SBC Core

Release Notes

Software Release: 12.01.05R000
Document Revision: 01.01
Published: 28 March 2025

Contents

SBC Core RAMP support only

Beginning with release 12.0, the SBC Core supports the Ribbon Application Management Platform (RAMP), which replaces the EMS. However, the EMA, CLI and API will continue to include EMS-labeled parameters and screens to facilitate SBC migrations from older releases. Accordingly, any references to "EMS" in this documentation pertain to the RAMP platform.

Refer to Migrate Insight EMS to RAMP for additional details.

Note

For CNe download details, contact your designated Ribbon representative.

About SBC Release Notes

This release note describes new features, the latest hardware and software requirements, known limitations and other pertinent release information for the latest release of SBC Core.

Please note that all Ribbon bugs reported by customers on a given software release will be fixed in the latest release on that software release branch.

To view and download the latest End of Product Sale (EoPS) and other End Of Life (EOL) notices, navigate to the Resource Library on the corporate website (https://ribboncommunications.com/company/get-help/resource-library).

Related Documentation

The SBC Core 12.01.x documentation is located at the following Wiki space: SBC Core 12.1.x Documentation

Release Notes Use and Distribution

Associated Ribbon Announcements

The following Ribbon announcements (formerly known as WBAs) are referenced in this release note:

Bulletin ID	Description	Fixed in Release
Warning-17-00022689	Duplicate Trunk Group or Zone names can cause unexpected behavior	6.1.0
Warning-14-00020748	Verify system and databases are fully in sync prior to Live Software Upgrade (LSWU). Applies to all SBC platforms (HW, SWe, Cloud) except the SBCs deployed in a Distributed SBC (D-SBC) architecture	N/A
Warning-22-00030027	Verify ESXi Version Prior Software Upgrade to 10.1.x or 9.2.3	9.2.3, 10.1.x

To view/subscribe to announcements (Warnings, Bulletins, Alerts, or PCNs):

1. Click here to go to the "Announcements" page in the Ribbon Support Portal.
2. Enter the announcement number (last eight numbers) in the search field and click the magnifying glass icon (or press **Return**). You can alternatively use the filter tools located on the left side of the screen to narrow your search.

Problems or Questions

For problems or questions, contact the Global Support Assistance Center:

Ribbon Support Portal: https://ribboncommunications.com/services/ribbon-support-portal • **Voice**: +1-833-RIBBON1 (1-833-742-2661)

About SBC Core

The SBC Core platforms address the next-generation needs of SIP communications by delivering media transcoding, robust security and advanced call routing in a high-performance, 2RU, and 5RU form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP trunking, secure Unified Communications and Voice over IP (VoIP).

For more product information, refer to the section About SBC Core in the main documentation space.

Note

Unless explicitly specified, SBC Core features are not supported over GW. Please contact your Ribbon account team/channel partner for further details.

Compatibility with Ribbon Products

Tip

When upgrading your network, upgrade each product to the most current release to take advantage of the latest features, enhancements, and fixes.

Info

For complete interoperability details between various Ribbon products, including backwards compatibility, refer to Ribbon Product Interoperability.

Refer to SBC Core Portfolio Interoperability Matrix for the latest and minimum compatible product versions supporting this release.

New Features

New Features in 12.01.05R000 Release

Refer to New in SBC 12.01.05R000.

New Features in Previous Releases

For the list of features in previous 12.01.xx releases, refer to the following release notes.

- New in SBC 12.01.04R000
- SBC Core 12.01.03R000 Release Notes
- ENGINEERING DRAFT SBC Core 12.01.02R000 Release Notes
- SBC Core 12.01.01R000 Release Notes
- SBC Core 12.01.00R000 Release Notes

Sample Heat Templates Included in This Release

To instantiate the SBC instances, use the following templates:

SBC Heat Templates

Template Name	Description
heatRgNoDhcp.yaml	Used to instantiate no DHCP, IPv4 or IPv6 deployments. The template supports I-SBC, M-SBC, S-SBC, MRFP and SLB node types. This template includes instructions to enable port redundancy.
heatOamNoDhcp.yaml	Used to instantiate an OAM node.
heatRgNoDhcp-TSBC-template.yaml	Used to instantiate a T-SBC node.

Note

Example template files are packaged together in .tar.gz and .sha256 files separate from the SBC Core application installation and upgrade files:

- cloudTemplates.tar.gz
- cloudTemplates.tar.gz.sha256

Compute Host Hardware and Software Requirements

The system hosting the SBC SWe Cloud must meet specific requirements.

Note

Each subsection specifies the minimum supported hardware configuration, but must accommodate the actual VM sizing of all VMs deployed on the compute hardware.

Note

For more information about the supported range of VM sizing, refer to the SBC Provisioning Limits.

Note

CNe (global) products are installed on Kubernetes clusters operating on bare-metal servers supplied by the customer. Ribbon does not provide hardware and software resources for these clusters; the operators' network engineers must provide the resources.

For details on specified hardware and software requirements refer to one of the following links:

- OpenStack Hardware and Software Requirements
- KVM Hypervisor Hardware and Software Requirements
- VMware Hardware and Software Requirements

Required Software and Firmware Versions

The following SBC 5400 and SBC 7000 software and firmware versions are required for this release. For 5xx0, the BIOS is installed during application installation; whereas, for 5400 and 7000, the BMC/BIOS is included in the firmware package and installed during the firmware upgrade.

Important

The SBC 5100, SBC 5110, SBC 5200, and SBC 5210 platforms are no longer supported beginning with the SBC Core 10.0.0R0 release. This release supports SBC 5400/7000/SWe/Cloud Native edition (CNe) platforms. Contact Ribbon Sales for upgrade information.

How to Verify Currently Installed Software/Firmware Versions

Use the EMA to verify the currently installed software and firmware versions.

Log on to the EMA, and from the main screen navigate to **Monitoring** > **Dashboard** > **System and Software Info**.

Firmware

SBC Core BMC Firmware

Note

In the table below, versions in blue font indicate changes since the previous supported release.

Platform	12.01.04Rx
SBC 5400	BMC: V03.28.00-R000 BIOS: V1.18.0
SBC 7000	BMC: V03.28.00-R000 BIOS: V2.14.0

SBC 5400 Firmware

- firmware-5400-V03.28.00-R000.img
- firmware-5400-V03.28.00-R000.img.md5

SBC 7000 Firmware

- firmware-7X00-V03.28.00-R000.img
- firmware-7X00-V03.28.00-R000.img.md5

Note

Use the Method Of Procedure (MOP) below only to upgrade the FPGA image of an SBC 7000 DSP-LC card when the SBC 7000 DSP-LC FPGA version is 0x14. The MOP can be applied at any version time, with the only restriction being that the BMC firmware version is at least 1.25.0. However, if the SBC application is running version V05.01.00R000 or higher, then the DSPs will be set to disabled and transcoding and transrating calls will fail if the SBC 7000 DSP-LC FPGA version is 0x14. Therefore, it is necessary to upgrade the SBC 7000 DSP-LC FPGA if the version is 0x14, before upgrading the SBC to 5.1.0. However, the MOP can be applied if the application version is higher than 5.1.0. Click Here to view the 550-06210_DSP-LC_FPGA_Upgrade_MOP.

Software Bundles

The following software release bundles are available for download from the Customer Portal:

- SBC_Core-12.01.05R000

Download the appropriate software packages for your desired configuration. Refer to Downloading Software from the Global Software Center.

Note

When upgrading from release 9.0 and above, upload the SHA256 checksum file. Otherwise, use the MD5 file.

Note

For CNe download details, contact your designated Ribbon representative.

SBC Core Operating System Installation Package

The ConnexIP Operating System installation package for SBC Core:

- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.iso
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.iso.sha256

Note

Once the ConnexIP ISO procedure is completed, the SBC application package is automatically uploaded to SBC platforms.

SBC Core Application Package

The SBC Application installation and upgrade package for SBC Core:

- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.qcow2
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.qcow2.sha256
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.qcow2.md5
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.ova
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.ova.sha256
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.iso.sha256

- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.iso.md5
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.iso
- sbc-V12.01.05-R000.x86_64.tar.gz
- sbc-V12.01.05-R000.x86_64.sha256
- sbc-V12.01.05-R000.x86_64.md5
- sbc-V12.01.05-R000.x86_64.signature

For detailed information on installation and upgrade procedures, refer to SBC Core Software Installation and Upgrade Guide.

Cloud Service Archive (CSAR) Packages for VNFM Deployment on OpenStack

These files are for SBC SWe deployments in the OpenStack cloud using VNFM.

For VNFM deployment, the VNF Descriptor (VNFD) file is provided in a Cloud Service Archive (CSAR) package for the type of SBC cluster being deploying. VNFs are independent and CSAR definitions are imported into the VNFM via an Onboarding mechanism. There is a procedure for producing the required CSAR variant, for different personalities (S-SBC, M-SBC), different interface types (virtio, sriov).

Files required for CSAR creation:

- createVnfmCsar.py
- vnfmSol002VnfdTemplate.yaml
- sbc-V12.01.05R000-connexip-os_11.01.00-R000_204_amd64.qcow2

For detailed information on installation and upgrade procedures, refer to SBC Core Software Installation and Upgrade Guide.

For details on CSAR creation, refer to Creating a CSAR Package File for SBC SWe on OpenStack.

Accessing Public Cloud Images

Note

If you require assistance with accessing public could images , open a Salesforce case with the following details:

Azure: The SAS URL link required to access the Azure image is provided in the release notes and it is valid for six months from the time of the release. To extend this date, open a Salesforce case and include:

- Software release version

AWS:

- Software release version
- Customer AWS account ID
- Customer name
- AWS region where the image is required

GCP:

- Software release version
- Customer GCP project number
- Customer GCP registered email address

Azure SAS URL Links

AZURE_IMAGE_SASURL.txt

```
https://rbbncustomerimagestorage.blob.core.windows.net/swe-initial-image-share/
release-sbc-v12-01-05r000-03-26-25-02-10.vhd?
st=2025-03-26T02%3A40%3A34Z&se=2025-09-24T02%3A40%3A34Z&sp=r&sv=2021-06-08&sr=c&sig
=2CBmiP2d%2BKO%2Besyo9FFddg6NEB/qteDyWkQt8YLfuqA%3D
```

AZURE_IMAGE_SNAPSHOT.txt

```
/subscriptions/1c125f94-dd63-4190-97e3-2c353ca68b96/resourceGroups/SBC-Core-Images-
RG/providers/Microsoft.Compute/snapshots/release-sbc-
v12-01-05r000-03-26-25-02-10.snap
```

Ribbon OEM Host Operating System (ROHOS)

The minimum ROHOS version and the Dell firmware versions compatible with this release are provided below:

ROHOS	Dell Firmware
02.08.04 or higher	• iDRAC: iDRAC9 • BIOS: 5.00.20.10 • Firmware: 2.13.3

Use the following procedure when installing or upgrading an SBC SWe 1:1 HA pair on KVM using a QCOW2 image file and an ISO config drive you create using the CLI tool createConfigDrive.py:

Installation and Image Replacement Upgrade on KVM Using a QCOW2 File

Important Note Before Upgrading SBC SWe on VMware or KVM Hypervisor

The SBC Core includes a feature that extends the use of hyper-threading to SBC SWe when it is installed on either the VMware or KVM Hypervisor platform. To take advantage of the performance improvements provided by hyper-threading, you must increase (double) the number of vCPUs configured in the VM prior to a software upgrade if upgrading SBC SWe KVM Hypervisor or VMware from pre-07.01.00R000 release to 07.01.00R000 or higher.

If upgrading vCPUs from less than 10 to 10 or more, click here and perform the steps as described.

Upgrade Notes

Using older versions of ESXi can trigger a VM instance shutdown. To prevent this from occurring, you must upgrade the VMware ESXi -- refer to the End of General Support column on https://lifecycle.vmware.com/#/ for supported versions.

Note

Before a VNFM upgrade, make sure that the OAM and RAMP has connectivity.

If an OAM-RAMP connectivity has issues during an installation/upgrade, all nodes would come up and connectivity would try and run in the background. All post-services that are up and running must check if the RAMP connectivity is restored and if the RAMP cluster already has the previous config revisions stored, check if the first revision is uploaded to RAMP and marked as an active revision. If yes, restore the previous highest revision number.

Note

Customers using ERE Active Directory service (LDAP over TLS and AD server uses SHA1 hashing algorithm), they need to renew the certificates using SHA2 hashing algorithm. Alternatively, customers can ignore the server certificate validation at the SBC by manually updating the ldap.conf file(add new line 'TLS_REQCERT allow' in the file before the upgrade).

Note

Release 8.2 and later requires additional user account security practices for SBC SWe deployments in OpenStack cloud environments. During upgrade of SBC SWe cloud instances deployed using Heat templates, you must use a template that includes SSH keys or passwords for the admin and linuxadmin accounts. The example Heat templates have been updated to include information on how to specify this type of data in the userdata section of a template.

Note

For the procedure specific to SBC SWe upgrades on KVM Hypervisor or VMware to take advantage of performance improvements due to hyper-threading, refer to MOP to increase vCPUs Prior to Upgrading SBC SWe on VMware or KVM Hypervisor.

Note

The number of rules across SMM profiles in a system is limited to 10,000, and the number of actions across profiles in a system is limited to 50,000. Ensure these conditions are met before LSWU.

Note

In NFV environments, the method used for upgrades involves rebuilding the instance, which requires additional disk space on the host. The minimum disk space needed for this operation is listed in the table below.

Flavor	Extra Space Required (GB)
S-SBC	80
M-SBC	80
PSX-M	360
PSX-S	360

Flavor	Extra Space Required (GB)
PSX-Test	360
RAMP_SA	150

Note

SWe SBC software enforces I-SBC instances to run only with a single vNUMA node in order to achieve deterministic performance. SWe SBC VM having >8 vCPUs hosted on dual-socket physical server with VMware ESXi software needs to follow the steps below to correct vNUMA topology before upgrading to latest SWe SBC software:

- Check 'numa.nodeAffinity' settings on VM. It should be either 0 or 1 based on which NUMA node PKT ports are connected. The following command on ESXi host can be used to check PKT port NUMA affinity:

```
vsish -e get /net/pNics/<PKT port name - vmnicX>/properties | grep "NUMA"
```

If any of the above settings requires modification, follow the steps below on SWe SBC HA system:

- Shutdown the standby instance.
- If 'numa.nodeAffinity' settings are missing, add the following rows:

numa.autosize.once = FALSE

numa.nodeAffinity' = 0 or 1 (based on PKT port NIC affinity)

On ESXi 6.5 and above releases, vSphere web client can be used to add above rows under Edit settings > VM options > configuration parameters > add parameters;

For more information, refer to:

- Creating Virtual Machines using SR-IOV Interfaces
- Creating a New SBC SWe VM Instance with Direct IO Pass-Through

(The vSphere Distributed Switch feature is no longer supported)

Note

If the TRF/MRB Features are configured and enabled – some calls are unable to be cleared post upgrade if using the TRF/MRB attributes.

The upgrade is successful and calls continue but some calls may fail to clean up release post upgrade. Session KeepAlive and RTP Inactivity functions will clean any stale calls.

Enable the sessionKeepalive or rtpInactivity monitoring to ensure that mirrored calls are cleaned up post upgrade.

```
set addressContext default zone ZONE_AS sipTrunkGroup TG_AS_SIPP signaling timers sessionKeepalive <value>
```

-or-

```
set system media mediaPeerInactivity <value>
```

```
set profiles media packetServiceProfile DEFAULT peerAbsenceAction
peerAbsenceTrapAndDisconnect
```

Note

The SBC 11.1 and later versions do not support tls_ecdh_ecdsa_with_aes_256_cbc_sha384. You must replace it with a valid Cipher before upgrading the SBC. For more details, refer to Security Configuration - TLS Profile.

Important Upgrade Information

Warning

Prior to performing an upgrade to this release, you must remove usernames that do not conform to the SBC user-naming rules to prevent upgrade failure. Upgrade can proceed successfully after removing all invalid usernames. The following user-naming rules apply:

- Usernames can begin with A-Z a-z _ only.
- Usernames cannot start with a period, dash, or digit.
- Usernames can contain a period(.), dash(-), alphabetic characters, digits, or underscore(_).
- Usernames cannot consist of digits only.
- Usernames can contain a maximum of 23 characters.

The following names are not allowed:

tty disk kmem dialout fax voice cdrom floppy tape sudo audio dip src utmp video sasl plugdev staff users nogroup i2c dba operator

Note: Any CLI usernames consisting of digits only or not conforming to new user naming rules will be removed after performing a restore config in this release.

