Avaya Session Border Controller for Enterprise 8.1.3.0 Release Notes

Release 8.1.3.0
Issue 1
August 2021

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

Table of contents:

Overview

This document provides information about the new features/enhancements, upgrade support, platforms supported, software download information, list of fixed, known issues and workarounds in ASBCE Release 8.1.3.0

Licensing

New licensing codes have been introduced with 8.1.3.0 release.

New Features Introduced in 8.1.3.0 release

Edge Friendly Gateway

Avaya One Cloud Private® is a managed service offer from Avaya (private cloud) that has UC and CC call processing capabilities at core datacenters with endpoints, device adapters, H248 gateways at branches. The endpoints and gateways operate in local NAT address domains at the branch office sites, while the Avaya server products remains in the data centers. The data centers operate in a private address space as well. The Avaya SBCE supports end-to-end communication from the data centers to public service provider networks and ultimately serving the branch office sites. Avaya SBCE allows access of PRI trunk, DCP phones, Analog phones from branch to One Cloud Private core through public internet or SD-WAN. The feature is designed to keep media optimized and local to branch for all cases of PRI trunk. DCP phones, Analog phones, and SIP phones from within the same branch or across branches with a common NAT. Avaya SBCE provides media access to the One Cloud Private core in case of any media treatment is required from the One Cloud Private datacenter.
The G4xx gateways operating as an Edge Gateway are on the public network side of the Firewall from the Avaya SBCE. While Avaya Products within the Data Center communicates with private IP Addresses to the private network side of SBC, G4xx Gateways sends H248 signaling over a TCP/TLS connection toward port 2944 of Avaya SBC. Avaya SBC proxies H248 messages and NATs appropriate IP addresses and sets up the media path if anchored through the SBC. The Avaya SBCE acts as a H248 Proxy server to modify the address6 fields and forward these messages on toward TCP port 2944 on the Communication Manager. Management functionals on G4xx GW like SNMP, SCP, SSH are done using SBC relay mechanism, by tunneling these protocols via a proprietary protocol.

AMR (Adaptive Multi-Rate audio) codec

With 8.1.3 release, ASBCE Supports AMR (Adaptive Multi Rate codec, RFC 4867) and AMR-WB (Adaptive Multi Rate codec – Wideband, HD voice, RFC 4867) transcoding. AMR (narrowband) and AMR-WB (wideband) audio codecs used mostly in CDMA, GSM, 3G and LTE networks. Transcoding/Transrating is supported from AMR/AMR-WB to any other codec. AMR-WB codec involved sessions requires strict license enforcement due to royalties, AMR narrowband is treated as any other codec. AAMS is replaced with Jade Media Server in co-res deployment mode. External AAMS continues to be supported for transcoding as external server for the codecs other than AMR and AMR-WB. For NG911, supporting AMR/AMR-WB codec transcoding is mandatory as any mobile carrier can deliver 911 calls without transcoding resources in their network.

Media-Sec Support

MediaSec is a capability to distinguish security mechanisms that apply to the media plane by defining a new Session Initiation Protocol (SIP) header field parameter to label such security mechanisms. ASBCE added support for MediaSec in accordance with 1TR119 “Technical Specification of the SIP-Trunking Interface for CompanyFlex of Deutsche Telekom”

RTCP-Mon Enhancement

In the prior releases, SBCE used to send context ID in CNAME type field, for the Source Description Message. With release of ASBCE 8.1.3, SBC now adds UCID in 'Priv Type' of SDES message to have unique identifier at across calls. This is useful for the customers trying to correlate runtime media stats with a call from SM CDR.

Small Foot-Print Support on VMWARE

ASBCE 8.1.3 release now supports a smaller footprint on VMWARE for smaller deployments with following resource requirements. This type of deployment supports both SA-ASBCE [EMS+SBCE] and ASBCE only as well.

STUN/TURN Support with IPV6

TURN interface on Public or Enterprise side supports IPv6 or IPv4 and relay address on the opposite interface supports IPv6 or IPv4 towards AMS/MCU. The SBC Turn server converts Turn IPv6 for Stun/Turn/ICE messages to IPv4 for ICE and media. This is applicable for both Turn control messages and Turn media. HTTP load and health monitoring interface should support IPv6 or IPv4.

