Avaya Session Border Controller for Enterprise 7.2.2.7 Release Notes

Release 7.2.2.7
Issue 1
February 2021

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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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. Note that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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).

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

Overview

This document provides information about the new features and enhancements in ASBCE Release 7.2.2.7.

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
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

Build Download Location

File Name	PLDS ID	MD5SUM	Remarks
sbce-7.2.2.7-34-19980-82f8018b14bd796b3de8f8107a97f214.tar.gz	SBCE0000230	82f8018b14bd796b3de8f8107a97f214	Upgrade package for upgrading to 7.2.2.7 release
sbce-7.2.2.7-34-19980-82f8018b14bd796b3de8f8107a97f214.tar.gz.asc	SBCE0000231	6842cf950d7f44722d0b5ee3a5a1345e	Signature files to be used for upgrade to 7.2.2.7 release
sbce-7.2.2.7-34-19980-signatures.tar.gz	SBCE0000232	493aa82c2e9a4407ac99c86363499d68	Key Bundle to validate RPM signatures

Upgrade Path

Avaya SBCE with releases prior to 7.2.2 must be upgraded to 7.2.2 release in order to upgrade to 7.2.2.7 (7.2 FP2 SP7)

Supported upgrade path:

7.2.2.0 GA -> 7.2.2.7(GUI &CLI both supported, GUI is recommended)

7.2.2.4 GA -> 7.2.2.7 (GUI &CLI both supported, GUI is recommended)

7.2.2.5 GA -> 7.2.2.7 (GUI &CLI both supported, GUI is recommended)

7.2.2.6 GA -> 7.2.2.7 (GUI &CLI both supported, GUI is recommended)

Upgrade Procedures

Before starting the upgrade, you must run pre-upgrade-check on each setup, to check whether the upgrade works or not in that setup/platform. If pre-upgrade-check passes, you can start upgrading. Otherwise, you need to follow Migration procedure.

For ASBCE upgrade and migration procedure, please refer to "Upgrading Avaya Session Border Controller for Enterprise" guide available at https://downloads.avaya.com/css/P8/documents/101040283

List of Issues Fixed

#	ID	Minimum Conditions	Visible Symptoms	Found in Release
1	AURORA-23826	Enable and Relay RTCP message	SBCE crashed while relaying RTCP message (Bind Err: 22)	7.2.2.4
2	AURORA-23669	When SBC receives UPDATE message with SDP	SBC respond with 491 for update message	8.0.1.0
3	AURORA-23073	Enable RTCP report generation on Trunk side of SBC	Enable RTCP report generation in a trunking SBC caused crash, about twice a day.	8.0.1.0
4	AURORA-24631	SBC generating RTCP message	SBCE crashed when generating the RTCP msg	7.2.2.4
5	AURORA-23882	Refer Handling enabled with transferee use UDP transport	SBCE routes re-INVITE on wrong transport	8.0.1.0, 8.1.1.0, 7.2.2.5
6	AURORA-23672	After 30s of call, enter DTMF.	SBCE is not converting the SIP INFO signal * and # to RFC 2833	8.0.1.0, 8.1.1.0, 7.2.2.5
7	AURORA-21991	When the message contains large number of custom headers	traceSBC doesn't show gethomeresponse passing toward endpoint	8.1.0.0
8	AURORA-23854	Race condition between BYE and Re-Invite	SBC not processing any messages if stale call resources hanging for more than an hour	7.2.2.5
9	AURORA-25040	SIP recording enabled	ssyndi crash when sip rec is enabled	8.1.1.0
10	AURORA-25192	SIPs not allowed, shuffling enabled in CM, one leg of the sip trunk is sip/rtp and other leg is sip/srtp	Few outbound calls from agent to SIP trunk failed, due to SBC used rtp after CM shuffle.	8.1.0.0