Warning

Prior to performing an upgrade to the 10.1 release, the dnsGroups with type mgmt must be specified/ updated with the "interface" field. The steps are included in announcement "W-17-00022847".
If the above MOP is not run, the LSWU process may fail because of duplicate trunk group or zone names.

Warning

Prior to performing an upgrade to 10.1 release, the duplicate trunk groups or zones must be removed. The steps are included in announcement "W-17-00022689".

Note

There is no CAM version change in 12.1.4. The CAM version for SBC 12.1.1 is 104.00.00 (major CAM version is 104, minor CAM version is 0, special CAM version is 0). The associated hex format of this CAM file version is 00680000.

Note

An SBC CNe upgrade using SIP Registrations is supported from 12.1.3 onwards.

Note

In case of upgrade scenario in CNF deployment, when DB goes for upgrade, there is a possibility that RAC will not be able to update the pod role information to the DB for few seconds. Due to this, RAC might go to a split-brain scenario. After resolving split-brain, if current active RAC gets standby role, then it goes for a graceful restart.

This will not impact any calls.

Warning

An SBC CNe-FR with ERE cannot be upgraded to 12.1.5.

SBC SWe Pre-Upgrade Requirements

VM CPU resource allocation requirements

CPU resource allocation requirements for SBC SWe VM are strictly enforced. You must review and verify these VM settings (including co-hosted VMs) against the documented "VM Configuration Recommendations" on the VMware Hardware and Software Requirements page before upgrading.

If you encounter a problem, correct the CPU reservation settings as specified in step 6 of the "Adjust Resource Allocations" procedure on Creating a New SBC SWe VM Instance with VMXNET3.

Set the CPU reservation for the VM so that it equals the physical processor CPU speed, multiplied by the number of vCPUs divided by two.

For example, a configuration of 4 vCPUs with a processor of 2.99 GHz CPU speed, reserve: 2992 * 4/2 = 5984 MHz

If the VM uses the same number of vCPUs as the number of physical processors on the server, this reservation may not be possible. In this case, reduce the number of vCPUs assigned to VM by **one** and set the CPU reservation to the appropriate value.

When using the `show table system serverSoftwareUpgradeStatus` command during the upgrade, the Standby server's LSWU status will always display "Upgrading" even though the upgrade may have failed due to **host checker validation**. To check if host validation failed for the Standby, check for **HostCheck Validation Failed** message in the `upgrade.out` log.

Manually check for Hostcheck Validation Failed message

Perform the following procedure on the Standby to check for the **Hostcheck Validation Failed** message in the `upgrade.out` log.

1. Log on to **ESXi** of the Standby SBC SWe.
2. Check in `/opt/sonus/staging/upgrade.out` (this log shows the **Hostcheck Validation Failed** error).
3. Power off the VM.
4. Reduce the number of vCPUs assigned to VM by **one** and set the CPU reservation to the appropriate value.

5. Power on the VM. The SBC SWe successfully upgrades to the latest version 6.2.0.
6. Run the command `show table system serverSoftwareUpgradeStatus` to confirm the successful upgrade.
7. Perform similar procedure for LSWU on Active.

Preparing for Upgrade (All Platforms)

Warning

Prior to performing a Live Software Upgrade (LSWU), verify if the system and the databases are in sync. The steps are included in announcement "Warning-14-00020748".

Warning

Customers who are using the SBC to interop with MS Teams need to review and compare their configuration against the latest configuration guide especially the SMM as it might result in call failures after upgrade if the older SMM is left in place. For more information, refer to the MS Teams Solution Guide.

(There are no changes to the *MS Teams Solution Guide* since release 8.2, so the guide is still applicable to later releases)

Supported Live Software Upgrade (LSWU) Paths

Attention

This release includes all bug fixes implemented in the releases which are documented in the Supported Upgrade Paths table of this release note. To view bug fixes in previous releases, refer to the release note(s) of interest from the SBC Core Documentation Home page.

The SBC Core supports Live Software Upgrades from the following releases:

V09.02.xx	V10.00.00Rx	V10.01.xx	V11.xx	V12.xx
V09.02.00 R000-R002	V10.00.00 R000-R004	V10.01.00 R000-R002	V11.00.00 R000	V12.00.00 R000
V09.02.01 R000-R010	V10.00.00 S100	V10.01.01 R000-R003	V11.01.00 R000-R001	V12.00.00 S100-S200
V09.02.02 R000-R009		V10.01.01 R100-R101	V11.01.01 R000-R007	V12.01.00 R000
V09.02.03 R000-R009		V10.01.02 R000-R003	V11.01.02 R000	V12.01.01 R000-R002

V09.02.xx	V10.00.00Rx	V10.01.xx	V11.xx	V12.xx
V09.02.04 R000-R006		V10.01.03 R000-R004		V12.01.02 R000-R003
V09.02.05 R000-R011		V10.01.04 R000-R004		V12.01.03 R000-R002
		V10.01.05 R000-R008		V12.01.04 R000-R000
		V10.01.06 R000-R001		

Security Vulnerabilities

The following security vulnerabilities are resolved in this release.

Note

The Severity is based on the CVSSv3.x scores. For more details about the individual CVE, refer to https://nvd.nist.gov/vuln/search. Some low severity issues may not be listed.

Severity	Fixed CVEs
Critical	4 (CVE-2021-29921,CVE-2024-47685,CVE-2022-36227,CVE-2022-48174)
High	143 (CVE-2024-49860,CVE-2025-21687,CVE-2024-49889,CVE-2024-57908,CVE-2024-57907,CVE-2024-47742,CVE-2024-50234,CVE-2024-53171,CVE-2024-50264,CVE-2024-56601,CVE-2024-46854,CVE-2023-52356,CVE-2024-50007,CVE-2024-50131,CVE-2024-47723,CVE-2024-46849,CVE-2024-57900,CVE-2024-50115,CVE-2024-49995,CVE-2021-42378,CVE-2024-47697,CVE-2024-50033,CVE-2024-53061,CVE-2024-56598,CVE-2024-56662,CVE-2024-50193,CVE-2021-3737,CVE-2024-49884,CVE-2024-53237,CVE-2024-7592,CVE-2024-56548,CVE-2024-50267,CVE-2024-20696,CVE-2024-50035,CVE-2024-53142,CVE-2024-57887,CVE-2024-49982,CVE-2024-47757,CVE-2024-50262,CVE-2024-56631,CVE-2024-56596,CVE-2021-42379,CVE-2024-56595,CVE-2024-53156,CVE-2024-38588,CVE-2024-49930,CVE-2024-57850,CVE-2024-49903,CVE-2024-50180,CVE-2024-38538,CVE-2024-47698,CVE-2024-50301,CVE-2024-57892,CVE-2022-42919,CVE-2021-42380,CVE-2024-44940,CVE-2024-49900,CVE-2024-49936,CVE-2024-53096,CVE-2021-28861,CVE-2024-50055,CVE-2024-47696,CVE-2024-9287,CVE-2024-57912,CVE-2024-56650,CVE-2024-53239,CVE-2020-10735,CVE-2024-10979,CVE-2024-50127,CVE-2024-53059,CVE-2024-57910,CVE-2024-6232,CVE-2021-42381,CVE-2023-24329,CVE-2024-47701,CVE-2024-53103,CVE-2024-57911,CVE-2024-50059,CVE-2024-56759,CVE-2024-7006,CVE-2024-50282,CVE-2024-56615,CVE-2024-25062,CVE-2024-50209,CVE-2025-27113,CVE-2022-45061,CVE-2024-49983,CVE-2024-53099,CVE-2024-50278,CVE-2024-53155,CVE-2024-56605,CVE-2024-50036,CVE-2024-49981,CVE-2021-28831,CVE-2024-57906,CVE-2024-49895,CVE-2024-50121,CVE-2024-50151,CVE-2024-53141,CVE-2021-42386,CVE-2024-49966,CVE-2024-50074,CVE-2024-50083,CVE-2024-53150,CVE-2024-56603,CVE-2024-53104,CVE-2024-47718,CVE-2021-42384,CVE-2024-50150,CVE-2024-49894,CVE-2024-50230,CVE-2021-42382,CVE-2024-56642,CVE-2024-50269,CVE-2024-53173,CVE-2024-56672,CVE-2024-49883,CVE-2024-56581,CVE-2024-36899,CVE-2024-47748,CVE-2024-53227,CVE-2024-56766,CVE-2024-56602,CVE-2024-57951,CVE-2024-50279,CVE-2023-43804,CVE-2024-50268,CVE-2024-49969,CVE-2024-47670,CVE-2021-42385,CVE-2025-21692,CVE-2024-46853,CVE-2024-56704,CVE-2024-53057,CVE-2024-49996,CVE-2024-49882,CVE-2023-52530,CVE-2024-56606,CVE-2024-46865,CVE-2024-46858,CVE-2024-57896,CVE-2015-20107,CVE-2024-56600)

Severity	Fixed CVEs
Medium	229 (CVE-2024-50304,CVE-2024-50045,CVE-2024-53097,CVE-2024-50299,CVE-2024-50024,CVE-2024-47699,CVE-2024-50233,CVE-2024-57802,CVE-2024-56643,CVE-2021-42374,CVE-2023-26966,CVE-2025-21683,CVE-2024-41080,CVE-2024-49973,CVE-2024-56779,CVE-2024-47671,CVE-2024-53226,CVE-2024-47713,CVE-2024-49948,CVE-2024-56593,CVE-2023-45803,CVE-2024-56748,CVE-2024-43098,CVE-2024-57901,CVE-2024-46695,CVE-2024-47692,CVE-2024-56754,CVE-2025-21694,CVE-2024-53157,CVE-2024-49902,CVE-2024-50134,CVE-2024-53119,CVE-2024-47749,CVE-2024-49965,CVE-2024-49878,CVE-2024-56629,CVE-2024-53060,CVE-2024-56716,CVE-2024-57902,CVE-2023-38469,CVE-2024-50265,CVE-2024-50184,CVE-2023-42364,CVE-2025-21640,CVE-2024-53130,CVE-2023-2908,CVE-2024-50302,CVE-2024-53101,CVE-2025-21669,CVE-2023-42365,CVE-2024-56670,CVE-2024-49851,CVE-2023-26965,CVE-2024-47739,CVE-2023-45322,CVE-2024-49896,CVE-2024-50058,CVE-2024-56569,CVE-2024-49863,CVE-2024-50287,CVE-2025-21666,CVE-2024-10978,CVE-2023-27043,CVE-2024-50236,CVE-2024-53136,CVE-2024-53131,CVE-2024-50072,CVE-2024-53112,CVE-2024-50205,CVE-2024-49955,CVE-2024-56769,CVE-2022-26280,CVE-2024-50001,CVE-2023-25433,CVE-2024-50046,CVE-2024-50096,CVE-2024-53052,CVE-2024-53135,CVE-2024-56720,CVE-2024-56767,CVE-2024-50148,CVE-2024-49867,CVE-2024-50013,CVE-2024-53217,CVE-2024-56723,CVE-2021-4189,CVE-2024-49944,CVE-2024-47709,CVE-2024-50185,CVE-2024-49933,CVE-2024-57922,CVE-2024-8508,CVE-2024-50015,CVE-2024-47143,CVE-2024-27017,CVE-2024-10976,CVE-2024-49881,CVE-2024-50292,CVE-2024-46841,CVE-2024-53127,CVE-2024-47674,CVE-2024-56567,CVE-2024-56747,CVE-2024-56623,CVE-2025-21699,CVE-2024-44931,CVE-2024-49858,CVE-2024-50229,CVE-2024-56694,CVE-2024-50167,CVE-2021-3426,CVE-2021-3733,CVE-2024-56659,CVE-2024-42315,CVE-2025-21689,CVE-2024-50188,CVE-2024-50099,CVE-2024-49879,CVE-2024-47706,CVE-2021-36976,CVE-2024-49985,CVE-2024-56648,CVE-2023-40217,CVE-2024-50208,CVE-2023-38473,CVE-2024-49875,CVE-2024-50049,CVE-2024-57807,CVE-2024-49975,CVE-2024-57874,CVE-2024-49890,CVE-2024-50198,CVE-2024-49892,CVE-2023-3618,CVE-2023-1981,CVE-2024-50095,CVE-2024-57938,CVE-2024-49962,CVE-2024-50010,CVE-2024-50040,CVE-2024-56756,CVE-2024-47684,CVE-2024-49963,CVE-2024-50201,CVE-2024-50082,CVE-2024-49957,CVE-2024-50006,CVE-2023-3316,CVE-2024-53042,CVE-2024-53161,CVE-2024-47707,CVE-2024-50153,CVE-2024-50194,CVE-2024-56770,CVE-2025-21639,CVE-2024-47737,CVE-2024-50273,CVE-2024-49938,CVE-2024-50039,CVE-2024-47705,CVE-2024-41060,CVE-2023-38471,CVE-2024-56698,CVE-2024-53138,CVE-2024-57946,CVE-2024-56728,CVE-2023-38470,CVE-2024-53121,CVE-2024-47710,CVE-2024-57890,CVE-2024-53146,CVE-2024-56724,CVE-2024-50202,CVE-2024-49958,CVE-2025-21697,CVE-2024-50116,CVE-2023-39615,CVE-2024-57913,CVE-2024-49868,CVE-2024-49977,CVE-2025-26465,CVE-2024-56780,CVE-2024-47679,CVE-2024-49949,CVE-2024-46809,CVE-2024-48881,CVE-2024-36476,CVE-2024-53063,CVE-2024-47756,CVE-2025-21688,CVE-2024-56587,CVE-2025-21638,CVE-2024-47672,CVE-2024-56661,CVE-2024-38591,CVE-2024-47712,CVE-2024-49959,CVE-2024-50103,CVE-2024-49974,CVE-2024-56574,CVE-2024-56739,CVE-2024-50237,CVE-2024-50171,CVE-2024-50251,CVE-2024-50117,CVE-2024-50192,CVE-2024-49952,CVE-2024-56688,CVE-2024-57940,CVE-2024-50142,CVE-2024-49877,CVE-2024-53140,CVE-2024-56568,CVE-2024-49913,CVE-2024-53145,CVE-2023-38472,CVE-2024-22195,CVE-2024-47735,CVE-2024-56634,CVE-2024-53124,CVE-2024-50195,CVE-2024-49907,CVE-2024-53066,CVE-2024-55916,CVE-2024-56763,CVE-2024-50210,CVE-2024-50008,CVE-2024-50296,CVE-2024-50179)

Severity	Fixed CVEs
Low	2 (CVE-2024-50044,CVE-2024-10977)

Resolved Issues

Note

The Resolved Issues tables are updated to include the "Original Issues" column that identifies the JIRA ID and original issue and release version from which this issue was ported. When "Original Issues" specifies "N/A," the current "JIRA ID" is the original release version.