If Stun interface on public or private side is on IPv6 or IPv4, the reflexive address is always IPv6. SBC Stun Server does not support embedded IPv6 address for reflexive address. Embedded IPV6 address is not supported for Turn and ICE messages

CEC Compliance: FQDN support

SBCE uses FQDN for ASBCE address instead of IP address for headers added by ASBCE. Following are the applicable headers and operations:

Via - add, remove
Record-Route - add
Route - remove
Contact

This feature interworks with topology hiding. Topology hiding has precedence over this feature. The FQDN is configurable at end point flow level. If FQDN is not configured, fall back is to use IP address.

Upgrades

Before starting the upgrade, you must execute the pre-upgrade-check on each setup to verify the upgrade will succeed or not in that deployment. If pre-upgrade-check is passed, the upgrade can proceed, otherwise the Migration procedure must be followed. Upgrade and Migration procedures can be found in the "Upgrading Avaya Session Border Controller for Enterprise" document.

Supported Platforms for Upgrade

Below are the platforms which are supported for upgrading and installing ASBCE 8.1.3.0 release.

1. Dell R320
2. Dell R330
3. Dell R340
4. Dell R620
5. Dell R630
6. HP DL 360 G9
7. Portwell CAD-0230
8. VMWARE ESXI Version 6.5/6.7/7.0

9. ACP 3 and ACP 5
10. CAF 251

Migration only supported platforms

Below are the platforms which are supported for upgrading using migration procedure only and installing ASBCE 8.1.2.0 release.

1. HP DL360 G8
2. Nutanix
3. AWS
4. Azure

Migration procedure can be found in the Upgrading document(https://support.avaya.com/css/P8/documents/101063930)

Non-Supported Platforms

Below are the platforms which are not supported for upgrading or Installing ASBCE 8.1.3.0 release

1. CAD 0280

Pre-upgrade check procedure

Please follow pre upgrade check procedure mentioned in the following upgrade document https://downloads.avaya.com/css/P8/documents/101055506 on page 14 under section "Checking the current system for upgrade support"

Supported Upgrade paths

The following ASBCE versions are supported for upgrading directly to ASBCE 8.1.3.0

1. ASBCE 7.2.2.8
2. ASBCE 8.0.0.0
3. ASBCE 8.0.1.0
4. ASBCE 8.1.0.0
5. ASBCE 8.1.1.0
6. ASBCE 8.1.2.0

An ASBCE/EMS which is on a pre-7.2.2.0 version needs to first upgrade to 7.2.2.8 or 8.x version and then upgrade to ASBCE 8.1.3.0 release.

Note:

- Adding a secondary EMS with lower version to primary EMS with 8.1.3 version is not supported. In this case upgrading secondary the EMS will fail. You must add an 8.1.3 secondary EMS to the 8.1.3 primary EMS.
- Customers on 7.1.x release wanting to upgrade to 8.1.3 release, need to migrate to 8.1 release and then upgrade to 8.1.3 release

Upgrade through GUI from 8.0.x

In Avaya SBCE 8.1 and later, the size of the upgrade package is more than 2GB. Avaya SBCE 8.0.x (GA version) upgrade from GUI will fail. A patch must be installed on all EMS/SA-SBC before the upgrade. However, upgrading through CLI will not require any patch. Details of the patch are given below.

- **Upgrading from 8.0.0.0 [This is to be updated based on release numbers]**
  Requires sbce-8.0.0.0-19-16991-hotfix-11142019.tar.gz or later patch.
  sbce-8.0.0.0-19-16991-hotfix-11142019.tar.gz - MD5SUM: 7bdaa7dc0146911eab11a86cf532b37a

- **Upgrading from 8.0.1.0**
  Requires sbce-8.0.1.0-10- hotfix 17555-hotfix-10172019.tar.gz or later patch.
  sbce-8.0.1.0-10-17555-hotfix-10172019.tar.gz - MD5SUM: 5eb226ba5a0ee4044fdd2607c476bb37

- **Upgrading from 8.1.2.0**
  Requires sbce-8.1.2.0-37-21065-hotfix-08042021.tar.gz or later patch.
  sbce-8.1.2.0-37-21065-hotfix-08042021.tar.gz- md5sum: a942c1aa823f815a167a28bc3f34c965

Note: Please refer latest PSN release notes for respective SBCE releases for Hotfix/Patch installation procedure.