11	AURORA-22987	NA	SNMP OID's missing in 8.1 MIB version 113	8.1.0.0
12	AURORA-24733	Far end responds 481 to Re-Invite message sent by SBC.	Call leak - calls with response code 481 to RE-INVITE not cleared by SBCE	7.2.2.4
13	AURORA-24977	High Traffic	SBCE audit (IPO Call Cleanup) clean up the call leg even when it has signaling in the last few secs	8.1.0.0
14	AURORA-25072	Offer with multiple G722 codec (with different sampling) and different payload number	SBCE - Removes the G722 codec number 9 when multiple G722 offers are available	7.2.2.5
15	AURORA-24644	UI limitation	user cannot add/edit secondary DNS server in GUI	8.1.1.0
16	AURORA-25402	Create a new TLS Server Profile and assign to it the existing ID certificate that is already in use on the original TLS profile. Then, on the RW Signaling Interface, just change the TLS Server Profile to the new profile	TLS Server Profile doesn't update correctly in Signaling Interface	8.1.0.0
17	AURORA-23528	Remote worker with dual registration	One-way audio issue on RW while media Anchoring is disable	7.2.2.2
18	AURORA-25409	Run traceSBC for HTTP/WebRTC messages	Service disruption when user run tracesbc with captturing HTTP/WEBRTC traffic in SBC	7.2.2.6
19	AURORA-25361	RTCP monitoring enabled	memory rapidly leak in RW SBC, likely due to that RTCPmonitoring feature, after install hotfix sbce-8.1.0.0-14-19623	8.1.0.0
20	AURORA-25542	Handling 200 response to CCMS message from IPO.	ssyndi process restarting multiple times a day due to state machine couldnt process the request.	8.1.1.0
21	AURORA-25515	Handling multiple error response from far node	SSYNDI crashed on SBC 8.0.1.0-19154	8.0.1.0
22	AURORA-25530	Enable Refer handling with delayed SDP	SBCE adds wrong dialog contact in the Request URI of BYE	8.1.1.0
23	AURORA-23653	Race conditions between ReInvite(replace) and BYE	INVITE Replace: Notify and BYE are not routed to Recorde routes	8.1.1.0
24	AURORA-24709	When main call is SRTP passthrough and ROC value incremented	audio (sometime trunk user side, sometimes both sides) are missing in selective SIPrec recorder	8.1.0.0
25	AURORA-22546	NA	CE Found open TCP Ports owned by java process on B1 interface.	8.0.0.0

26	AURORA-23790	NA	CVE-2020-10713 security vulnerability	7.2.2.4
27	AURORA-25703	Use snmp passphrase with more than 12 characters.	oampserver is crashing when snmp auth passphrase exceeding 12 characters	8.1.1.0
28	AURORA-23657	RTCP monitoring enabled	SBC crash due to port leak of RTCP msg after applying patch 8.1-19115	8.1.0.0
29	AURORA-25753	Message glare/Race conditions	SBE wrongly detects glare and removes SDP on calls involving 401 Unauthorized response	8.0.1.0

Known Issues and Workaround

ID	Minimum Conditions	Visible Symptoms	Workaround (if any)
AURORA-25741		sbce remove part of diversion header results call failure in multi transfer scenario.	Fix planned in 7.2.2.7 monthly patch
AURORA-25314		SBC crash due to Call Walking DoS feature	Fix planned in 7.2.2.7 monthly patch
AURORA-25224		Frequent kernel crash observed causing abrupt system reboot	Fix planned in 7.2.2.7 monthly patch
AURORA-25859		Removal sha1 weak algorithm from the ssh config	Fix planned in 7.2.2.7 monthly patch
		Rollback from 7.2.2.7 to 7.2.2.0 fails with db creation and Not able to compare prev and current db schema versions	a.) Create /usr/local/ipcs/db/scripts/stopreplication.sql file with below contents: \c sbcedb BEGIN; SET LOCAL bdr.skip_ddl_locking = on; SET LOCAL bdr.permit_unsafe_ddl_commands = on; SET LOCAL bdr.skip_ddl_replication = on; SECURITY LABEL FOR bdr ON DATABASE sbcedb IS NULL; DELETE FROM bdr.bdr_connections; DELETE FROM bdr.bdr_nodes; SELECT bdr.bdr_connections_changed(); COMMIT; BEGIN; SELECT pg_terminate_backend(pid) FROM pg_stat_activity