Resolved Issues in 12.01.05R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135320	SBX-134898 (11.1.1)	1	SBC lost redundancy with processAbnormalTermination during an upgrade to R7 **Impact:** A backup and restore DB operation from SBC version 11.1.1R005 to 11.1.1R007 resulted in SBCs in standby continuously performing application restarts when running registrations. **Root Cause:** The backup and restore operation did not re-activate the memory config profile on an active SBC, resulting in different estimates for the registration capacity across an HA pair. This mismatch of registration capacity resulted in illegal memory access by the standby SBC when registrations landed on the active SBC, resulting in a continuous application crash on standby. **Steps to Replicate:** To reproduce the issue, perform the following steps: 1. Activate large sweConfigProfile on the HA pair in SBC version 11.1.1R005. 2. Back up the CDB in SBC version 11.1.1R005. 3. Upgrade the HA pair to SBC version 11.1.1R007. 4. Restore the backed-up CDB .tar on SBC version 11.1.1R007. 5. When the application sync is complete, verify the file /opt/sonus/conf/swe/.sweCfgProfile.txt ◦ an active SBC will have a value of 0 ◦ an SBC in standby will have the value of 1.	The code is modified to ensure that the SWeConfigProfileSelection profile was correctly applied on the active SBC as part of a backup-restore mechanism. **Workaround:** After a backup-restore mechanism operation is complete, reboot the active SBC once after the HA SBC application syncs.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135548	SBX-135237 (12.1.3)	1	Scm process crashed while running registration from user with PLMN info received from PCRF **Impact:** The SCM Process crashes upon receiving an RAR message with a 3GPP-SGSN-MCC-MNC AVP and without a 3GPP-User-Location-Info AVP. **Root Cause:** Upon receiving an RAR with a 3GPP-SGSN-MCC-MNC AVP and without a 3GPP-User-Location-Info AVP, the SBC tries to fetch values from 3GPP-User-Location-Info AVP, even though it is not received in RAR, which causes ScmProcess to crash. **Steps to Replicate:** 1. Enable the RX feature 2. Simulate the PCRF to send a RAR message with a 3GPP-SGSN-MCC-MNC AVP 3. Make a call from a Registered User	The code was modifed to read the value from 3GPP-User-Location-Info AVP only if the AVP is received in a RAR message. **Workaround:** NA.
SBX-135192	SBX-135189 (12.1.4)	1	Unable to change the "cnxipmadmin" default password. **Impact:** Users are not able to change the cnxipmadmin default password **Root Cause:** Users are not able to get a peer's cnxipmadmin passwordd due to not having execute permission on the directory /opt/sonus/shared/ and /opt/sonus/shared/passwdadmin **Steps to Replicate:** 1. Run "$ENCRYPTED_STORE_SH cnxipmadmin" 2. Verify that the cnxipmadmin password is not "Cnx1PmAdm1n" randomized	The code was modified by adding rwx so that cnxipmadmin can get a peer's password as expected. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136106	SBX-133355 (12.1.4)	1	CNF - removing dependency on CGROUP version **Impact:** The SBC CNF fails to load when the cgroup version 2 is configured on the worker node. **Root Cause:** The cgroup version 2 has a different directory structure for accessing the information about the CPU, memory, hugepages and other resources allotted to the container. The mechanism in which the container ID is obtained from within the container also changes. **Steps to Replicate:** Launch the SBC CNF on a worker node configured with cgroup version2. The SBC CNF application's FM Master component on SC, SLB, OAM and SG fails to load.	The code was modified by adding support for running the SBC CNF with cgroup version 2 configured on the kubernetes worker node. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134947	SBX-133734 (10.1.6)	1	After a switchover, call hold/unhold fails since the SBC is not able to send any in-dialog SIP messages to the registered endpoint - broken between 10.1.4R3 and 10.1.5R1 **Impact:** After a switchover, call hold/unhold failed because the SBC is not able to send any in-dialog SIP messages to the registered endpoint. A refresh register routine occurs post switchover and a new port may be allocated, however the SBC used the old port number. **Root Cause:** The Call Control Block (CCB) was not updated with the correct value when the Registration Control Block (RCB) got updated post switchover. **Steps to Replicate:** This issue occurs when the endpoints use TCP and TLS transports. Replicate these steps on the HA-Pair: 1. One endpoint needs to be registered from the IP/Port. 2. Initiate a basic call from the endpoint 3. After the switchover, the endpoint re-registers from a different IP/port than earlier. 4. The registrar endpoint sends a SIP NOTIFY message, followed by a Re-INVITE from the UAS to the endpoint. 5. The SBC sends a Re-INVITE message to the new destination port . The above steps needs to be followed for the exact recreation of the issue.	The code was modified updating the CCB with the Ip/Port for the new Connection from the Address of Record (AOR) block. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133932	N/A	1	RS registration is not retained post upgrade from 12.1.2-R001-333 to 12.1.3-13 **Impact:** The registration data is not retained post-upgrade **Root Cause:** The application cannot reconstruct registration data on upgrade. **Steps to Replicate:** Upgrading the SBC CNe to 12.1.3 will reproduce this issue. This issue does not occur while upgrading to 12.1.5.	The application is enhanced to successfully reconstruct registration data during an upgrade **Workaround:** No workaround
SBX-136049	N/A	1	Azure: Errors observed while installing Hfe2.1 SBC on Azure when hfe_vm_username parameter is given value other than default value "rbbn" **Impact:** Errors observed while installing Hfe2.1 SBC on Azure when hfe_vm_username parameter is given value other than default value "rbbn". **Root Cause:** hfe_vm_username value and ssh_key_path is not same, in ssh_key_path 'rbbn' is hardcoded. **Steps to Replicate:** Test scenario: 1.Take latest iac tarball and launch sbc_hfe2.1 on Azure with any username for hfe. Expected result: 1. SBC hfe_2.1 should come up successfully and should able to login with hfe username.	Updated ssh_key_path to reflect the value of hfe_vm_username **Workaround:** No Workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136219	N/A	1	Post icne container crash callRouting configuration is missing in the instance **Impact:** postgres db is not showing route details during corner case where both pods restart. **Root Cause:** postgres db after both pod restart was not updating the db from pvc. **Steps to Replicate:** Same as Jira description	Changes were done to get the db dump from pvc and update. **Workaround:** No Workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136215	N/A	1	The mgt1 interface ip is not pinging after upgrade. **Impact:** When a VMware 11.1.1R1 SBC instance which has a mgt1 interface added/attached post application installation, is upgraded to 12.1.5 release, the mgt1 interface's IP address is not pingable/reachable from external endpoints. **Root Cause:** The VMware platform does not abide by the PCI slot-number ordering rules when a new interface is added after the CVM is created, thereby generating a custom interface renaming rules. The custom interface renaming(udev) rules are not retained during the upgrade, which results in renaming of the interfaces after upgrade, leading to jumbling of mac address with the interface names. **Steps to Replicate:** 1. Launch a VMware 11.1.1R1 SBC instance with 4 interfaces (mgt0, ha0, pkt0 and pkt1). 2. Stop the instance and attach mgt1 interface and assign IP address to mgt1. Record the MAC address and test its connectivity. 3. Upgrade the SBC to 12.1.5 release. 4. Record the MAC address of mgt1 and test its connectivity.	The custom interface(udev) rules are retained during the upgrade operation. **Workaround:** Manually restore the following files post upgrade and reboot the upgraded VM: • /etc/udev/rules.d/70-persistent-net.rules • /opt/sonus/conf/interface_mapping.json

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135894	N/A	1	ERE Policy server status is down in 17984 build **Impact:** iCNE: ERE Policy server status is down **Root Cause:** The default user for ICNE currently is sonusadmin as the rbbnuser(anyuser) implementation is still in progress. So, when the system is brought up as anyuser, it will give issue from psx-psql POV. **Steps to Replicate:** Not Applicable	Adding large UID/GID and making sonusadmin default user for ICNE. **Workaround:** Not Applicable
SBX-136144	N/A	1	Failure to copy ACT files to the external CDR server **Impact:** Cdr file transfer to cdrServer is failing **Root Cause:** User Id and Group Id were hard coded in the script which copies the files to bkup directory **Steps to Replicate:** 1. Configure CDR server. 2. Rollover ACT files	Get userId and groupId from username and fsgroup respectively **Workaround:** Not Applicable
SBX-136377	N/A	1	Installation failing with duplicate keys in the Helm chart **Impact:** Installation failing with duplicate keys in 12.1.5-127 Helm chart **Root Cause:** Keys in ns deployment for selector labels were duplicate for "app.kubernetes.io/name". This was causing the installation to fail only via GitOps as the Helm sdk used by flux is more strict about the schema than Helm cli. Helm cli installation was working just fine. **Steps to Replicate:** 1. Install via gitops 2. Make sure the HelmRelease is created	Removed duplicate label keys while maintaining the DT "require-labels" cluster policy requirement **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136201	N/A	1	ChmProcess core is observed after switchover of the pod. **Impact:** The Process Watchdog was still running when the SBC was still the process of coming up, causing a force-restart of the SBC, and chm cored. **Root Cause:** Observed that the restore revision calls for a system reboot, then the SM process (where the shutdown script is called with SUDO). This is why the docker stop and sbx stop would run as root, which corrupted the watchdog kill, due to lack of permission. **Steps to Replicate:** Reboot the system after it is up.	Removing SUDO when call Shutdown script **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136395	N/A	1	TLS related configuration is failing in latest 12.1.5 builds **Impact:** TLS config were failing due to a fix that was provided in SBX-136222. **Root Cause:** The error occurred because the script was being called even for remote certificates, leading to a situation where either the certificate or the private key was NULL. The function CpxSecurityValidateCertKey was being called without checking if both the certificate (x509) and the private key (privKey) were present. **Steps to Replicate:** 1. Put create-TLS and create-expect_tls.exp in SBC at path /home/linuxadmin and give full permission to both files. 2. Enter the command ./ `create-expect_tls.exp` 3. Transfer all the newly generated files in SBC at path /opt/sonus/external from /home/linuxadmin. 4. Enter this command at /opt/sonus/external: `openssl x509 -inform der -in pk-ca.crt.der -out pk-ca.crt.pem` 5. Enter this command at /opt/sonus/external: `openssl pkcs12 -in server_p12.p12 -out server_p12.pem -nodes ( Password is : gsx9000)`	Added a check to call the function only when both the cert and private key are present. **Workaround:** No Workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
			6. Enter these commands in SBC admin mode: `set system security pki certificate server fileName server_p12.p12 passPhrase gsx9000 type local state enabled` `set system security pki certificate CA-cert fileName pk-ca.crt.der type remote state enabled` `set profiles security tlsProfile defaultTlsProfile serverCertName server clientCertName CA-cert`	
SBX-135933	N/A	1	Helm upgrade failed for the NS pod from 12.1.4.R000 to 12.1.5 **Impact:** Upgrade was failing from 12.1.4 to 12.1.5 for the NS pod. **Root Cause:** Upgrade was failing due to a new label. The name label was introduced in SBX-135709 for customer compliance, removing it from ns as it causes upgrade to fail, ns never had name label, other pods had name label. **Steps to Replicate:** Upgrade from 12.1.4 to 12.1.5, ensure upgrade is successful and all pods are up (especially NS).	Removed name label from selector labels **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135924	N/A	1	Observed ChmProcess crash in SLB during customer callmix load over the weekend **Impact:** When the container was going down and before the marker file safplus_restart_disable gets created, the watchdog process notices safplus_amf was not running, so it initiated force_restart_safplus, thats when we see the CHM core. **Root Cause:** When RAC signaled reboot for SLB pod, as a rare case, the /openclovis/bin/ safplus_amf was stopped before the safplus_watchdog process. Graceful shutdown/SBC cleanup has the step to create the marker file safplus_restart_disable which restricts the force_restart_safplus by watchdog when safplus_amf is not running. When the container was going down and before markup file gets created, the watchdog process notices safplus_amf was not running, so it initiated force_restart_safplus, thats when we see the CHM core. **Steps to Replicate:** Stop / openclovis/bin/safplus_amf before safplus_watchdog process and trigger a container restart.	Create the Marker file, before the TERM signal is sent to my-init, so when container is already going down, we should not see application starting up, hence avoid the chm core. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136119	N/A	1	OAM is not getting recreated when upgrade is performed changing values of RAMP IP to FQDN **Impact:** RAMP configmap changes was not triggering the container restart for update the configurations **Root Cause:** RAMP configmap is converted to Secrets in latest implementation so it was not included in checksum validation in deployment **Steps to Replicate:** Update the RAMP configmap/secret content in Helm chart when upgrading	Added the secret along with config map for checksum validation to trigger the container respawn/restart in case upgrade or changes in contents of secrets (in recent builds) and configmap (older builds) for OAM pods. **Workaround:** Not Applicable
SBX-135550	N/A	1	./exportConfig script is failing to import the configuration **Impact:** EMA import configuration feature is failing when remote policy server configurations are present in config bundle. **Root Cause:** While importing the configuration, both local policy server(got added as part of SBC initial configuration) and remote policy server(added by user in older version) are causing validation failure, because of this config import failed. **Steps to Replicate:** 1) Bring up CNF deployment, and configure remote policy server details. 2) Export the configuration using EMA page or using exportConfig,sh script. 3) clear the DB and import the configurations.	As local policy server is not applicable to OAM type deployments, removed it from initial SBC configurations in OAM type deployments. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135621	N/A	1	ScmProcess restarted while making call from registered end point **Impact: The** ScmProcess crashes on getting AAA/RAR with 3GPP-User-Location-Info AVP without 3GPP-SGSN-MCC-MNC AVP. **Root Cause:** On getting AAA/RAR with 3GPP-User-Location-Info AVP and without 3GPP-SGSN-MCC-MNC AVP , SBC tries to fetch 3GPP-SGSN-MCC-MNC AVP value eventhogh 3GPP-SGSN-MCC-MNC AVP not received and this results in ScmProcess to crash. **Steps to Replicate:** 1. Enable Rx feature. 2. Simulate PCRF to send only 3GPP-User-Location-Info AVP in AAA/RAR. 3. Run a basic call from registered user.	Added fix not fetch 3GPP-SGSN-MCC-MNC AVP AVP value when it is not received in AAA/RAR. **Workaround:** 1. Always send both 3GPP-User-Location-Info AVP and 3GPP-SGSN-MCC-MNC AVPs in AAA/RAR.
SBX-135016	N/A	1	Media stats are displayed in SBC callMediaStats for Direct Media calls post callMix Load **Impact:** Media stats are displayed in SBC callMediaStats for Direct Media calls. **Root Cause:** Call Details Data are getting populated in nrmActiveCallCsv.c from “callStatPtr” which comes from “xrmMediaStats” in XrmNrmMsgProc.c And RIDs stats is not resets in case of Direct Media Call, so it will show stats related to the old call. **Steps to Replicate:** Follow the same steps as while reproducing issue.	Update the “bufPtr” for Call Media Status Data only when call media type is not Direct Media. **Workaround:** Adding "if condition" for callStatPtr->sonusActiveCallMediaType != ENUM_sonusActiveCallMediaType_directmedia

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136292	N/A	1	Observing CPXProcess coredump on CONFD Pods post upgrade form 12.1.4 to12.1.5-18131 build **Impact:** When CNF deployment is upgraded from 12.1.3/12.1.4 to 12.1.5 version, we are seeing cores in Chm, Enm and Cpx processes while accessing PVC directories/PVC files. **Root Cause:** Permissions and ownership of PVC directories have been changed in 12.1.5 due to non-root and read-only file system changes, because of this, during upgrade where older version and newer version pods co-exist for few minutes, pods are seeing permission denied while accessing PVC locations. **Steps to Replicate:** 1. Bring up CNF deployment in 12.1.4 version, upgrade the set up to 12.1.5. 2. Roll back the system to 12.1.4 version again, during rollback no cores should be seen.	Added Exception handling to ignore the permission denied errors during the upgrade phase to prevent Cpx,Chm and Enm process cores. **Workaround:** No Workaround
SBX-136367	N/A	1	Observing CPX process core in CONFD 12.1.4 pods during upgrade from 12.1.4 to 12.1.5-122 **Impact:** Observing CPX process core in CONFD 12.1.4 pods during upgrade from 12.1.4 to 12.1.5 on CNF solution of SBC. **Root Cause:** While upgrading, 12.1.5 revokes the access for the 12.1.4 on the directory which is actively used by CPX Process, so due to the access denial CPX coring in 12.1.4 **Steps to Replicate:** upgrade SBC-CNF from version 12.1.4 to 12.1.5-122	12.1.5 will share the directory access with 12.1.4 (old pods) to avoid coring. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132906	N/A	1	Post network issue SSPs are found in SLBs which are not registered in SBC (EMA or CLI) **Impact:** Deleted SSPs in SSBC were registering again to SLB post SWO/sbxrestart. **Root Cause:** SSBC were selecting previous SSP SLB name even if no SLB were configured in next SSP config. **Steps to Replicate:** 1. Configure more than 1 sigports with slbname in SSBC. 2. Configure more than 1 sigports without any slbname configurations in SSBC. 3. In SLB, “request sbx sipcm debug command slb\ status” o/p should show only SSP that is having slbname in SSBC config. 4. Do sbxrestart and same o/p should be present. 5. Do SWO and same o/p should be present. 6. Delete sigports from SSBC. 7. Verify “request sbx sipcm debug command slb\ status” o/p before and after SWO/sbxrestart again.	Code changes are done to ignore SSP to SLB registration if no SLB name is configured in SSP. **Workaround:** delete complete SSP instead of deleting only SLB name from SSP in SSBC
SBX-135328	N/A	1	Active SBC went into Hung state (Disk Issue) - Standby could not take over **Impact:** In HA setup, when active machine is in hand state and not released DRBD device, standby will fail to make DRBD as primary to become active. **Root Cause:** Active machine is not released DRBD. **Steps to Replicate:** Bring up HA setup on hardware, power off SSD on active machine via BMC.	Make DRBD as primary on standby forcefully **Workaround:** Reboot Active machine.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134495	N/A	1	MS Teams Call Transfer failure **Impact:** Call transfer fails as SBC sends BYE upon second transfer from Teams client. **Root Cause:** At SBC, a transferred call is bridged across multiple GCIDs. During Teams transfer request to move from Internal to External interface, the SBC moves/modifies the corresponding IP resource during which it fails to pick the correct call leg corresponding to this resource. This leads to failure and call tear down. **Steps to Replicate:** 1. Party-A calls Party-B(TEAMs client) which responds with "X-MS-UserLocation: external" 2. Party-B transfers the call and sends REFER to SBC 3. SBC initiates new call to Party-C (TEAMs client) which responds with "X-MS-UserLocation: internal" 4. Party-C sends re-Invite to SBC with "X-MS-UserLocation: external" (To switch from internal to external interface) Expected Result: Re-Invite to switch to external is successful. Actual Result (without fix): Re-Invite to switch to external fails.	The Code has been modified to let SBC choose the call-leg based on the leg's GCID rather than the call GCID while handling the resource's modification. **Workaround:** Remove mediaIpsecondaryinterfacegroupname & change the mediaipinterfacegroupname to a public IP