Software Downloads

Software downloads are available at following links:
https://support.avaya.com/downloads/
https://plds.avaya.com

File Name	PLDS ID	MD5SUM	Remarks
sbce-8.1.3.0-31-21052-563c74d7bdc7b0d1115031a5fa0f1927.tar.gz	SBCE0000253	563c74d7bdc7b0d1115031a5fa0f1927	Upgrade package for upgrade 8.1.3.0 release
sbce-8.1.3.0-31-21052-563c74d7bdc7b0d1115031a5fa0f1927.tar.gz.asc	SBCE0000254	f2f9023b2752671be9c4d200bc602b82	Signature file to be used to upgrade to 8.1.3.0 release
sbce-8.1.3.0-31-21052-signatures.tar.gz	SBCE0000255	6a7c960613c01e1e450895ea5edbdfa5	Key Bundle to validate RPM signatures
sbce-8.1.3.0-31-21052.iso	SBCE0000250	92f28cc016392ca616a8fd3b2e5e5e53	ISO image for fresh install on hardware
sbce-8.1.3.0-31-21052.ova	SBCE0000249	f2c7c1d2e8b54c86da8d8535a96660a7	OVA for fresh Installation on VMWare Note: Please refer to Known issue section and its workaround
sbce-8.1.3.0-31-21052-aws-001.ova	SBCE0000256	2d68e3e139c4679b3d75d1447ed6527b	OVA for Fresh Installation on AWS Platform
sbce-8.1.3.0-31-21052.qcow2	SBCE0000251	ec6161cf4f36d8dfda1fc92c5e235c43	QCOW2 image for fresh installation on Nutanix and Azure
sbce-8.1.3.0-31-21052_2dbf5ef8901e7491644bd3ab130125eb.img	SBCE0000252	814819d449246aabb0a1263b604fe2d5	Image file for creating USB Installer for fresh install on hardware
sbce-8.1.3.0-31-21052_uberutility-0c6ad4acbfc832f7e8bd1dea5125ef93.tar.gz	SBCE0000257	0c6ad4acbfc832f7e8bd1dea5125ef93	Uber utility Script is applicable for migration only, one must use target release uber utility Script for migration
AVAYA-SBCE-MIB_R811.mib	SBCE0000202	774e62365af182661de5a99519acaf1f	MIB File for ASBCE 8.1.2.0

Documentation

Title	Support Site Link
Avaya Session Border Controller for Enterprise Overview and Specification	https://support.avaya.com/css/P8/documents/101063920
Deploying Avaya Session Border Controller for Enterprise on a Hardware Platform	https://support.avaya.com/css/P8/documents/101063922
Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform	https://support.avaya.com/css/P8/documents/101063924
Deploying Avaya Session Border Controller for Enterprise on an Avaya Aura® Appliance Virtualization Platform	https://support.avaya.com/css/P8/documents/101063926
Deploying Avaya Session Border Controller for Enterprise on an Amazon Web Services Platform	https://support.avaya.com/css/P8/documents/101070040
Deploying Avaya Session Border Controller for Enterprise on a Microsoft Azure Platform	https://support.avaya.com/css/P8/documents/101069884
Upgrading Avaya Session Border Controller for Enterprise	https://support.avaya.com/css/P8/documents/101063930
Administering Avaya Session Border Controller for Enterprise	https://support.avaya.com/css/P8/documents/101063932
Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise	https://support.avaya.com/css/P8/documents/101063938
Working with Avaya Session Border Controller for Enterprise and Microsoft Teams	https://support.avaya.com/css/P8/documents/101069910
Working with Avaya Session Border Controller for Enterprise Multi-Tenancy	https://support.avaya.com/css/P8/documents/101063934
Working with Avaya Session Border Controller for Enterprise Geographic-Redundant Deployments	https://support.avaya.com/css/P8/documents/101063936
Avaya Session Border Controller for Enterprise 8.1.3 PDF Library	https://support.avaya.com/css/P8/documents/101066431
Avaya Session Border Controller for Enterprise Release Notes	https://download.avaya.com/css/public/documents/101076998
Avaya Session Border Controller for Enterprise Port Matrix	https://support.avaya.com/css/P8/documents/101064449
Avaya Session Border Controller for Enterprise Product Privacy Statement	https://support.avaya.com/css/P8/documents/101063993
Avaya SBCE 8.1 Security Configuration and Best Practices Guide	https://support.avaya.com/css/P8/documents/101065050

