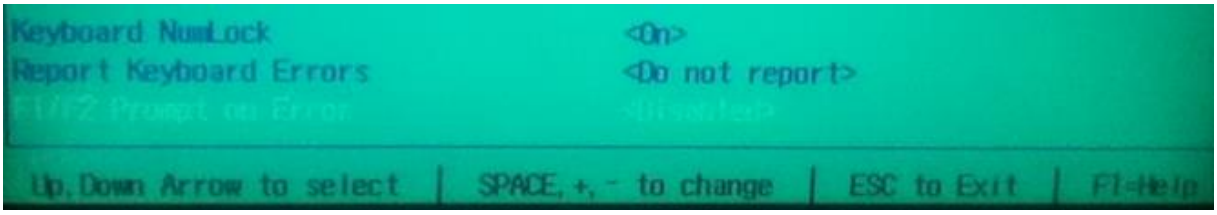
XMPP/HTTP for multi-tenant

ASBCE 7.2 provides domain based routing to route XMPP/HTTP traffic. ASBCE has ability to handle all XMPP/HTTP traffic from multi-tenant on a single external/public IP address, and route the traffic inside the core network based on the domain observed in the XMPP/HTTP message or based on the configured domain. This features supports up to 50 next hop entries for a single external address.

Prerequisite for ASBCE installed on Dell210 Servers

It is mandatory that BIOS firmware of the server is upgraded to latest version to avoid issues related to interface configuration missing post upgrade. If the target is "Dell PowerEdge R210 II" and BIOS version is below 2.1.2, ASBCE upgrade process will exit safely, with a message to upgrade the BIOS before re-trying upgrade.

Before proceeding with BIOS upgrade please ensure to disable "F1/F2 Prompt on Error" option to avoid ASBCE's getting stuck at F1/F2 prompt and having to perform manual reboot



BIOS Upgrade steps:

Download location -

http://www.dell.com/support/home/in/en/inbsdt1/Drivers/DriversDetails?driverId=YFWXP

Readme - https://downloads.dell.com/FOLDER00802491M/1/PER210II-020102BIOS.txt

Upgrade Path

SBCE/EMS on pre-7.1 version, need to be first upgraded to 7.1 before upgrading to 7.2 version.

Supported Upgrade Paths

ASBCE7.1 → ASBCE7.2

ASBCE7.1 SP1 → ASBCE7.2

ASBCE7.1 SP2 → ASBCE7.2

Prerequisites for Servers with 7.1 SP1 and above:

- Please make sure to upload .asc file for upgrades from 7.1 SP1 OR for 7.1 SP2 build upgrades. This procedure is also documented in 7.1 SP1 and 7.1 SP2 release notes on Avaya Support site.
- For servers which are on ASBCE7.1 SP1 with hotfix installed, please check whether hotfix "sbce-7.1.0.1-07-hotfix-12222016.tgz" is installed on the server by executing "ipcs-version" command, then verify that application shows up version as "Application : 7.1.0.1-12805". The output of "ipcs-version" command is as follows:

```
[ipcs@hostname ~]$ ipcs-version
SBCE Version : 7.1.0.1-07-12368
GUI : 7.1.0.1-12624
Database : 7.1.0.1-12368
Kernel : 2.6.32-642.11.1.el6.AV1
Application : 7.1.0.1-12805
ICU : 7.1.0.1-12815
PCF Module : 7.1.0.1-12604
```

  Run the following commands on EMS and SBCE's, before initiating the upgrade logged in as root user.

  "su – root"
  "touch /archive/SBC-RPM-Repository/RPMs/sbce-bin-7.1.0.1-12937.x86_64.rpm"

Post Upgrade Patch Installation

Please note that it is mandatory to install this patch post upgrade or Fresh Install of ASBCE's to 7.2 version.

Please download the patch file sbce-7.2.0.0-18-13712-hotfix-06012017.tar.gz from PLDS and upload it to /home/ipcs directory using winscp.

Patch installation procedure:

1. Login to the CLI of Avaya SBCE by using the login ipcs.
2. Verify the md5sum of the patch is '811b959df17e947a183c12279a09800c'
   `md5sum sbce-7.2.0.0-18-13712-hotfix- 06012017.tar.gz`
3. Switch the user to root
   `su – root`
4. Create a directory /usr/local/ipcs/patch (If directory already exists make sure it is empty)
   `mkdir /usr/local/ipcs/patch`
5. Change the directory to /usr/local/ipcs/patch
   `cd /usr/local/ipcs/patch/`
6. copy sbce-7.2.0.0-18-13712-hotfix-6012017.tar.gz from /home/ipcs/ to /usr/local/ipcs/patch/

```
cp /home/ipcs/ sbce-7.2.0.0-18-13712-hotfix-6012017.tar.gz /usr/local/ipcs/patch/
```

7. Untar the patch file
```
tar –zxvf  sbce-7.2.0.0-18-13712-hotfix-6012017.tar.gz
```
8. Run the Install_patch.sh script
```
sh install_hotfix.sh
```
9. Reboot the system
```
/sbin/reboot
```

List of the issues fixed through patch sbce-7.2.0.0-18-13712-hotfix-06012017.tar.gz:

AURORA-11743:Off-Boarded AMS and Transcoding: Call gets dropped on performing hold when send hold notification is enabled

AURORA-11499: License summary shows improper data, after editing dynamic license

AURORA-11752:[Tilera] All Media Packets Are Getting Dropped.