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135268	N/A	1	Ingress Route PSP contains a non-zero value of mediaInactTimeout intermittently on SBC 5400 with ERE **Impact:** Ingress Route PSP intermittently contains a non-zero value for mediaInactTimeout when using ERE **Root Cause:** An uninitialized variable holds the value of mediaInactTimeout from responce. If not present in the responce, then random value could be used if buffer was not null and failures may be seen. **Steps to Replicate:** 1. Configure a basic call 2. Attach PSP profile to ingress and egress trunk group. 3. Run 1000+ calls. 4. Call should be successful	Code changes were made to Initialize mediaInactTimeout to 0. **Workaround:** None
SBX-136608	N/A	1	Observed CoreDump (core.2.dataagent_4256.1742794669) while performing admin switchover during callmix loadrun. **Impact:** While performing CLI admin swo from standby to active got a coredump (core.2.dataagent_4256.1742794669) on standby instance **Root Cause:** Issue was introduced after upgrading dataagent to 1.48.161-22 **Steps to Replicate:** 1. Bring up an HA setup 2. Configured the setup to run callmix load 3. Make sure there are no dataagent coredumps while performing CLI admin swo from standby to active	Reverted back to dataagent version 1.48.157-18 **Workaround:** No Workaround

The following severity 2-3 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136484	SBX-136308 (12.1.3)	2	SCM Coredump on 12.1.3R3 **Impact:** The SCM Process cored when handling NOTIFY messages for registration. **Root Cause:** When receiving a NOTIFY message, the SBC attempted to print a log that also printed the GUID. Because a NULL pointer accessed the GUID, the SCM Process cored. **Steps to Replicate:** IMS Registrations with NOTIFY message can cause this coredump	The code was modified so that it no longer attempts to access a NULL pointer when printing the GUID. **Workaround:** No Workaround
SBX-135037	SBX-134763 (12.1.3R001)	2	SSHD service is not running on oam pod 12.1.3 R001 #154 **Impact:** The sshd service does not run in oam pods **Root Cause:** The Ribbon-maintained version of openssl is overridden by the stock version from Debian. **Steps to Replicate:** Deploy the oam pods with the version of sshd supplied in v12.13R001 or earlier.	Upgraded the maintained version of openssl to the latest version from Debian. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136227	SBX-136183 (10.1.5)	2	PS-SBC High memory usage **Impact:** When the tone is configured with criteria on the ingress or egress trunk group, and multiple crankbacks occur, there is a memory leak during the tone criteria processing. **Root Cause:** The SBC overwrote the tone profile memory block before freeing any memory stored at a memory address within that contained trigger information. **Steps to Replicate:** 1. Configure tone criteria on the ingress or egress leg 2. Initiate a call that uses advanced routing through multiple routes 3. Wait for the first egress timeout, then trigger a crankback to the second route.	The code was modified to check if a pointer to trigger information exists. If so, then free the previous pointer, delete it, and allocate a new one. **Workaround:** Disable criteria on both legs
SBX-135150	SBX-134672 (12.1.3)	2	DSBC: Config Export and Import Stuck while using EMA. **Impact:** The import configuration was getting stuck due to an exception. **Root Cause:** There was a typecast issue at the Actions class **Steps to Replicate:** 1. Configure SBC and export the configurations from EMA 2. Clear the configurations 3. Try to import the configurations from EMA	The code was modified so that the maxSetsPerCommit changes from the YangList to the YangNode class. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136094	SBX-135876 (11.1.3)	2	SBC memory leak **Impact:** The Rx Feature 's8hrSupport' and the 're-query PSX registration refresh enable' may cause a memory leak. The 'SMM trunkgroup prefixed feature' also causes memory leaks for the 'relay nonInvite' feature. **Root Cause:** When processing a 're-query PSX for registration refresh' response, the SBC allocated a new memory block and overwrite the existing one. This causes the previous allocated leak. **Steps to Replicate:** Enable the features 's8hrSupport' and 're-query PSX registration refresh'.	The code was modified so that new memory is not allocated if it has already done so. **Workaround:** Disable 're-query PSX registration refresh', and disable 'SMM trunkgroup prefixed' for relay NonInvite messages.
SBX-135984	SBX-135914 (11.1.1)	2	DiamProcess Coredump Observed on 11.1.1R Build 108 **Impact:** DiamProcess cores when an invalid peer IP is configured **Root Cause:** If the peer IP is invalid, the SBC tries to access the pointer even if it was NULL. **Steps to Replicate:** Configure an invalid peer IP on the Rx interface	The code was modified to not access the null pointer. **Workaround:** Configure a valid Peer IP on the Rx interface will avoid a coredump.
SBX-136064	SBX-135242 (12.1.3)	2	LI - pktcV1 flavor - EM header incorrectly set Timezone **Impact:** The signaling messages in Packet Cable LI do not contain the correct timezone in the EM header. **Root Cause: The** TimeZone field was filled with blanks. **Steps to Replicate:** In a Packet cable LI setup, make an intercepted call. Check the signaling Start message for the EM Header timezone. It should have the appropriate value as per the SBC's time zone.	The code was modified to fill the time zone field correctly as per the format mentioned in the PC V1 specification; 0+HHMMSS, 0-HHMMSS, 1+HHMMSS, or 1-HHMMSS. The first byte is filled 1 for DST, if it is applicable. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135360	SBX-133174 (12.1.1)	2	SLB application down creating coredumps **Impact:** Due to a failure to obtain a postgres DB connection, the Cpx cores while the application comes online. This results in an intentional exit/abort. **Root Cause:** During the CPX initialization, the requests to Postgress DB come in before the DB's initialization. **Steps to Replicate:** Run a script for the SNMP to query Postgress data. In parallel, initialize the SBX application.	The code was modified to throw an error message when a race condition happens, such as a request to Postgress DB before its initialization. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135351	SBX-135081 (10.1.6)	2	EnmP coredump **Impact:** The ENM cores while performing a switchover. **Root Cause:** The customer upgraded from 10.1.5R0 to 10.1.6R0, which results in an issue of losing encrypted fields from CDB after the upgrade (SBX-133822). Due to this, the CDR server password field was lost after the upgrade, so CDR file transfers were left pending for a long time. This may result in more than 10K transfer files pending in the list. **Steps to Replicate:** Method 1 1. Bring up an HA 1:1 setup, installed with an 10.1.5R0 image, with the CDR server details configured, and configure the eventLog typeAdmin acct fileCount (eg: 500). 2. Perform an upgrade. 3. Check whether the configured CDR server password is present in CDB. If it is present in CDB go for method 2, if not continue to step 4. 4. Use a REST API script to perform a rollover on the acct files so that the pendingTransfers list can grow. 5. Check whether the list grows beyond the configured fileCount value. The configured fileCount should limit the pendingTransfers count.	The code was modified to limit the pendingTransfers list to match the number of files(fileCount) configured under eventLog typeAdmin. The result is that the pending transfer list will not grow to a critical value. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
			6. Perform a switchover to see if a core occurs. Method 2 1. Add a code hack so that the error "ENM: . .EnmFileXfer_i::checkForWork: ServerAdmin Structure is not properly initialized: type 1" will be logged 2. Comment out the line in EnmCdrServerCacheCdrServerAdmin (hornet/enm/lib/src/EnmCdrServer.cpp) IPUtilDecimalIP2Dotted(ip[0], (UCHAR*)EnmCdrServerAdmin[cdrIndex].ipAddrChar, sizeof(EnmCdrServerAdmin[cdrIndex].ipAddrChar)); 3. Clear the field EnmCdrServerAdmin[cdrIndex].userChar in the checkForWork function 4. Use a REST API script to perform a rollover on acct files so that the pendingTransfers list can grow. 5. Check whether the list grows beyond the configured fileCount value. The configured fileCount should limit the list pendingTransfers count. 6. Perform switchover to see if the system cores.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136099	SBX-134412	2	Unable to create more than 64 ipInterface addresses **Impact:** The SBC should not be able to configure IP and port combinations such that more than 4 million UDP ports would be allocated. Calculation assumes max ports per interface. **Root Cause:** A check was added to restrict to 64 in the CPX, countIP * numofPorts > 4 million to limite the number of combinations. This check needs to be smarter. **Steps to Replicate:** 1. Leave the media UDP Port ranges as default 2. Create more than 64 IP Interfaces 3. Verify if the code allows this configuration or not.	The code change now looks at sum of # bearer ports assigned to each IP interface as this total should not go over 4 million. **Workaround:** Ensure that the IP and ports configurations is lower than CPX_MAX_IPPORT_COMBINATION which today is 4 million.
SBX-132408	N/A	2	MCT not working with Dynamic LRBT (DLRBT)- sending 503 error to MCT Server **Impact:** When an MCT recording is triggered for a DLRBT call, the SBC rejects the MCT sessions with a 503 message, and no recording is triggered. **Root Cause:** MCT recordings for a DLRBT scenario was never supported. **Steps to Replicate:** 1. Configure the MCT and enable DLRBT on the SBC 2. Ensure the MCT Server is running. 3. When the CS is established between A and B, the SBC sends NOTIFY messages. 4. The MCT initiates the INVITE for call recording. 5. The SBC rejects one of the MCT INVITE messages with a 503 response.	MCT recording is now supported for DLRBT scenarios. Recording of tones shall not be supported, only audio streams for the call shall be recorded once the call is answered. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136191	N/A	2	Observing "SystemManager::Unable to extract message" for the SmProcess in the SBC pods during the call load. **Impact:** "SystemManager::Unable to extract message" warnings appear in the log. **Root Cause:** An ELSE block is missing. **Steps to Replicate:** license	The code was modified to include an ELSE block, making the SystemManager warning only appear when expected. **Workaround:** not applicable
SBX-135601	N/A	2	LDAP Authentication : IDM user not able to login via GUI but success when log in via ssh cli. **Impact:** IDM users are not able to log in using the GUI, but are successful when logging in through the SSH CLI. **Root Cause:** Passwords entered by the user are encoded using UTF-8, however they were decoded using ISO-8859-1. As a result there is a mismatch in the password after decoding causing the login to fail. **Steps to Replicate:** 1. Create a user with password containing an accented character (for example "Â") 2. Log in to the EMA The log in should be rejected	The code was modified to encode passwords using ISO-8859-1. **Workaround:** No workaround
SBX-134884	N/A	2	CVEs found in 12.1.4 closer to GA. **Impact:** Vulnerabilities present in Debian packages. **Root Cause:** Vulnerabilities are present in Debian-maintained packages used in the SBC. **Steps to Replicate:** Install the build without the fix. Run a scan to confirm the CVEs are present.	Run OSPD to get up-to-date with all the fixes from the Debian repo. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135800	N/A	2	Egress invite from SBC is not containing sip header UserInfo with length of 512 bytes **Impact:** The SIP Header "UserInfo" on the egress INVITE from the SBC does not have the full length of 512 bytes. **Root Cause:** The called number is formatted incorrectly while processing the egress INVITE. **Steps to Replicate:** Refer test cases 1410942 and 1410943 under SBX-107515/CLONE - SIP header Userinfo support for up to 512 bytes	The code was modified to correctly format the called number. **Workaround:** Not Applicable
SBX-135891	N/A	2	Not able to configure ipacl with v6 **Impact:** The CNF is not able to configure ipacl with v6. **Root Cause:** Instead of validating destIpV6Name, destIpV4Name was validated twice. **Steps to Replicate:** 1. Configure the ipacl with v6 2. Run 'show table' on the ipacl The configured ipacl should be displayed	The destIpV4Name was updated to destIpV6Name **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136208	N/A	2	SBC is rejecting the subscribe sent with the received reg-info and DTG parameters in the request URI with a 408 Request Timeout. **Impact:** The SBC rejects subscriptions sent with the received reg-info and DTG parameters in the request URI with a 408 Request Timeout. This was a side-effect of changes done for SBX-134179 **Root Cause:** Due to changes in SBX-134179, the Peer Ip was picked up as the next hop IP of the registered endpoint, instead of using thecontact header Ip of Register **Steps to Replicate:** 1. Enable honorContactInRegisterForTCPTLSCalls. 2. Have EP1 send a REGISTER from IP2:PORT2 using the contact user1@IP1:PORT1 over TLS 3. From core-network, send a SUBSCRIBE with the received reg-info and DTG parameters in the request URI. 4. Send a 200 OK message for SUBSCRIBE from EP1, with the record router header containing a different IP as the Record-Route: <sip:IP3:PORT3;lr> and contact as user1@IP1:PORT1 5. From core-network, send a re-fresh SUBSCRIBE with the received reg-info and DTG parameters in the request URI. 6. The SUBSCRIBE should go out properly to the registered endpoint contact	Changes that for SBX-134179 were reverted. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134938	N/A	2	EMA issues on SBC 5400 **Impact:** The SBC 5400 has EMA access issues. **Root Cause:** The EMA uses an SSH connection to authenticate the user. The SBC takes too long to authenticate the user, due to the SSH connection timing out. **Steps to Replicate:** 1. Log in to EMA. 2. The log in should be successful. 3. Perform some operations in EMA and all the operations should be successful.	The code was modified to increase the timeout from 12 seconds to 30 seconds. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136574	N/A	2	SBC is rejecting the OOD MESSAGE/REFER request received from CORE network with 408 Request Timeout. **Impact:** The SBC rejects OOD MESSAGE/REFER requests received from the CORE network with a 408 Request Timeout. This was a side effect of changes done for SBX-134179 **Root Cause:** Due to SBX-134179 changes, the Peer Ip was picked up as the next hop IP registered endpoint, instead of using the contact header IP of Register. **Steps to Replicate:** 1. From PBX(IP-1:PORT-1), send the Initial REGISTER request. The REGISTER request contains: Contact: <sip:userA@IP-2:PORT-2> From: <sip:userA@rbbn.com> To: <sip:userA@rbbn.com> 2. From CORE, send a 401 response. 3. From PBX(IP-1:PORT-1), send a Challenge REGISTER request. The REGISTER request contains: Contact: <sip:userA@IP-2:PORT-2> From: <sip:userA@rbbn.com> To: <sip:userA@rbbn.com> 4. From CORE, send a 200 OK response.	Changes that for SBX-134179 were reverted. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
			5. From PBX(IP-1:PORT-1), send an Initial REGISTER request. The REGISTER request contains: Contact: <sip:userA@IP-3:PORT-3> From: <sip:userA@rbbn.com> To: <sip:userA@rbbn.com> 6. From CORE, send a 401 response. 7. From PBX(IP-1:PORT-1), send a Challenge REGISTER request. The REGISTER request contains: Contact: <sip:userA@IP-3:PORT-3> From: <sip:userA@rbbn.com> To: <sip:userA@rbbn.com> 8. From CORE, send a 200 OK response. 9. From CORE, send an OOD MESSAGE request. The OOD MESSAGE request contains: requestURI: sip:userA@IP-2:PORT-2;reginfo=RCB1;dtg=INGRESS_TG 10. From CORE, send an OOD REFER request. The OOD REFER request contains: requestURI: sip:userA@IP-3:PORT-3;reginfo=RCB2;dtg=INGRESS_TG Both the MESSAGE and REFER should be sent successfully to the registered endpoint.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135967	N/A	2	When Signaling is disabled in all MS and only Media TCP is enabled then media interception is not working. **Impact:** When Signaling is disabled, media is not intercepting. **Root Cause:** When mode and state are disabled for Signaling, it updates the state/mode as disabled for TCP media interception. The SBC fails to intercept media when TCP is not in service. **Steps to Replicate:** 1. The SBC is up and running. 2. Configure IMSLI with the settings below, and with multiple MS: MS1 signalling disabled/OOS + Media TCP enabled/ inService MS2 signalling disabled/OOS + Media TCP enabled/ inService MS3 Media TCP enabled/ inService 3. Provision one target to function as the Called number as the DN for the intercepting Egress leg. Test Step: Make a call. Observed result: Media is not intercepted.	The code was modified to update signaling and media's state and mode separately. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136385	N/A	2	XrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 4d gcid ffffffff observed in 12.1.5 while running hold-resume call load with RTCP **Impact:** The error 'XrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 4d' appears in the DBG log. **Root Cause:** The RTCP Gen command can be sent from XRM and BRM, and depending on which stage of the call and the type of the call the NP command is added to the XRM or BRM queue. When NAPT learning is enabled, the XRM sends the RTCP Gen commands ENABLE and MODIFY to NP, however the user handle XRM used to send the commands were not consistent. Therefore, the ENABLE and MODIFY commands were added in different user queues, which caused the error. **Steps to Replicate:** Repeat the same tests where the XrmAsyncCmdErrHdlr message was observed.	This is the second part of the fixes from SBX-134636, aiming to use consistent user a handle to send RTCP Gen commands. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136276	N/A	2	LDAP bind operation (sasl/md5) for systemUsername and systemPassword is failing on SBC (ExternalAuthentication) with cat: /etc/container_environment.json: No such file or directory. **Impact:** The operation LDAP bind (sasl/md5) for systemUsername and systemPassword is failing on the SBC (ExternalAuthentication) with cat: /etc/container_environment.json: No such file or directory. **Root Cause:** The binary attempted to display the contexts of the json file when the file was not present in SBC VNF. **Steps to Replicate:** 1. Set ldapConfigurationMode to advanced. For example: set oam ldapAuthentication ldapConfigurationMode advanced 2. Configure an LDAP server: set oam ldapAuthentication ldapServer AD25 ldapServerAddress AD.rbbnedge.com ldapServerPort 636 priority 25 transport ldaps bindMethod sasl saslMechanism digest-md5 binddn cn={0},CN=Users,dc=rbbnedge,dc=com searchbase dc=rbbnedge,dc=com searchFilter (&(objectClass=group)(member=CN={0},CN=Users,DC=rbbnedge,DC=com)) returnAttribute cn state enabled systemUsername admin111375 systemPassword <>	The code has been modified to check the presence of the file before trying to run cat command. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
			3. Set externalAuthenticationEnabled to true and externalAuthenticationType to ldap. For example: set system admin vsbcSystem externalAuthenticationEnabled true externalAuthenticationType ldap 4. Verify in advanced mode SBC LDAP client will bind with the systemUsername and systemPassword of 25th server. Expected Results 1. Configuration should be successful. 2. Login should be successful.	
SBX-136232	N/A	2	Observing "CcProcessSessionRegisterNfy" and "DS_SESSION_REGISTER_NFY" log flood in the DBG log of SC pod during passthrough call load **Impact:** The Debug Logs were printed in the SC pod several times, which could impact the SBC performance during the call load. **Root Cause:** The log statement was written with MAJOR level. **Steps to Replicate:** Run a basic passthrough call with the Major log level	Modified the level of this log from MAJOR to Info. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136513	N/A	2	SBC failed to send update message with new codec from Egress **Impact:** The SBC failed to send an UPDATE message with the new codec change from the egress. **Root Cause:** The auto answering logic fails to identify that the change in codec was received from the egress. **Steps to Replicate:** 1. UAC sends INV with 0 8 18 2. SBC sends INV with 0 8 18 3. UAS sends 183 with 0 4. SBC sends 183 with 0 5. UAS sends 183 with 8 6. SBC sends 183 with 0 to UAC 7. SBC fails to send UPDATE with 8 towards UAC	Modified the auto answering logic at the ingress so that it identifies the change in codec from the egress. **Workaround:** None
SBX-135574	N/A	2	Remove uploadCertificate section from Security Configuration - PKI document. **Impact:** The PKI Security Configuration documentation is no longer accurate. **Root Cause:** Update the SBC Core document to remove the section "Upload PKI Certificates" since SBC 12.1.5 does not support this functionality. **Steps to Replicate:** N/A	Updated the SBC Core document to remove the section "Upload PKI Certificates" since the SBC version 12.1.5 does not support this functionality. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131832	N/A	2	Text is not received on UAS for g711-g711 (t140-tty) transcoding in SBX-SBX gateway-gateway scenario **Impact:** The DSP was not able to convert the T.140 packets received to TTY, and vice-versa. **Root Cause:** While the application sends the data to the DSP, the payload values for the Ingress and Egress text was recorded as 0. **Steps to Replicate:** 1. Make a GW-GW setup in the SBC, version 10.1.5 or higher. 2. Make an Audio and Text call from the Ingress endpoint 3. Reject the text from the Egress endpoint. 4. The call should be transcoded between Text to TTY on Egress and passthru on Ingress.	Modified the NRMA code to update the payload values appropriately. **Workaround:** No workaround
SBX-135183	N/A	2	RCA Required: HKG SBC drbd in diskless state [continuation case from 241204-824864] **Impact:** If the SBC has two hard disks, one SDA for root file system and one SDB for DRBD, in some case after a reboot the hard disk naming will be swapped, causing issues for the DRBD. **Root Cause:** Because of name swap, the SBC fails to mount the DRBD and instead mounts the root file system. **Steps to Replicate:** 1. Attach two SDDs on a VM 2. Bring up HA and make it sync 3. Shut down the standby and swap the SDD 4. Power on the instance The unit will be on standby and register as diskless	The DRBD partition was modifed to update in drbd.conf, before the DRBD service starts. **Workaround:** Power off the instance, swap the SDDs, then power it back on.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136053	N/A	2	Traps are getting not generated correctly when the acct logs over relp **Impact:** Traps were not generating as a result of remote rsyslog connection issues and connection recovery. **Root Cause:** The rsyslogServerChecker cron commented out rsyslog.conf rules after finding a rule with a configured remote rsyslog server IP which is not reachable anymore. This prevents the rsyslog spool from filling up and affecting the local logging. This logic was incorrect as the script would comment out rules based on server name and not the actual port and IP combination. This would lead the logic to comment out using an incorrect rule, and would never re-establish the connection after the remote rsyslog server restart as the rule was commented. **Steps to Replicate:** TEST 1: 1. Configure the debug logs to be sent to server1 over TCP. 2. Enable syslogState 3. Verify on the remote host that logs are present 4. Stop the remote rsyslog server "systemctl stop syslog.socket rsyslog" 5. Wait 5 minutes, then verify that snmp trap sonusCpSystemRsyslogRemoteServerConnectionIssue is generated TEST 2: 1. Configure the debug logs for server1 over TCP and ACCT logs for server1 over RELP to the same remote rsyslog IP	Fixed the logic for commenting/ uncommenting rules of unreachable rsyslog servers. Enhanced it to use actual port and IP combination to find the rsyslog facility for the server. Upon finding a connection issue with the remote IP, all rules for the IP will be commented out and a trap will be generated, like before. Upon finding a recovered connection, all rules for the IP will be uncommented and a trap will be generated, like before. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. Enable syslogState NOTE: if already enabled, disable and enable it 3. Verify on the remote host that the logs are present 4. Stop the remote host rsyslog 5. Wait 5 minutes. Verify that the trap sonusCpSystemRsyslogRemoteServerConnectionIssue is generated on the SBC 6. Start the remote host rsyslog 7. Wait 5 minutes. Verify that the trap sonusCpSystemRsyslogRemoteServerConnectionRecovered is generated	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134560	N/A	2	SBC is discarding rtcp packets after unhold in Video call scenarion with NATed eps **Impact:** The SBC discards RTCP packets after an un-hold with NATed EPs, instead of learning the RTCP port from an EP. **Root Cause:** In the SBC NP, there was code to support RTCP EP's Address and Port learning, but the RTCP port alone learning the case code was missing. That combination was used after un-hold scenario, causing the NAT to discard packets. **Steps to Replicate:** 1. Make a video call from a NATed EP1 to EP2 2. Answer the call on EP2 3. EP1 sends Video RTCP and Audio RTCP, followed by Video RTP and Audio RTP. 4. After a few seconds, EP2 also starts sending RTCP video and audio packets, and then RTP packets for both audio & video streams. 5. EP1 sends a hold with with c=0.0.0.0 6. EP1 sends an unhold, with a connection IPAddress. 7. EP2 also starts sending RTCP video and audio packets, and then RTP packets for both audio and video streams after an unhold. 8. Disconnect the call from EP1. Expected Results: 1. The video call from NATed endpoint EP1 to EP2 is successfully connected. 2. EP2 answers the call, and the call is established. 3. The SBC learns the RTP and RTCP port and IP from the packets received from EP1.	The NP code is updated to support learning the RTCP port alone in the un-hold use case combination. **Workaround:** none