List of Known Issues with Workarounds

Issue Summary	Workaround
SBC may show “The Certificate is not trusted” and “The OVA package contains advanced …” warnings during OVA installation on ESXI/Vmware.	Ignore the warnings and proceed for installation. For more details on “The Certificate is not trusted” and “The OVA package contains advanced wanning, you may refer to Vmware KB article: https://kb.vmware.com/s/article/84240
Network management in SBC: after change default gateway on GUI, old default gateway record does not be wiped out from ip route table	Reboot required on both HA SBCEs
While deployment of fresh installation on AVP, user may encounter some related to interface names and plugin () is failing	Continue to deployment to finish Change the interfaces with respect to mac address after deployment on AVP
EMS GUI was not coming UP (Nginx process is not coming up) due to IPV6 address after upgrade from 7.2.2.x to 8.1.3.0	By following below work around and this work around should be followed in EMS and SBC's as well. Open sysinfo file /usr/local/ipcs/etc/sysinfo Change the line MGMT_IP_V6=2a07:2a41:ae05:103:10:130:19:55 To: MGMT_IP_V6= Open the file: /usr/local/nginx/conf/GUI-nginx-main.conf Change the line listen [2a07:2a41:ae05:103:10:130:19:55]:443 ssl; ## EMS MGMT_IP v6 To: listen [::1]:443 ssl; ## EMS MGMT_IP v6 Restart nginx-mgmt
SBCE Upgrade from 7.2.2.8 to 8.1.3 shows upgrade failed	Upgrade was progressing at the backend and status shows as Upgrading, the logs were showing failed, but after while SBCE's came back up fine upgraded to 8.1.3.0
Edge-friendly Gateway - One way talk path when SIP phone calls DCP phone in same branch for Un-anchor	As a workaround configure matching encryption media policy on both legs of ASBCE with same media setting on CM
Media is anchored on SBC in case of Encrypted RTCP/Interworking Enabled	Workaround is to match SBCE media policy configuration with phones offer
Syslog configuration changes do not take effect immediately	Workaround is to restart the Syslog service
Failure of Transcoding calls beyond 20k	Removed 4sec transaction timers from server interworking
DYNAMIC_LICENSING_ENABLED is not updated on transition from dynamic -> static license	workaround is to delete the DYNAMIC_LICENSING_ENABLED entry from the SS_CONFIG_PARAMETERS table on every SBCE with assistance from Support team
nginx process fails to start if FQDN in Reverse Proxy cannot be resolved or DNS Server is unreachable	Workaround is to fix the DNS Server reachability

Final page for OVA deployment doesn't show summary values for VMWARE-ESXI 7.0	Continue to deploy the OVA by completing the process without summary values in display
Radius Role name should display '0' after upgrade from Previous release	default attribute is displayed correctly after deleting '0'

List of fixed issues

Key	Summary
AURORA-27405	NG911 call fails after upgrading to 8.1.3.0-20940
AURORA-27371	SBCE fails to rewrite the PPMServiceURI in the PPM getHomeCapabilitiesResponse
AURORA-27185	ASBCE Training option in EMS help menu redirects to no offer available error page
AURORA-27152	Continuous ssyndi restart due to loop cause by Routing profile misconfiguration
AURORA-27141	SBCE GUI vulnerability to XSS attack (Syslog Viewer)
AURORA-27134	Sip Recorder-Server Flow match failed with URI group
AURORA-27113	SBCE crashing when SIP trunk towards SP with authentication and registration with ping
AURORA-27097	Migration failure from 7.1.0.8-01-17404 to 8.1.0 GA failed
AURORA-26986	destination custom port (4digit) assignment for SNMP configuration doesn't work
AURORA-26977	200 OK is not Processed by SBC due to MID Present in SDP Attribute
AURORA-26954	Ssyndi process on secondary server crashes continuously during HA serialization
AURORA-26952	Remote Workers unable to register with regular expression rules, if header is IPV6
AURORA-26950	SBC crash after applying 8.1.2.0-37-20545 hotfix, when RW phone register, with server profile as customer in routing profile
AURORA-26901	NG911 Call transfer fail with Service Provider send in URN Request Line in ReINVITE after transfer
AURORA-26889	SBC's on the EMS dashboard do not appear in order
AURORA-26854	snap-shot creation failed "Cannot read status file 'client_file_name'"
AURORA-26853	SBCE changes DTMF payload event type 101 to 97 when transcoding and codec prioritization is enabled
AURORA-26846	DB update script update_commondb_5608.sql fails in migration from 7.1.0.2 to 8.1.2
AURORA-26774	Call transfer failed because SBC fall into "semi_attended transfer" state
AURORA-26762	After REFER, SBCE routes PRACK on wrong transport
AURORA-26731	SBC drop the SDP over 200 ok with 2543 interworking and PRACK in 180Ringing
AURORA-26683	Approx. 30 sec RTP lost in failover test by unplugging A1/B1 cables
AURORA-26627	After upgrading to SBCE 7.2.2.7 when user hold and unhold there is no audio (SBCE return 491 Request pending response)
AURORA-26532	SBC did not switch the media ports as expected to SIPREC recorder.
AURORA-26488	RHSA-2020:4285, CVE-2020-25692, RHSA-2020:5023, CVE-2020-15778
AURORA-26362	SSYNDI crash while processing REGISTER message