AURORA-11763:No audio for 45 seconds after HA fail over for transcoded call

AURORA-11758:[Tilera] ASBCE Is Raising License Error Logs For MIN License Allocation Value.

AURORA-11766:No talk path in case of back to back failover for transcoded calls

List of known issues with workarounds

Sr. No	Issue summary	Workaround
1	If number of Signaling and Media interfaces is not in same order as the target cloned ASBCE, Cloning configuration does not map Signaling and media interfaces correctly	edit the media and signaling interfaces manually
2	Statistics Viewer show 'counter not found' for active calls	Login to ASBCE as root user and run following: /usr/local/ipcs/icu/scripts/installConfigureNetSnmp.sh -l "Location" -c "Avaya" -n "ASBCE" -o ".1.3.6.1.4.1.6889.1.77" -d "Avaya Session Border Controller for Enterprise" || :
3	Local WebLM server in EMS does not provide the Server Properties/host ID	Login to EMS as root user and run following : 1. setfacl -m u:tomcat:rwx /etc/hosts 2. cd /usr/local/weblm/server/scripts 3. Run below commands: ./manage-weblm.py -d ./manage-weblm.py –e
4	Multiple certs for CLIENT Profile causing the nginx process to not start	merge all CA certificates in one file and use this as CA certificate For example, to merge three CA certificates by name ca1.pem, ca2.pem and ca3.pem, run the below command. cat ca1.pem cat2.pem ca3.pem >> combinedca.pem

5	IPv6 End to END - SIP Trunk Traffic Test - Packet Loss and low RTP MOS for some calls at multiple sessions in higher traffic conditions	If this issue is experienced use TCP instead of UDP end to end.
6	SBC on AWS: SBC does not allow configuring FQDN for NTP server.	Use IP address for the NTP server instead of FQDN

7	Cannot view ASBCE license allocations when local WebLM is used. Blank white page appears when user clicks on "Installed Products" in local WebLM server. This issue is caused due to accessing Faulty URL.	To address this issue, replace the faulty URL appearing in the browser address bar with a correct URL and access the page to view the ASBCE license allocations.
		
		For correct URL, remove the part of the Faulty URL starting from pipe symbol i.e. "| {standard.product.name}".
		
		Faulty URL:
		
		`https://<IP>/WebLM/faces/pages/view_license_allocations.xhtml?product=Session_Border_Controller_E_AE&id=weblm.pagesidebar.main.menu.licensedproducts|`
		`{standard.product.name}`
		
		Correct URL:
		
		`https://<IP>/WebLM/faces/pages/view_license_allocations.xhtml?product=Session_Border_Controller_E_AE&id=weblm.pagesidebar.main.menu.licensedproducts`

8	error message "Problem Connecting to WebLM server" shown even though WebLM is reachable	Check if a valid ASBCE license file is installed in WebLM server. In case it is not installed, install a valid license file and check.
9	ASBCE cannot obtain licenses from WebLM server.	Please refer to below KB article for fixing this issue. https://support.avaya.com/ext/index?page=content&id=SOLN318580

List of known issues

AURORA-11765: No media after HA fail over followed by call transfer

AURORA-11755: Call hold failed after CAll transfer between trunk users if Trunk server do not support Update method

AURORA-11612: Incident Viewer shows nothing on multiHA setup if one of the HA pair is in down state or unreachable

AURORA-11611: Statistics Viewer showing error for policy based stat on multiHA setup if one of the HA pair is in down state or unreachable

AURORA-11789: IPv6 End to End Traffic scenario - after 30 plus+ hours of traffic run failed

AURORA-11741: IPv6 End to END - SIP Trunk Traffic Test - Packet Loss and low RTP MOS for some calls at multiple sessions in higher traffic conditions.

AURORA-11747:RW-RW call has Noise on the call after Hold/ Resume if SBCE handle SRTP interworking with one leg as Dual stack and other Non-ANAT

AURORA-11462: Back to Back to Back SBC Deployment SSYNDI Restarted And Core Dumped On New Primary After Failover.

AURORA-10983: unable to re-add a HA Pair once deleted from GUI.

AURORA-11071: Back to Back to Back SBC Deployment SSYNDI taking longtime to process ipv6 sip messages.

AURORA-11759: Back to Back to Back SBC Deployment ASBCE Is Sending RTP/AVP For SRTP Call Towards SM After Core SBC Application Restart.