Issue Id	Original Issue	Sev	Problem Description	Resolution
			4. The SBC sends the received RTP packets from EP2 to the learned IP and port, and sends the received RTCP to the learned IP and port. 5. The SBC should not learn the RTP and RTCP port and IP again after receiving a=sendrecv from EP1. 6. The SBC sends the received RTP packets from EP2 to the learned IP and port (learned before hold), then sends the received RTCP to the learned IP and port 7. The call is successfully disconnected from EP1 with BYE and 200 OK messages.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134796	N/A	2	SBX-119575 caused the SBC to increment the target port number by 1 when relaying out-of-dialog NOTIFY messages from the registrar to endpoints registered over TLS; in-dialog NOTIFY messages are relayed fine **Impact:** The SBC increments the target port number incorrectly by 1 when relaying out-of-dialog NOTIFY messages from the registrar to endpoints registered over TLS. **Root Cause:** When UsePsxRouteForSubscribe is enabled on the ingress leg, the SBC increments the target port by 1 even though the PSX dip did not happen. **Steps to Replicate:** 1. Make a basic A to B call setup for REGISTER call (TLS). 2. Enable the psxrouteforsubscribe flag on the ingress leg. 3. Disable the psxrouteforsubscribe flag on the egress leg. 4. Establish a successful REGISTER call from Party A to B with registered port 1234. 5. Use the Reg-ID from the REGISTER message to send an Out-of-Dialog (OOD) NOTIFY message to the registered user. 6. The SBC tries to send the OOD NOTIFY message to target port 1235.	The code was modified so that the target port is incremented only when the PSX dip happens, and UsePsxRouteForSubscribe is enabled on the registrar/egress leg. **Workaround:** No workaround.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135173	N/A	2	Last restart reason processAbnormalTermination in SBC (cpx coredump) **Impact:** The cpx process crashes while deleting a user. **Root Cause:** Freeing a ConfD structure which is not properly initialized. **Steps to Replicate:** Run a load script to create and delete users under the path /oam/localAuth/user.	The code was modified with added checks to make sure ConfD structure is freed in appropriate cases. **Workaround:** Not Applicable
SBX-136080	N/A	2	Permission denied prompts are displayed when changing the admin password. **Impact:** The SBC displays permission denied prompts when changing the admin password in the Confd CLI. **Root Cause:** Semaphore issues these waring messages due to access/permission differences in the non-root system. **Steps to Replicate:** 1. Launch an SBC CNF non-root solution (version lower than 12.1.5) 2. Log in to ConfD CLI and change the admin password 3. The password change will be successful, but the system will produce semaphore warnings	The code was modified to suppress the semaphore warning messages and redirect them to /var/log/warn. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134737	N/A	2	SC container went for restart **Impact:** The SC container restarts due to a deadlock. **Root Cause:** When the SC pod tries to come online after a restart, it gets stuck reading a file from PVC which is used to find the active SBC and create a GRPC channel. The SC likely gets stuck due to PVC slowness, as the active NS pod also takes nearly 5 minutes to write contents to same the PVC file. This causes a deadlock and triggered another restart. **Steps to Replicate:** 1. Have both NS pods active, and while the SC pod is coming up, add or modify configuration 2. Delete the active NS or perform a switchover 3. Add or modify a network segment- or LIF-related configuration 4. Perform a SC switchover 5. Add or modify a network segment- or LIF-related configuration 6. Scale down both NS servers and then scale them up. Alternatively, delete the NS pods, and after the NS pods are up, add or modify some network segment- or LIF-related configuration. 7. Scale down both the NS servers. 8. Restart or delete the SC pods, then scale up the NS pods. 9. After the NS pods up, add or modify a LIF configuration 10. Scale down the Cache pod, and delete the NS pods. 11. After the NS pods are active, add or modify some network segment-related configuration.	The SC pod code was modified to discover NS pods and try creating a GRPC channel with discovered pods. The channel creation will only successfully create a channel with an active NS pod, and this channel will be used for communication between SC and NS. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
			12. Begin a test with Ipv4 and Ipv6 interpod communication interface. 13. Check that the media re-construction is not affected. 14. Begin an upgrade test	
SBX-135451	N/A	2	SIPSG is printing missing TrunkGroup for normal call **Impact:** SIPSG prints the minor level error log "SipSgSendSipPdu: missing TrunkGroup" in the INFO level logging for a normal INVITE and non-INVITE call when TrunkGroup is enabled. **Root Cause:** While processing the outgoing SIP PDU in SIPSG, before forwarding it to SIPFE, the SBC is expected to fetch the TrunkGroup from the service group only for (1) SIP Request messages (excluding CANCEL, ACK, PRACK, REFER and BYE) and (2) SIP responses where a new IPTG is selected based on SMM operation (storeIpTg). Since, TrunkGroup is not fetched other SIP messages, it prints the error log for other SIP messages. **Steps to Replicate:** 1. Make a REGISTER call between Party A and B. 2. Check the info level log. The minor error "SipSgSendSipPdu: missing TrunkGroup" is logged for outgoing 200 OK response of incoming REGISTER	The code was modified so that the necessary condition is added such that error log is printed only for those SIP messages for which TrunkGroup is fetched from the service group. **Workaround:** No Workaround.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135584	N/A	2	emssftp Account Expiry in SBC **Impact:** The emssftp account expired in the SBC. **Root Cause:** The emssftp account expired in the SBC because the account aging script was called, and it was changed for default expiry age, which is 30 days. **Steps to Replicate:** Once the application online and connected to RAMP, check the emssftp expiry date using; $sudo chage l emssftp	The code was modified to skip the emssftp from account age modification calls. **Workaround:** Not Applicable
SBX-134613	N/A	2	EMA cosmetic issue in filter under 'SIP Deleted Register Name Status' **Impact:** Searches and filters would not locate 'Register Timer Expired' due to issues with the mapping. The netconf was expecting reg, but the SBC was passing the register. **Root Cause:** Design issue; this parameter was missing in the mapping. **Steps to Replicate:** 1. From the EMA GUI, navigate to Monitoring > Trunks and Subscribers > SIP Deleted Register Name Status 2. Initiate an issue that contains Register Timer Expired 3. Apply a filter to search 'Reason Code = Register Timer Expired' No results will be found 4. Apply a filter to search 'Reason Code = ANY' The deleted register name will be logged as 'Register Timer Expired'	The mapping was corrected. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135304	N/A	2	Script dmesgAnalyzer.sh is filling tmp dir **Impact:** There is a syntax error in the latest dmesgAnalyzer.sh script which fills the tmp directory by creating .tmp files of zero size every minute. **Root Cause:** There is a syntax error in dmesgAnalyzer.sh, causing the SBC to not delete .tmp files of zero size. **Steps to Replicate:** 1. Install the fix version 2. Confirm the folder /var/log/sonus/tmp/ is not flooding with .tmp files of zero size	The code was modified to fix the syntax error in dmesgAnalyzer.sh **Workaround:** No workaround
SBX-134843	N/A	2	Port Status not Showing in EMA after upgrade from 9.2 to 11.1.2 **Impact:** The commands packetPortStatus and mgmtPortStatus do not execute when issued from the EMA. **Root Cause:** An issue with how the SBC implements get_object for the packetPortStatus and mgmtPortStatus commands prevents them from executing correctly. **Steps to Replicate:** 1. Execute the packetPortStatus and mgmtPortStatus commands from the EMA 2. Execute the packetPortStatus and mgmtPortStatus commands with keys from the CLI 3. Execute the packetPortStatus and mgmtPortStatus commands without keys from the CLI	The code was modified to return a correct response when get_object keys include ce_name. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136418	N/A	2	Failures are being observed while Applying Kyverno policies via k8s-kyverno-policies cli **Impact:** Kyverno validation for the SBC-CNF failed due to policy violations in the Helm charts. **Root Cause:** The Helm chart was missing several necessary flags, and some policies required patching. **Steps to Replicate:** 1. Download and Install Kyverno CLI 2. Render your policies with patches from ribbon k8s-kyverno-policies repo 3. Render your Helm charts into resources.yaml 4. Scan your rendered resources for policy compliance against rendered policy. For more details refer: https://bitbucket.rbbn.com/projects/IN/repos/k8s-kyverno-policies/browse/kyverno-cli	The required flags and policies were patched into the Helm charts. **Workaround:** Manually patch the policies and update the Helm charts with missing flags