			WHERE datname = current_database() AND application_name LIKE '%): perdb'; DROP EXTENSION bdr CASCADE; DROP EXTENSION btree_gist; COMMIT; b.) Save the file. c.) # psql -U postgres -d sbcedb sbcedb=# \i /usr/local/ipcs/db/scripts/stopreplication.sql sbcedb=#\q 1.) #/etc/init.d/ipcs-db stop 2.) #/etc/init.d/ipcs-db start 3.) #psql -U postgres -c "update pg_database set datallowconn = 'true' where datname = 'sbcedb';" 4.) #psql -U postgres \c sbcedb select slot_name from pg_replication_slots where database = 'sbcedb'; select pg_drop_replication_slot ('<slot_name>'); where slot_name is output returned by previous command \c postgres update pg_database set datallowconn = 'false' where datname = 'sbcedb'; select pg_terminate_backend (pid) from pg_stat_activity where pg_stat_activity.datname = 'sbcedb'; drop database sbcedb ; \q 5.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbcreate --dbname sbcedb --dbtype sbcedb 6.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbimport default --dbname sbcedb --dbtype sbcedb 7.) #mkdir -p /archive/temp/dbBackup For rollback issue to 7.2.2.0 use the below command:

			#tar xjfm /archive/backup/db/db.7.2.2.0-15522.tar.bz2 -C /archive/temp/dbBackup #chmod 755 -R /archive/temp/dbBackup #/usr/local/ipcs/db/scripts/dbupgrade.py --upgrade-dir /archive/temp/dbBackup/dat --upgrade 1 8.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbimport upgrade --dbname sbcedb --dbtype sbcedb 9.) #rm -rf /archive/temp/dbBackup 10.) #/usr/local/ipcs/db/scripts/handleHAUpgrade.py --mgmt-ip=<MGMT_IP of primary> --node-id=<Node id of primary> --ems-addr=<EMS address> --new-version=<Current version number> --ha-info=Primary --ipcs-id=<IPCS_ID> 11.) In /usr/local/ipcs/etc/sysinfo: set UPGRADE_STATE as below : UPGRADE_STATE=UPGRADE_COMPLETED (The UPGRADE_STATE will be either UPGRADE_FAILED or RPMS_INSTALLED . Update it to UPGRADE_COMPLETED) 12.) # SBCEConfigurator.py update-connection-info 13.) Reboot #/sbin/reboot **If DB Issue happens on higher node id sbce, follow the below steps on Higher node id sbce:** ========== a.) Create /usr/local/ipcs/db/scripts/stopreplication.sql file with below contents: \c sbcedb BEGIN; SET LOCAL bdr.skip_ddl_locking = on; SET LOCAL bdr.permit_unsafe_ddl_commands = on; SET LOCAL bdr.skip_ddl_replication = on; SECURITY LABEL FOR bdr ON DATABASE sbcedb IS NULL; DELETE FROM bdr.bdr_connections; DELETE FROM bdr.bdr_nodes; SELECT bdr.bdr_connections_changed();