AURORA-26358	After adding second IP Address to the B2 Interface, OPTIONS (keepalive) message from SBC to trunk server on the same B2 interface was failing.
AURORA-26337	spirit agent using 100% CPU in 7.2.2.6
AURORA-26172	localweblm license in grace period after upgrade to 8.1.2, due to license not preserved during upgrade
AURORA-26161	SBCE crash when it processes the re-invite from AWG
AURORA-26130	SSYNDI crash in handle_relay_provitional_msg
AURORA-26128	upgrade will fail if the server status is REGISTERED from 8.1.x to 8.1.2
AURORA-26062	upgrade successful with no DB data for EMS/SBC on 8.1.2 release
AURORA-25963	SBCE doesn't forward cancel when caller hangs up the call
AURORA-25943	"parsing error" after upgrade to 8.1.2
AURORA-25913	SBCE relaying the incorrect ip address in SDP towards SM
AURORA-25892	CVE Security - Multiple security vulnerabilities detected in 8.1.2
AURORA-25863	SSYNDI crash if cancel is received while waiting for DNS response
AURORA-25861	SBC crash due to subscriberInfoMap in 8.1.1
AURORA-25859	removal sha1 weak algorithm from the ssh config
AURORA-25753	SBE wrongly detects glare and removes SDP on calls involving 401 Unauthorized response
AURORA-25741	sbce remove part of diversion header results call failure in multi transfer scenario.
AURORA-25704	custom defined variables in sigma script not working
AURORA-25703	oampserver is crashing when SNMP auth passphrase exceeding 12 characters
AURORA-25624	SSYNDI crash on media tunneling calls to Video enabled meeting rooms
AURORA-25615	Out of 3 servers, one server doesn't REGISTER to priority server and other 2 servers are REGISTERED with priority servers
AURORA-24735	SYSMON process getting stopped
AURORA-23334	snmpd service status shows as failed even when snmpd process is running
AURORA-23328	turn controller logging the logs in /var/tmp directory and no log rotation on those logs
AURORA-23327	SBCE snapshot to windows SFTP remote server fails
AURORA-22402	Nginx doesn't use HTTP/1.1 for upstream, even if the request from downstream was on http/1.1, in RP
AURORA-21163	localweblm not able to load in a license in 8.1
AURORA-19029	SBC terminates a call on hold with complete silence after about 20 min

Security Updates Fixed in 8.1.3.0 release

JIRA	Advisory
AURORA-27231	RHSA-2021:2314
AURORA-26488	RHSA-2020:5023

AURORA-27233	RHSA-2021:2260
AURORA-27232	RHSA-2021:2305
AURORA-27230	RHSA-2021:2357
AURORA-26984	RHSA-2021:2147
AURORA-26820	RHSA-2021:1389
AURORA-26822	RHSA-2021:1469
AURORA-26724	RHSA-2021:1071, RHSA-2021:0221
AURORA-26523	RHBA-2021:0623
AURORA-26524	RHBA-2021:0351
AURORA-27403	Update Tomcat to 9.0.50-1 to address CVE-2021-30640

List of Open issues

Key	Summary
AURORA-27523	SBCE statistics window doesn't show remote users subscription status
AURORA-27332	Edge Friendly Gateway - One way talk path when SIP softphone calls DCP phone in the same branch
. AURORA-27499	6 secs RTP loss when primary SBCE is abruptly shutdown with SBCE-HA Environment
AURORA-27365	SBCE Upgrade from 7.2.2.8 to 8.1.3 shows upgrade failed, although upgrade runs fine in back-end
AURORA-27363	Final page for OVA deployment doesn’t show summary values
. AURORA-27384	Media is anchored on SBC in case of Encrypted RTCP/Interworking Enabled for Un-anchored call
. AURORA-27293	SRTP handling: Call failed if RWs offer different media encryption type
AURORA-27524	Security RHSA-2021:2725 Kernel-update, RHSA-2021:2784: java-11-openjdk-11.0.12.0.7-0, RHSA-2021:2845 for Update java-1.8.0-openjdk,
. AURORA-25268	‘Clear Cache’ button for LDAP is always grayed out