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136383	N/A	2	TLS certficates are not applied to SLB (Managed Pods) which causes config sync issue. **Impact:** TLS certficates are not applied to SLB Managed Pods, causing a config sync issue with managed pods. **Root Cause:** When a TLS certificate is at set using the CLI set command (set system security pki certificate) along with a TLS key, the TLS key was not copied to the managed pod which, causing playback at managed pods to fail. **Steps to Replicate:** 1. In the OAM pod, create the following certificate: set system security pki certificate SBC_CERT fileName sonuscert.pem passPhrase gsx9000 state enabled type local keyFileName sonuscert.key 2. Commit the request: request system admin vsbcSystem saveAndActivate The playbackfile import will fail	Modified the code to correctly copy the required file. **Workaround:** There is no issue in setting PKCS#12 format certificate file, which does not require key file.
SBX-135181	N/A	2	EnmP coredump during update to V12.01.03R000 **Impact:** The ENM process is blocked, resulting in a core dump. **Root Cause:** The fstrim service is triggered during a switchover after an upgrade, locking up the DRBD partition and discarding unused blocks. This block ENM as it tries to write logs in that partition. **Steps to Replicate:** Upgrade SBC HA to 12.1.4 and make sure that ENM is not coredumping during a switchover.	The 'Persistent' field value was modified to 'false' in the fstrim.timer service so that the timer does not get triggered when running 'systemctl daemon-reload' during switchover. **Workaround:** No workaround.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135278	SBX-130504 (10.1.6)	3	Inconsistency in 'disconnect initiator' CDR field when call disconnected due to teardown SMM **Impact:** A disconnected initiator shows the incorrect reason in the CDR for an ingress SMM teardown. **Root Cause:** The disconnect initiator was not properly updated for the ingress SMM teardown flow. **Steps to Replicate:** Configure the SBC with a basic call config, and provision the ingress and egress SMM rules that utilize the call clear action. For egress - check the CDR, disconnect initiator field (expected = 2) For ingress - check the CDR, disconnect initiator field (expected = 1)	Modified the disconnect initiator to indicate 0,1 or 2 when SMM tears down the call flow. **Workaround:** None
SBX-135277	SBX-130312 (10.1.6)	3	Alarm "sonusSbxNodeResourceCallTraceResetNotification" is not visible in show command **Impact:** The alarm "sonusSbxNodeResourceCallTraceResetNotification" is not visible in 'show command'. **Root Cause:** The sonusSbxNodeResourceCallTraceResetNotification Alarm was not present in confd's display section **Steps to Replicate:** In Admin mode, enter in the CLI: show configuration oam traps admin sonusSbxNodeResourceCallTrace, Expected results: the alarm sonusSbxNodeResourceCallTraceResetNotification will be present	Added this alarm to confd's display section. **Workaround:** none

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135478	SBX-133106 (10.1.6)	3	Fixed - Additional CDR field appears due to SMM **Impact:** Additional CDR field appears after SMM rule to reject certain called numbers with 480 **Root Cause:** For QSBC CDR delimiter is semicolon. So if there is semicolon in the data to CDR field, it would be considered as next field data. **Steps to Replicate:** 1. Configure SBC for a basic SIP-SIP call , configure for QSBC-CDR and do SMM configuration to reject called number of format +444xxxx as given in JIRA. 2. Make a call for number +444xxxx and SBC rejects the Request with 480. **Without Fix:** Generated QSBC CDR record is undecodable with Decoder tool (CDR Tool - SBC 5000 Series) and appears like additional fields for QSBC CDR. **With Fix:** Generated QSBC CDR record is decodable with Decoder tool (CDR Tool - SBC 5000 Series) and no additional fields with QSBC.	The semicolon is removed before writing data to fields of QSBC-CDR. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135479	SBX-133470 (10.1.6)	3	Date and Time is not populated in the Q-CDR format when rejected by SMM **Impact:** Start field (Field 1 and 2) of QSBC is not filled up in customer call scenario of call rejected by SMM and other call scenarios like SBC rejecting call for Parse error. **Root Cause:** Since the call is getting rejected very early, reference timestamps , are not filled up in the record sent by SIPSG. In normal ATTEMPT record, this scenario is handled by checking if reference timestamp is 0 ,and if so ,then take present time of day as disconnect time and calculating backwards to get start time. **Steps to Replicate:** 1.a) Configure SBC for a basic SIP-SIP call , configure for QSBC-CDR and do SMM configuration to reject called number of format +444xxxx as given in JIRA. b) Make a call for number +444xxxx and SBC rejects the Request with 480. Without Fix- Generated QSBC CDR record have 1 & 2 fields(Start Field)empty With Fix- Generated QSBC CDR record have 1 & 2 fields(Start field) value filled up properly.	If reference timestamp is not filled, get disconnect time as present time of day and calculate start time based on it by working backwards ie a. Take delta from calldisconnettime and callattempttime b. Reduce this delta from disconnecttime to get the start time. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135945	SBX-129566 (10.1.5)	3	Bad Codec management with an update with mutliple codecs **Impact:** When the egress endpoint sent an update with multiple codecs, G711 is the first-choice despite of that SBC sent a different codec list on ingress side. **Root Cause:** When UPDATE is received from egress endpoint, a new modify offer gets triggered towards ingress which is getting auto answered with all the ingress peer supported codec instead of the last negotiated codec. This makes SBC to negotiate AMR codec instead of PCMU **Steps to Replicate:** 1. UAC sends AMR, PCMA to SBC. 2. SBC sends AMR, PCMA to UAS. 3. UAS sends 183 w/ PCMA 4. SBC sends 183 w/ PCMA 5. UAS sends UPDATE w/ PCMA, AMR 6. SBC sends UPDATE w/ AMR to UAC At step 6, SBC is sending UPDATE with AMR instead of PCMA.	Modified the auto answering logic so that it answers with the last negotiated codec. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135234	SBX-124004 (11.1.2)	3	RTP flow is asymmetric between the Ingress and egress legs in a GW-GW call **Impact: The** RTP flow is asymmetric when the SBCX auto-answers to an incoming Re-INVITE with all the potential codecs from route PSP instead of negotiated codec from initial offer-answer. **Root Cause:** When the SBC performs an auto answer to an incoming Re-INVITE, it sends out all the potential codecs from the route PSP. This results in the asymmetric RTP flow as the answer is with codecs list different than the negotiated codec in initial Offer-Answer. **Steps to Replicate:** 1. Make a SIPp(A) - SBX - SIPp setup(B) 2. Follow the codecs in same sequence. 3. Ingress PSP: a. G711A, packet size 10, RFC 2833 b. G729A, packet size 10, RFC 2833 c. G711U, packet size 10, RFC 2833 d. This leg: G711A, G711U, G729, T38 e. Other leg: G711A, G711U, G729, T38 f. Transcode conditional 4. Egress PSP: a. G729AB, RFC 2833 b. G711A, RFC 2833 c. This leg: G711A, G711U, G729 d. Other leg: G711A, G711U, G729 e. Transcode conditional 5. Ingress IPSP: Minimize Relaying of Media 6. Egress IPSP: Minimize Relaying of Media	A code fix is introduced in SG-FSM so that when the SBC performs auto-answer, it auto-answers with last negotiated codec. **Workaround:** No Workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
			7. A calls B, B responds with G711A. A offers with 18 8 0 101. 8. Call between A and B is established with codec 8. 9. B sends a Re-INVITE with new offer 8 18 101 10. SBC auto-answer this Re-INVITE with 8 18 101	
SBX-135805	SBX-129189 (11.1.3)	3	The code change made under SBX-126714 requires enhancement **Impact: The** SBC accepts invalid crypto tag value. **Root Cause:** Missing logic to validate the crypto tag **Steps to Replicate:** Incoming call with crypto tag value 0 or greater than 9	Add logic to respond with 400. **Workaround:** Use SMM to correct the crypto tag value.
SBX-133131	GSX-64173	3	Distorted Faxes on V9 **Impact:** Distorted Faxes on V9 **Root Cause:** Packet is getting discarded whenever peer's redundancy setting is higher than the SBC's redundancy setting. **Steps to Replicate:** 1. test0 > (1> {}(t38 numberOfRedundantPackets in SBC(default config in SBC)),2{-}>(UDPTL Redundancy depth image in rightfax)) 2. test2 > (0>(t38 numberOfRedundantPackets in SBC),2>(UDPTL Redundancy depth image in rightfax	When the SBC's redundancy is set to 2, there are no discards regardless of the peer's settings. Redundancy set is configurable under PSP, but configuring this through PSP sends additional redundant packet. There is no need for redundant packets, rather interested in increasing credit rate only. The SBC is set with a default redundancy 2 (T38_HS_RED_PKT_2) instead of PSP configuration (pktRedNum). This changes will increase only credit rate and won't send any redundant packets. **Workaround:** -

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133798	SBX-130752 (10.1.6)	3	The SWe SBC is up and running as Active when UXPAD is down. (UXPAD is responsible for Packet de-queuing and RTP handling and playout processing). **Impact:** The problem is related to when the UXPAD process on the active node segfaults or dies. When the standby node takes over as the active node, the UXPAD process on the installed standby node has also been killed, resulting in the UXPAD being down even though the Swe SBC is active. **Root Cause:** The root cause of the problem is that when the UXPAD process on the active node is killed, and the standby node takes over as the active node, the UXPAD process on the newly active node could also get killed. At this time, a proper restart should be triggered on the node whose current role is active **Steps to Replicate:** Perform a switchover and 'kill -9' UXPAD process on SBC going active.	Added Timer function to monitor for UXPAD restart events, In case of restart then timer will wait until timeout - check health of UXPAD and trigger restart of the node again. **Workaround:** Restart SBC node.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134492	N/A	3	Due to using an abnormal workflow, the SBC was unable to properly register to RAMP and save its configuration to RAMP. **Impact:** If SBC-B is the active SBC when pair is first registered to RAMP, then after switchover, it may not be able to connect again and the following error is seen; `.SM *ConfigManager::processConfigRevision: getEmsCredentials failed!` **Root Cause:** Acl rules do not get not added correctly after switchover on new standby. **Steps to Replicate:** 1. Bring up SBC 1:1 HA pair. 2. Once both the active and standby SBC are up, perform a switchover. 3. Wait for the new standby SBC to come up. 4. Create cluster on RAMP 5. The new standby should be able to register to RAMP.	To add ACL if not present during every retry of registration to RAMP **Workaround:** reboot the standby node post every switchover

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-136350	N/A	3	The option to drop REFER from ALLOW header was available in 9.x VNF SBC but this is not available on 12.x CNF SBC. **Impact:** "methods refer reject" option not available under TG signaling option in CNF **Root Cause:** The issue was seen because of a conditional check that prevented the configuration to allow/reject for method refer from being displayed in microservices. **Steps to Replicate:** TC1 : 1. Configure - set addressContext default zone <zone> sipTrunkGroup <siptrunkgroup> signaling methods refer reject Expected results : The above configuration should be successfully committed.	The code has been modified to allow the configuration for microservices. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133981	N/A	3	Changes made to 'eventLog -> saveTo' setting not honored after an upgrade **Impact: The '**eventLog -> saveTo' setting would revert back to default after reboot. **Root Cause:** Post switchover/ upgrade sonusEvLogTypeSaveTo is always set to the default value [Disk]. As a result, after the switchover/upgrade, SBC is always saving the logs locally. **Steps to Replicate:** 1. Make a basic sip-sip configuration on an HA pair. 2. Modify the saveTo as follows: `set oam eventLog typeAdmin trace saveTo none` `set oam eventLog typeAdmin acct saveTo none` Note: Check for all log types. 3. Rollover the respective log; SBC will not allow rollover. Verify that the log type for which saveTo is set to none is not saved in evlog. 4. Do a switchover and verify the saveTo setting in the current active SBC. 5. Rollover the respective log; SBC will not allow rollover. 6. Run a call Verify that the log type for which saveTo is set to none is not saved in evlog.	Made code change such that the value is not reverted back to "Disk" so that the saveTo setting is honored after an upgrade/ switchover. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134892	N/A	3	Upgrade pre-check failed on SBC running 10.01.05 to 12.1.0 due to Confd commit syntax change related to Gemalto License Server Configurations **Impact:** A pre-upgrade check which was added a while back in 10.1.x errored while executing the steps to remove the licenseServer details from the CDB failed. **Root Cause:** Confd commit command has changed in 12.1.3 and higher. Old command: $CONFD_CMD -e -c "maapi_lock;mdel system/licenseServer{EMS};ccommit;maapi_unlock" New command: $CONFD_CMD -e -c "maapi_lock;mdel system/licenseServer{EMS};mcommit2;ccommit;maapi_unlock" **Steps to Replicate:** 1. Bring up SBC in 9.2.3R4 (or any other version where / system/licenseServer table is supported) 2. Configure the licenseServer details 3. Upgrade to latest of 12.x where licenseServer has been deprecated. Results: Upgrade should go through without any issues. Export the CDB and check all the entries under system/licenseServer has been removed.	Added proper code to remove / system/licenseServer details during upgrade as this table has been marked obsolete in latest releases. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135904	N/A	3	Importing a valid SBC private key for CDR transfer to a CDR server using the `loadPrivateKeyFile` command may fail. **Impact:** When we added the logic to validate the type of key used for the CDR server, we missed the edge case where the customer can add a comment with spaces, and due to this it would fail, since the code will search for the 4th column and space can be a delimeter. **Root Cause:** The root cause was that we were searching for the 4th column, and hence when a comment with spaces was added, we would get the wrong value. **Steps to Replicate:** Create a key pair with a comment in the key ssh-keygen -f /opt/sonus/external/test1 -C "(ABC) Just a Comment" Load the key file in the CDR server	The system will now take the last column from the output of "ssh-keygen -lf" **Workaround:** No workaround, requires fix

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-135302	N/A	3	The SBC failed to start after an abrupt shutdown. **Impact:** The LCA is unable to restart the application due to disk corruption in the SBC VM. **Root Cause:** Disk corruption resulted in the `/opt/sonus/conf/platform.json` file being emptied. This prevented the index-exchange serf from starting. The LCA detects the serf failure and subsequently shuts down the application. **Steps to Reproduce:** 1. Manually clear the contents of `/opt/sonus/conf/platform.json`. 2. Reboot the SBC VM. 3. Observe that the application fails to start.	The Index Exchange Serf application is enhanced to detect and automatically recover from scenarios where the `platform.json` file is corrupted or emptied. The serf program is able to start up correctly. **Workaround:** To mitigate the issue without applying the update: 1. Delete the `/opt/sonus/conf/platform.json` file. 2. Reboot the SBC instance. 3. Observe that, upon reboot, the Serf application automatically generates a new `platform.json` file.
SBX-136310	SBX-136135 (11.1.2)	3	A memory leak was reported against version 12.01.04R000 when the "Store P-Charge-Vector" is enabled. **Impact:** A memory leak occurred under load with registrations when the "Store P-Charge-Vector" is enabled. **Root Cause:** The system lacks the necessary logic to free allocated memory after sending a 200OK registrations to the IAD (Integrated Access Device) during registration. **Steps to Reproduce:** 1. Enable the "Store P-Charge-Vector". 2. Initiate a registration request from an IAD containing a PCV header. 3. Observe memory consumption and verify if the memory is released after sending the 200 OK response.	Free PCV memory to resolve the issue. **Workaround:** Disable "Store PCV"

Resolved Issues in 12.01.04R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125500	N/A	1	SBC sends BYE to both ingress/ egress just after the call is established **Impact:** In a forking call, different dialogs use AMR-WB with different mode sets as the calls transition from an early dialog state to a call completion state. The SBC relays AMR-WB full mode and restricted mode sets end-to-end and not locally answered as it might result in no audio scenarios for short durations. This is observed in customer production networks and is currently resolved using SMM. **Root Cause:** In a forking call where different dialogs use AMR-WB, having different mode sets as the calls transition from an early dialog state to a call completion state. The SBC relays AMR-WB full mode and restricted mode sets end-to-end and not locally answered because it might lead to no audio scenarios for short durations. The SBC SG module needs to relay the AMRWB variants. **Steps to Replicate:** NA	N/A **Workaround:** NONE