			COMMIT; BEGIN; SELECT pg_terminate_backend(pid) FROM pg_stat_activity WHERE datname = current_database() AND application_name LIKE '%): perdb'; DROP EXTENSION bdr CASCADE; DROP EXTENSION btree_gist; COMMIT; b.) Save the file. c.) # psql -U postgres -d sbcedb sbcedb=# \i /usr/local/ipcs/db/scripts/stopreplication.sql sbcedb=#\q 1.) #/etc/init.d/ipcs-db stop 2.) #/etc/init.d/ipcs-db start 3.) #psql -U postgres \c sbcedb select slot_name from pg_replication_slots where database = 'sbcedb'; select pg_drop_replication_slot ('<slot_name>'); where slot_name is output returned by previous command update pg_database set datallowconn = 'false' where datname = 'sbcedb'; select pg_terminate_backend (pid) from pg_stat_activity where pg_stat_activity.datname = 'sbcedb'; drop database sbcedb ; \q 4.) From command line execute below commands to create database without any schema: /usr/local/ipcs/db/scripts/dbmanage.py --dbcreate -- dbname sbcedb --dbtype sbcedb --no-schema True 5.) Execute below script to join bdr group: /usr/local/ipcs/db/scripts/handleHAUpgrade.py -- mgmt-ip=<MGMT_IP of secondary> --node-id=<Node id of secondary> --ems-addr=<EMS address> --new-

			version=<Current version number> --ha-info=Secondary --ipcs-id=<IPCS_ID> 6.) In /usr/local/ipcs/etc/sysinfo: set UPGRADE_STATE as below: UPGRADE_STATE=UPGRADE_COMPLETED (The UPGRADE_STATE will be either UPGRADE_FAILED or RPMS_INSTALLED Update it to UPGRADE_COMPLETED) 7.)# SBCEConfigurator.py update-connection-info 8.) Reboot /sbin/reboot
		Rollback from 7.2.2.7 to 7.2.2.6/7.2.2.5/7.2.2.4 fails in DB creation	**DB Issue happens on low node id sbce, follow the below steps:** 1.) #/etc/init.d/ipcs-db stop 2.) #/etc/init.d/ipcs-db start 3.) #psql -U postgres -c "update pg_database set datallowconn = 'true' where datname = 'sbcedb';" 4.) #psql -U postgres \c sbcedb select slot_name from pg_replication_slots where database = 'sbcedb'; select pg_drop_replication_slot ('<slot_name>'); where slot_name is output returned by previous command \c postgres update pg_database set datallowconn = 'false' where datname = 'sbcedb'; select pg_terminate_backend (pid) from pg_stat_activity where pg_stat_activity.datname = 'sbcedb'; drop database sbcedb ; \q 5.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbcreate --dbname sbcedb --dbtype sbcedb 6.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbimport default --dbname sbcedb --dbtype sbcedb 7.) #mkdir -p /archive/temp/dbBackup

			For 7.2.2.6 use the below command: #tar xjfm /archive/backup/db/db.7.2.2.6-19436.tar.bz2 -C /archive/temp/dbBackup For 7.2.2.5 use the below command #tar xjfm /archive/backup/db/db.7.2.2.5-18982.tar.bz2 -C /archive/temp/dbBackup For 7.2.2.4 use the below command #tar xjfm /archive/backup/db/db.7.2.2.4-18529.tar.bz2 -C /archive/temp/dbBackup #chmod 755 -R /archive/temp/dbBackup #/usr/local/ipcs/db/scripts/dbupgrade.py --upgrade-dir /archive/temp/dbBackup/dat --upgrade 1 8.) #/usr/local/ipcs/db/scripts/dbmanage.py --dbimport upgrade --dbname sbcedb --dbtype sbcedb 9.) #rm -rf /archive/temp/dbBackup 10.) #/usr/local/ipcs/db/scripts/handleHAUpgrade.py --mgmt-ip=<MGMT_IP of primary> --node-id=<Node id of primary> --ems-addr=<EMS address> --new-version=<Current version number> --ha-info=Primary --ipcs-id=<IPCS_ID> 11.) In /usr/local/ipcs/etc/sysinfo: set UPGRADE_STATE as below : UPGRADE_STATE=UPGRADE_COMPLETED (The UPGRADE_STATE will be either UPGRADE_FAILED or RPMS_INSTALLED . Update it to UPGRADE_COMPLETED) 12.) # SBCEConfigurator.py update-connection-info 13.) Reboot #/sbin/reboot **If DB Issue happens on higher node id sbce, follow the below steps on Higher node id sbce:** ==========