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133608	N/A	1	[12.1.3] SBC services do not come up after enabling FIPS mode. **Impact**: The SBC services did not come up when enabling FIPS mode. Thus, users cannot see the "libcrypto does not support 'sha-512" message. **Root Cause:** As part of the confd upgrade, some set caps for confd-related binaries were added, which is fine in non-FIPS mode but gives the above error in FIPS mode. **Steps to Replicate:** 1. Bring up the system using the latest build. 2. Perform a FIPS configuration. After enabling fips, SBC services should come up fine.	These changes are commented out to fix this issue. **Workaround**: None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133696	N/A	1	CNF: Core dump not getting captured as part of SysDump pod **Impact:** Core dump is not getting captured as part of sysDump pod. **Root Cause:** 1. The coredump handler is present in a different namespace. 2. Cross-namespace access is not supported. 3. The sysDump pod does not have access to the coredump retriever pod. **Steps to Replicate:** Test Case Steps: 1. Download the sysDump pod Helm package. 2. Update the values.yaml file with the required configurations. 3. Install the Helm chart. Test Case Expected Results: 1. The package is downloaded successfully. 2. All required values in the values.yaml file are updated correctly. 3. The sysDump pod is running and can collect both the sysdump and coredump.	The code is modified in the following manner: 1. Added support for the sysDump pod to access the coredump retriever. 2. Enabled cross-namespace access between the sysDump and coredump namespaces. 3. The sysDump pod can now log into the coredump retriever pod and collect the coredumps. **Workaround:** None
SBX-133754	N/A	1	CNF-CSAR : Modify the README.createCnfCsar file after internal testing **Impact:** The README.createCnfCsar file requires modification. **Root Cause:** The command line argument "product_build" in one of the command examples was specified twice. **Steps to Replicate:** Review the changes Readme file changes.	The code is modified to remove the extra "product_build" argument from the command example. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134054	N/A	1	Machine congestion is experienced after upgrading to 12.1.2R0 **Impact:** After upgrading to 12.1.2 on an SBC 5400, users observed machine congestion when the Java process uses most CPUs. **Root Cause:** Ideally, Java only uses up to four CPUs from the 'batch' group. The cgroup batch was not created on the first boot after the upgrade because the sbxcgroup service, which is responsible for creating cgroups, could not determine the hostType since the post-upgrade initialization was not yet completed. **Steps to Replicate:** Perform an upgrade from pre-12.1.2 to 12.1.2 or later on 5400 and check for below string in /var/log/messages "/opt/sonus/etc/init.d/sbxcgroups - Not starting cgroups for unknown hwType - Standard."Alternatively, use the 'cset set' command to check if the group batch is created.With the fix, the above log does not appear, and the cset command shows the 'batch' cgroup.	As a fix, the service order is changed to ensure the sbxcgroup service runs only after the CHS service runs, as CHS determines and sets hostType. **Workaround**: Reboot the SBC to fix this issue.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134179	N/A	1	The SBC fails to relay SIP NOTIFY messages to non-NAT SIP endpoints after upgrading from 9.2.5R4 to 10.1.5R3 or later **Impact:** After upgrading from 9.2.5R4 to 10.1.5R3 or later, the SBC fails to relay SIP NOTIFY messages to non-NAT SIP endpoints. **Root Cause**: Implementing SBX-119575 introduced this issue.For non-NAT endpoints, the SBC populates the contact URI to the peerAddr; However, the SBC's connection manager sends the message using connectionId only.Previously (with the SBX-119575 fix), when incorrect data was present in a remote target, no issue was observed. Now that the SBC validates the remote TSAP with the address saved in CnxId, this fault was identified and corrected. **Steps to Replicate:** 1. Register a non-NAT IPv6 endpoint using modified via and contact headers, as well as actual via and contact headers. 2. Send a SUBSCRIBE and NOTIFY from the UAC and UAS, respectively. Expected: Notify completes successfully with 200ok and no timeouts. 3. Repeat the above test with non-NAT IPv4 endpoints.	Added a check to take the correct data from the RCB while creating the ingress PDU for non-NAT endpoints. **Workaround:** Enable signaling NAT.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134253	N/A	1	CNF: Observed a restart on the NS pod post-upgrade from 12.1.2-R001-333 to 12.1.3-127 build **Impact:** An NS pod restarted during the pod upgrade. **Root Cause:** Based on the analysis logs, the issue was caused by the following event during the NS upgrade. 1. One of the NS pods started an upgrade while the other NS pod was in an Active Role. 2. The RAC also started upgrading and came up with no agent entries. 3. With a readiness probe time of 30 seconds, Kubernetes does not broadcast the RAC IP in the service discovery query response for the next 30 seconds. 4. During the RAC 10-second learning window, it accepts registrations but does not accept new Role requests. a. The learning window expires after 10 seconds. Now, the RAC accepts any request from the Agents. 5. After 30 seconds, all agents get the RAC Active IP in the Service discovery response. 6. The NS pod that started upgrading receives the RAC IP first and then sends a Role request to the RAC Manager. 7. The RAC Manager checks for the Role. Since there are no Agent entries in the RAC. it assigns the active Role to the new NS pod.	The code is modified to delay the RAC Manager learning window for 30 seconds (Using the readiness probe timer) after coming up to allow the existing pod registration to complete, Once the learning window expires, the RAC then allows new role requests, **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
			8. Since an NS node already exists in the Active Role. it also sends a Registration request, which leads to a conflict in the Role since both NS pods have Active Roles. Thus, the RAC asks the original NS pod for a restart and fetches the Role again. 9. This causes the original NS pod to go for a restart. **Steps to Replicate:** 1. Bring up an SBC using the 12.1.2 333 build. 2. Upgrade to the 12.1.3-127 build, Issue Observed: A single restart occurs on the NS pod after the upgrade.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134410	SBX-133822 (10.1.6)	1	TLS connections fail after an upgrade to 10.1.6R0 - private keys of local and local-internal TLS certificates not retrievable from CDB **Impact:** The encrypted operation data fields were dropped during the upgrade. Consequently, the SBC application failed to read configuration encrypted fields after the upgrade. **Root Cause:** As part of FIPs changes, the confd encryption mechanism changed from tailf:des3-cbc-encrypted-string to tailf:aes-cfb-128-encrypted-string. During the upgrade, the confd could not upgrade this encrypted data automatically for some of the fields. **Steps to Replicate:** 1. Bring up the system using a 12.1.x release before 12.1.1 and configure all applicable encrypted-related tables. 2. Run the test cases where the SBC application uses these encrypted fields. 3. Upgrade the system to 12 1 4. 4. Re-run the test cases. Expected results: All tests run without any issues. **NOTE**: Use the following scenarios: • VMWare/Hardware HA • OpenStack 1:1 HA • OAM HA I-SBC OpenStack deployment	Modified the code to convert the data from DES to AES type during an upgrade for encrypted configuration fields and encrypted operational data. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134734	SBX-134495 (12.1.5)	1	MS Teams call transfer failure **Impact:** Call transfer fails when the SBC sends a BYE upon the second transfer from a Teams client. **Root Cause:** The SBC bridges a transferred call across multiple GCIDs. During an MS Teams transfer request to move from an Internal to an External interface, the SBC moves/modifies the corresponding IP resource, during which it fails to pick the correct call leg corresponding to this resource. This leads to a failure and a call tear-down. **Steps to Replicate:** 1. Party-A calls Party-B(TEAMs client), which responds with "X-MS-UserLocation: external." 2. Party-B transfers the call and sends a REFER to the SBC. 3. The SBC initiates a new call to Party-C (TEAMs client), which responds with "X-MS-UserLocation: internal." 4. Party-C sends a re-INVITE to the SBC with "X-MS-UserLocation: external" to switch from the internal to the external interface. Expected Result: The re-INVITE is successful. Actual Result (without fix): The re-INVITE fails.	Modified the code to let the SBC choose the call leg based on its GCID rather than the call GCID while handling the resource's modification. **Workaround:** Remove mediaIpsecondaryinterfacegroupname & change the mediaipinterfacegroupname to a public IP.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134833	N/A	1	CNF: ChmP core observed in OAM **Impact:** When a process is killed, the AMF tries to restart the SBC. Meanwhile, the liveness probe was killed, so the kubectl triggered a container restart, which killed serf and caused a CHM core. **Root Cause:** When the sbx application starts on the other side, the CHM process cores due to the unavailability of serf env variables. **Steps to Replicate:** The CHM core is seen when a process is killed. If the surplus watchdog tries the auto six restart and liveness probes are not yet created, the container will restart simultaneously.	The code is modified to prevent the SBC automatic bring-up if any CNF process fails. Additionally, a reboot is initiated if an abnormal serf process kill occurs. **Workaround:** Delete the pod so that it comes up new,
SBX-134854	SBX-134193 (12.1.3)	1	CNF: Cannot resolve FQDN for IPPEER post-upgrade from 12.1.2-R001 to 12.1.3-123 **Impact:** The IPPEER FQDN resolution started failing after couple of hours when running 10 cps. **Root Cause:** The SBC DNS Client internally toggles its sockets every 100 minutes to create a new socket with a different source port to send a DNS query. Socket toggling is failing. which results in DNS query failures. **Steps to Replicate:** 1. Create a DNS group. 2. Run a call in conjunction with 10 cps calls continuously for more than three hours. Expected results: The call continues after three hours. Actual result: Other calls were also running continuously after 3 hours.	Modified the code to toggle sockets so that a new socket is created properly after 100 minutes. **Workaround:** Delete and then recreate the DNS group.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134992	SBX-133734 (10.1.6)	1	After a switchover, call hold/unhold fails because the SBC is not able to send any in-dialog SIP messages to the registered endpoint **Impact**: After a switchover, call hold/unhold fails because the SBC is not able to send any in-dialog SIP messages to the registered endpoint. A refresh register routine occurs, and a new port may be allocated post-switchover. **Root Cause**: Call Control Block (ccbptr) was not updated with correct value from the updated RCB. **Steps to Replicate**: The issue is easily seen when the endpoints use TCP and TLS transports.Perform the following steps on an SBC HA pair to recreate the issue: 1. Register an endpoint from the IP/Port. 2. Process the endpoint through a basic call. 3. Perform a switchover. a. After the switchover, the endpoint reregisters from a different IP/port (Other than the previous one). 4. The registrar endpoint sends a SIP Notify and then a Re-invite (from UAS) to the endpoint. 5. The SBC is able to send the message (Re-Invite) to the new destination port.	The IP/Port for the new Connection from Address of Record(AOR) block to Call Control Block is updated. **Workaround:** None

The following severity 2-3 issues are resolved in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-127168	N/A	2	CNF: Not able to test SIP Adaptor profile from RAMP GUI for SBC **Impact:** In CNF deployment, not able to test the SIP Adaptor profile from the RAMP GUI for the SBC. **Root Cause:** Testing of SIP Adaptor Profile in CNF deployment was not supported hence the functionality was not working. **Steps to Replicate:** 1. In a CNF deployment, launch the SBC Configuration Manager from RAMP. 2. Under Service option in the left navigation, navigate to the Test Sip Adaptor Profile screen 3. Input the PDU and click **Test Profile.** 4. Profile should be tested and successful response should be displayed.	Code changes have been made to support testing of the SIP Adaptor profile in a CNF deployment. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-128209	N/A	3	SBC ERE delivering a PIPE error while configuring a DMPM rule although the error should contain a message that a POL-RTU license is required. **Impact:** SBC ERE delivering a PIPE error while configuring a DMPM rule although the error should contain a message that a POL-RTU license is required. **Root Cause:** Due to a code defect, the SBC deliverd the wrong error message: "Aborted: PIPE: An error occurred." **Steps to Replicate:** 1. SBX is up and running with the latest version of the 12.1.4 build. 2. Login to configuration mode as admin. 3. Configure the DMPM rule as mentioned in the jira. 4. If the 'SBC-POL-RTU' license is not available then configuring the DMPM rule should deliver the following error, `Aborted: Can't update dmPmRule subRule. License SBC-POL-RTU not available.`	The code has been fixed to deliver the correct error message "Aborted: Can't update dmPmRule subRule. License SBC-POL-RTU not available." **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-129376	N/A	2	The sipSigPortTlsStatistics ->currentServerSessions counter is leaking and stuck at value 20480 **Impact:** Under sipSigPortTlsStatistics ->currentServerSessions the counter does not appear to decrement when session terminates. **Root Cause:** When the remote connection shuts down and read fails, the counter is not decremented correctly. **Steps to Replicate:** Configure TLS Session Make a SIPP call for TLS Check the currentServerSessions counter Counter is not reduced after the session termination	Changes have been made to tear down the session when the Read fails due to remote termination. **Workaround:** NA
SBX-130407	N/A	3	The SBC is printing SIP logs in AUD log whenever SMM action is modified via the GUI **Impact:** A SIP message is entered into the AUD log whenever SMM action is modified in the SBC using EMA. **Root Cause:** SMM action responses were coming to AUD logs where AUD logs were meant for any create, update, or delete configuration. **Steps to Replicate:** 1. Create SMM rule profile (criteria all, action add a new header). 2. Select the SMM profile and run the test SMM. 3. Verify that input/output logs are in DBG logs.	A new extension at YANG level was introduced so that the action command results can be redirected to DBG logs. We can use this extension for directing any action command results to DBG logs. **Workaround:** Not Applicable

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-130581	N/A	3	The SRS Group Cluster showed additional entries after the upgrade **Impact:** The 'SRS Group Cluster' profile displayed additional entries after the upgrade. **Root Cause:** Incorrect upgrade code logic caused the profile to display additional entries. **Steps to Replicate:** Verify that no additional entries are displayed in the profile after the upgrade.	The upgrade code logic has been corrected, and the profile no longer displays additional entries after the upgrade. **Workaround:** NA

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-130778	N/A	2	SWe SBC XRM congestion alarm **Impact:** For SBCs that were recently upgraded to 11.1.1R1, an XRM congestion alarm was triggered at midnight almost every day **Root Cause:** Starting with SBC 11.1, Debian11 OS is in use and cgroupv2 is enabled by default in debian11. In this version, systemd defaults to the "unified" cgroup hierarchy. However, the SBC doesn't require it and we override this setting by passing grub kernel option: systemd.unified_cgroup_hierarchy=false. When we do an upgrade from pre-11.1 to 11.1+ in SWE, as part of upgrade we do a reboot and after boot via initrd we enable grub settings, update software and so on. Since we already booted by this time, our kernel options for current boot will still be same as pre-11.1 and we would be missing "systemd.unified_cgroup_hierarchy=false" in /proc/cmdline. This causes unified cgroup hierarchy to be 'on' after upgrade and causes missing cpuset files. **Steps to Replicate:** 1. Install SBC version 9.2.x. 2. Perform an upgrade to the fix version 3. After upgrade when the SBC comes up, the cpusets files shouldn't be missing and /proc/cmdline should have "systemd.unified_cgroup_hierarchy=false" set for 11.1+ versions.	The code has been modified to do the grub update before a current reboot to ensure proper kernel options on first boot with new software. **Workaround:** Do an additional reboot after upgrade.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-130861	N/A	2	The SBC fails to connect to the CDR server over SSH with non-RSA keys **Impact:** Not able to use CDR server with non RSA keys, and the SBC is accepting the keys that it doesnt even support **Root Cause:** Old libssh package and no proper validation for the acceptance of the key **Steps to Replicate:** request oam accounting cdrServer admin primary loadPrivateKeyFile fileName dsa	We have updated the libssh package which adds support for ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256 Proper validation of key is done, which rejects the key which it doesn't support **Workaround:** Fix is provided
SBX-132970	N/A	2	Input Validation should be provided for sshdConfig ciphers, sshdConfig macs, and sshdConfig kexalgorithms. **Impact:** sshdConfig inputs were not validated **Root Cause:** Input validation logic was missing. **Steps to Replicate:** `admin@vsbc1% set system admin vsbcSystem sshdConfig ciphers a [ok][2024-10-17 08:00:42] [edit] admin@vsbc1% co Aborted: 'system admin vsbcSystem sshdConfig': Invalid SSHD_CONFIG algorithm Suggested: 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-`	Added the input validation logic in ConfD commit phase. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
			gcm@openssh.com,chacha20-poly1305@openssh.com, [error][2024-10-17 08:00:44] admin@vsbc1% set system admin vsbcSystem sshdConfig ciphers (<This data type is used to model textual information taken from the NVT ASCII character set. This type is similar to SonusString but is much larger. It is a replacement for xs:string and xsd:string, since all strings must have a maxLength specified.>) (3des-cbc,): des [ok][2024-10-17 08:01:39] [edit] admin@vsbc1% co Aborted: 'system admin vsbcSystem sshdConfig': Invalid SSHD_CONFIG algorithm Suggested: 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-	