			a.) Create /usr/local/ipcs/db/scripts/stopreplication.sql file with below contents: 1.) #/etc/init.d/ipcs-db stop 2.) #/etc/init.d/ipcs-db start 3.) #psql -U postgres \c sbcedb select slot_name from pg_replication_slots where database = 'sbcedb'; select pg_drop_replication_slot ('<slot_name>'); where slot_name is output returned by previous command update pg_database set datallowconn = 'false' where datname = 'sbcedb'; select pg_terminate_backend (pid) from pg_stat_activity where pg_stat_activity.datname = 'sbcedb'; drop database sbcedb ; \q 4.) From command line execute below commands to create database without any schema: /usr/local/ipcs/db/scripts/dbmanage.py --dbcreate --dbname sbcedb --dbtype sbcedb --no-schema True 5.) Execute below script to join bdr group: /usr/local/ipcs/db/scripts/handleHAUpgrade.py --mgmt-ip=<MGMT_IP of secondary> --node-id=<Node id of secondary> --ems-addr=<EMS address> --new-version=<Current version number> --ha-info=Secondary --ipcs-id=<IPCS_ID> 6.) In /usr/local/ipcs/etc/sysinfo: set UPGRADE_STATE as below: UPGRADE_STATE=UPGRADE_COMPLETED (The UPGRADE_STATE will be either UPGRADE_FAILED or RPMS_INSTALLED Update it to UPGRADE_COMPLETED) 7.)# SBCEConfigurator.py update-connection-info 8.) Reboot /sbin/reboot

Security Upgrades

Note: Security updates that are published on or before 19th January 2021 and applicable to SBC 7.2.2.7 has been addressed in this service pack, listed below.

Advisory	Synopsys	Publish Date
https://access.redhat.com/errata/RHSA-2020:5566	Important: openssl security update	16 Dec 2020
https://access.redhat.com/errata/RHSA-2020:5437	Important: kernel security and bug fix update	15 Dec 2020
https://access.redhat.com/errata/RHSA-2020:5083	Moderate: microcode_ctl security, bug fix, and enhancement update	11 Nov 2020
https://access.redhat.com/errata/RHSA-2020:5011	Moderate: bind security and bug fix update	10 Nov 2020
https://access.redhat.com/errata/RHSA-2020:5009	Moderate: python security update	10 Nov 2020
https://access.redhat.com/errata/RHSA-2020:5002	Moderate: curl security update	10 Nov 2020
https://access.redhat.com/errata/RHSA-2020:4908	Important: libX11 security update	04 Nov 2020
https://access.redhat.com/errata/RHSA-2020:4350	Moderate: java-1.8.0-openjdk security and bug fix update	27 Oct 2020
https://access.redhat.com/errata/RHSA-2020:4076	Moderate: nss and nspr security, bug fix, and enhancement update	30 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4072	Moderate: libcroco security update	30 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4041	Moderate: openldap security update	30 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4032	Moderate: dbus security update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4026	Moderate: mariadb security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4011	Moderate: e2fsprogs security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4007	Low: systemd security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4005	Moderate: libxslt security updat	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4004	Important: tomcat security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:4003	Moderate: NetworkManager security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3996	Moderate: libxml2 security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3978	Moderate: glib2 and ibus security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3952	Moderate: expat security update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3915	Moderate: libssh2 security update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3908	Moderate: cpio security update	29 Sep 2020

https://access.redhat.com/errata/RHSA-2020:3902	Moderate: libtiff security update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3901	Low: libpng security update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3878	Low: dnsmasq security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3864	Moderate: cups security and bug fix update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3861	Low: glibc security, bug fix, and enhancement update	29 Sep 2020
https://access.redhat.com/errata/RHSA-2020:3848	Low: libmspack security updat	29 Sep 2020