Issue ID	Original Issue	Sev	Problem Description	Resolution
			poly1305@openssh.com, [error][2024-10-17 08:01:43] admin@vsbc1% set system admin vsbcSystem sshdConfig macs (<This data type is used to model textual information taken from the NVT ASCII character set. This type is similar to SonusString but is much larger. It is a replacement for xs:string and xsd:string, since all strings must have a maxLength specified.>) (hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com, hmac-sha2-256,hmac-sha2-512): scd [ok][2024-10-17 08:03:29] [edit] admin@vsbc1% co Aborted: 'system admin vsbcSystem sshdConfig': Invalid SSHD_CONFIG algorithm Suggested: hmac-sha1,hmac-sha1-96,hmac-sha2-256,hmac-sha2-512,hmac-md5,hmac-md5-96,umac-64@openssh.co	

Issue ID	Original Issue	Sev	Problem Description	Resolution
			m,umac-128@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-md5-etm@openssh.com,hmac-md5-96-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com, [error][2024-10-17 08:03:31]	

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133166	N/A	3	SWe: Modification of digitParameterHandling parameter presentation under subRule not working **Impact:** Modification of digitParameterHandling parameter presentation under subRule was displaying the wrong flag. **Root Cause:** Due to a code defect, the 'presentation' flag was retrieving the value from the wrong attribute column, causing it to display the incorrect flag. **Steps to Replicate:** 1. SBX is up and running with the latest version of the 12.1.4 build. 2. Login to the configuration mode as admin. 3. Execute the following command to configure the 'presentation' flag: `set profiles digitParameterHandling dmPmRule PAI_AND_FROM_HEADER subRule 0 parameterManipulation presentation allowed commit` `show configuration profiles digitParameterHandling dmPmRule PAI_AND_FROM_HEADER subRule 0 parameterManipulation presentation` 4. The 'presentation' flag should display the configured flag, `presentation allowed;`	The code has been fixed to fetch the value from the correct attribute column. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134339	SBX-133358 (12.1.2)	3	The SBC does not clear the sonusSbxNodeResourcesPacketLossThresholdExceededNotification2 alarm when the call disconnects **Impact:** The SBC does not clear the sonusSbxNodeResourcesPacketLossThresholdExceededNotification2 alarm when the call disconnects. **Root Cause:** The code present in the NrmaDeallocCallLeg() routine clears the sonusSbxNodeResourcesNoPacketsReceivedClearNotification2 alarm when the call disconnects, but no code is present to clear the sonusSbxNodeResourcesPacketLossThresholdExceededNotification2 alarm. For a generic call flow, the alarm gets cleared with the Helmp of NrmaPktLossTrapClear(), which is called from NrmaProcessXrmRtpActivityStatusNotify. But, if the call disconnects suddenly, this alarm does not clear properly. **Steps to Replicate:** 1. Set up a basic SIP-to-SIP call in a Standalone node. 2. Complete the following Config: `set profiles media packetServiceProfile DEFAULT peerAbsenceAction peerAbsenceTrap`	The code is modified to clear the alarm properly, along with the NrmaPktLossTrapGenerate trap. **Workaround:** None.

Issue ID	Original Issue	Sev	Problem Description	Resolution
			3. Set up packet Loss threshold at which the SBC should generate the alarm sonusSbxNodeResourcesPacketLossThresholdExceededNotification2 (for example, `set profiles media packetServiceProfile DEFAULT rtcpOptions rtcp enable packetLossThreshold 5000 packetLossAction packetLossTrap,` in this case if a number of packet Losses exceed 5% of a total number of packets.) 4. Check if the trap of packet loss is triggered in node (`show table alarms currentStatus`). 5. Run the call with media (which has some lost packets). 6. After trap generation, make a sudden disconnect. 7. Check in the node if traps are cleared automatically. In the log, verify whether logs related to NrmaPktLossTrapGenerate and NrmaPktLossTrapClear are present or not.	

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133684	N/A	3	SBC-CNF (12.1): The CSAR create Python script produces incorrect TOSCA.meta file contents **Impact:** CNF CSAR create Python script produces incorrect TOSCA.meta file contents. **Root Cause:** The TOSCA.meta file contents were incorrect due to a logical error while populating images and scripts path and typos "Created-By" and "Entry-Scripts". **Steps to Replicate:** Generate CSAR and check TOSCA.meta file contents	Corrected the logical error for populating images and scripts path and typos "Created-By" and "Entry-Scripts". **Workaround:** None
SBX-133729	N/A	3	The rsyslog service is restarted every 5 minutes **Impact:** The rsyslog daemon gets restarted every 5 minutes on the SBC. This does not cause any service impact. **Root Cause:** A cronjob configured to check health of remote syslog server was restarting rsyslog daemon if its RSS usage was going beyond 10MB or if memory usage was above 0.5%. **Steps to Replicate:** 1. After installing SBC 12.1.2 or later, check /var/log/syslog. 2. If rsyslog consumes more than 10MB RSS, we would see rsyslog restarts every 5mins without logs on reason for restart. 3. With the fix build, we will not see restarts unless RSS usage goes beyond 30MB and we would notice log entry in syslog regarding restart.	resource limits for rsyslog have been relaxed to avoid it getting restarted unnecessarily. **Workaround:** reboot

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133759	N/A	2	The SBC didn't send calling party number value in Accounting-Request (Radius protocol) **Impact:** When FROM header in INVITE comes with only digits and its length is more than 31, SBC considers it as Calling Party URI instead of Calling Party Number. Thus, SBC sends userpart as Calling Party URI to PSX/ERE. **Root Cause:** SBC does not validate the FROM header userpart for digits only. **Steps to Replicate:** 1. Make Basic A - SBC-B call using ERE setup 2. Make A to B call. From header userpart contains only digits more than 31. 3. Call is successful. 4. In info level debug log, INPUT DATA contains Calling Party Number with no Digits. 5. OUTPUT DATA contains Calling URI instead of Calling Number. 6. SBC does not truncate the calling number in FROM header of outgoing INVITE.	A new utility function is introduced which validates userpart of FROM header and if it contains only digits (global or local), then it is considered as Calling party number. **Workaround:** None
SBX-133832	N/A	3	SBC-CNF (12.1): CSAR create Python script fails for Cluster Readiness Checker tool **Impact:** CNF CSAR create Python script fails for Cluster Readiness Checker tool **Root Cause:** An array was defined to hold Helm chart name was hardcoded to accomodate only sbc core Helm chart name. **Steps to Replicate:** Validate for sbc Helm charts. Validate for cluster-readiness charts.	The fix is given with flexibility accommodate any Helm chart. **Workaround: N**one

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133924	SBX-133809 (10.1.5)	2	The SRTP SBC failed to reset the encryption ROC when INVITE w/ Replaces replaced the unencrypted call leg **Impact:** After a re-INVITE w/ Replaces, a new SSRC was generated but the SBC failed to reset the ROC which caused the audio issue. **Root Cause:** When ssrcRandomizeForSrtp is enabled, NRMA will generate a SSRC for RTP and send it in flow change command to XRM. XRM then saves it in XRES structure in order to detect future SSRC changes. When XRM is processing RTCP only flow change command, internal saved SSRC got cleared which causes XRM to not detect SSRC change in the new RTP flow change command. Therefore XRM failed to inform NP to reset ROC when programming new RID.	Ribbon modified XRM to only change SSRC value in XRES when processing RTP flow change command. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
			Steps to Replicate: Please use following procedure: 1. Make an SRTP to RTP call without transcoding; make sure that ssrcRandomizeForSrtp flag is enabled in the SRTP PSP. The mediaNat must be enabled in the SRTP PSP also. 2. Make sure that the SBC learned (media NAT learning) the remote RTP and RTCP IP:ports on the SRTP call leg successfully. 3. The call should be long enough to roll over the SRTP sequence number (SSN) so that the encryption ROC increments from 0 to at least 1. This would be more than 23 minutes for a call that uses 20 ms RTP packetization time. 4. Send an INVITE w/ Replaces to replace the RTP call leg; the SDP in the INVITE w/ Replaces shall have the same media IP:port, same codec, same SRTP crypto key as the SDP in the 200 OK to the initial INVITE. The SSRC of the RTP stream coming into the SBC from the RTP peer shall stay the same too. 5. Step 4 will trigger a re-INVITE to the SRTP call leg. After the SBC re-learns the RTP IP:port on the SRTP call leg, check the value of the encryption ROC on the SRTP call leg.	

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133927	SBX-133802 (10.1.x)	2	SG-FSM: SgOaMinimizeMediaChanges() unexpectedly suppressing re-Invite **Impact:** The SBC is not able to send a reInvite with new codec after playing a tone. **Root Cause:** The minimize relay flag is not supposed to suppress this reInvite. **Steps to Replicate:** A(8, 18, 101) ->B(8, 18, 101) 180 (8,101) <-180() playing tone 200(8,101) <-200 (18, 8, 101)	Even with minimize flag set, if the new active codec does not match the previous one (playing tone), SBC should send a reInvite. **Workaround:** Disable tone
SBX-133959	SBX-133497 (11.1.3)	3	SamP cored on the standby node **Impact:** Customer is seeing repeated cores of the SAM Process on the Standby. **Root Cause:** The cores are all a result of either a HashInsert or a HashRemove to a recording hash table. Calls may be put in this hash table if they are "recordable" (media recording is configured on the Trunk Group) but they are NOT of callType SIPFE_SIP_RECORDER_CALL: / ADDRESS_CONTEXT:/zone/ sipTrunkGroup/media/recordable The corruption in the hash table is the result of a call block which has been freed without having been removed from a hash table. **Steps to Replicate:** This issue is not reproducible.	Code has been added that will ensure that the call block is always removed from the hash table before the call block memory is freed. **Workaround:** The only prevention may be this issue by disabling media recording on all trunk groups.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133963	SBX-133780 (11.1.3)	3	ScmP cores **Impact:** SCM cores when processing a SUBSCRIBE message that has a NULL fromTag (and this request followed a previously challenged Subscribe). **Root Cause:** The code is missing a NULL pointer check. As a result, a core will occur when the fromTag in the incoming message is compared to the current "ingressRemoteTag" because the SBC will attempt to dereference a NULL pointer. NOTE: The incoming Subscribe is related to a request that was "Challenged" and the new fromTag is NULL **Steps to Replicate:** This bug was found by code inspection.	The code is modified to add a NULL pointer check has been added. **Workaround:** None.
SBX-134083	N/A	3	CNF: CSAR create Python script produces incorrect images path in TOSCA.meta file **Impact:** CNF CSAR create Python script produces incorrect images path in TOSCA.meta file **Root Cause:** The image path given while generating TOSCA.meta file was one directory level above the actual path. **Steps to Replicate:** Run the CSAR script and check the image path in TOSCA.meta file.	Fixed by providing actual image path while generating TOSCA.meta file. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134105	SBX-133154 (11.1.3)	2	Call cleanup occurring unexpectedly **Impact:** Calls are cleared incorrectly when a 'call audit' is initiated. **Root Cause:** During an extensive call audit, NRMA can get delayed while waiting for a CPC reply message if an audited call terminates/disconnects before the CPC sends a reply message. Due to this race condition, NRM's call cleanup is triggered consecutively, and some transient calls are cleaned incorrectly. **Steps to Replicate:** The extensive audit is triggered by unsolicited call cleanup events. This is a race condition issue and no instructions are available for simulating an audit and verifying the fixes.	The NrmaDeallocCall() is modified to define a new local fault type to register internally. A call is flagged with a new faultId to stop the audit reply timer. When the NRMA receives a response, it locates the corresponding fault management structure and notifies the NRM of the audit result. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134205	N/A	3	SWE FQDN appears in CANCEL R-URI **Impact:** When FQDN is used in the IP peer, the RURI of CANCEL and ACK does not match the original INVITE request message. **Root Cause:** Code is missing to update the RURI of CANCEL and ACK for non-2xx responses with the original INVITE when the IP Peer is set to FQDN. **Steps to Replicate:** 1. Make an A-to-B call in an ERE setup. Use FQDN in the IP Peer. 2. Create a local record for FQDN resolution and attach it to the egress leg. 3. Make the call. 4. The SBC sends an INVITE with a resolved IP address in RURI. 5. Send a CANCEL from the client script. 6. The SBC sends a CANCEL towards the egress with the FQDN in the RURI. 7. The server responds with a 487 Request Terminated. 8. The SBC responds back with an ACK that has the FQDN in its RURI.	The CANCEL and ACK RURI for non-2xx are updated with the RURI of the original INVITE by fetching the RURI from the INVITE transaction control block. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134232	SBX-134037 (10.1.6)	2	High SWe_NP CPU causing the XRM congestion on KVM SBC **Impact:** The SWeNP process is using 100% CPU usage for 1 worker-core deployment. **Root Cause:** When a call flow changes, XRM notified SWeNP to resume RTCP Generation but RTCP Generation was not enabled. SWeNP returned an error to XRM but mistakenly armed the RTCP Generation timer with 0 seconds, causing SWeNP to send out RTCP packets rapidly. **Steps to Replicate:** 1. Enable RTCP Termination. 2. Call performs a NAPT Learning for a remote IP that has never been used. 3. The SBC learns the remote IP from the RTP and sends out an ARP/ICMPV6 Neighbor Solicitation to resolve the remote IP's MAC. 4. Remote IP is slow to respond to the ARP/ICMP Neighbor Solicitation request.	Correct the error handling so the RTCP Generation timer does not get armed. **Workaround:** Do not enable RTCP termination.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134263	N/A	2	LI- Last_Redirecting_Party and Original_Called_Party are not getting populated from the OUTPUT DATA **Impact:** For the default LI intercepted call, the Signaling Start message does not correctly populate Last_Redirecting_Party and Original_Called_Party. **Root Cause:** In the Signaling Start message, the Last_Redirecting_Party and Original_Called_Party are not populated from the PSX OUTPUT DATA. **Steps to Replicate:** 1. Send an INVITE with two History-Info headers. 2. Provision the calling party number as a target and make a call. 3. Apply a DM/PM rule for a redirecting number to add +CC before the number. 4. SBC intercepts the ingress leg by sending a "Signaling Start" message. 5. Since the History-Info header has redirecting and original called numbers, they are sent in the Signaling Start message. 6. Send Invite with two history-Info headers. 7. Provision the calling party number as a target and make a call. 8. The SBC intercepts the ingress leg by sending a "Signaling Start" message. Expected results: The LI-Last_Redirecting_Party (+CC DN) and Original_Called_Party are populated in the Signaling Start message.	The code is modified so that if any DM/PM rule is applied for Last_Redirecting_Party and Original_Called_Party in the PSX, the modified numbers are sent in a Policy response. The SBC uses the latest numbers from the PSX to populate the Signaling Start message when a call is intercepted. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134289	N/A	3	MIB files SONUS-SBX-TRAP-CNF-MIB.mib and SONUS-SBX-TRAP-MIB.mib have syntax issues **Impact:** The MIB files "SONUS-SBX-TRAP-CNF-MIB.mib" and "SONUS-SBX-TRAP-MIB.mib" are missing a space at the bottom of the files between "=" and "{". **Root Cause:** While introducing the code change for SBX-119348, the syntax error was missed. **Steps to Replicate:** In the path / opt/sonus/sbx/mib check if the files "SONUS-SBX-TRAP-CNF-MIB.mib" and "SONUS-SBX-TRAP-MIB.mib" are properly identified.	Added space between "=" and "{" so that the parser does not throw a syntax error **Workaround:** None
SBX-134372	N/A	3	Phone-context parameter position in the TEL URI of a PAI header is incorrect **Impact:** The phone-context parameter position in the TEL URI of a PAI header is incorrect. **Root Cause:** The order in which the CPC and phone context were added is reversed. **Steps to Replicate:** 1. Make a SIP-I to SIP call. 2. Enable CPC and Privacy. 3. Run a call with SIP and TEL URI. The egress side TEL URI should contain the phone-context first, followed by cpc=ordinary.	Modified the code to change the order so that the phone context is added first, followed by the CPC parameter. **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134406	SBX-134388 (12.1.2)	3	Observing MAJOR logs in *.SEC related to external authentication. **Impact:** Observing MAJOR logs in *.SEC related to external authentication. **Root Cause:** The incoming request from RAMP is identified as a DIRECT request, not a proxied(SSO) request. Consequently, as per the design, the external authentication fails, and ConfD writes the "external authentication failed" logs, which are later recorded into security logs. **Steps to Replicate:** 1. Create a new setup with RAMP. 2. Verify the *.SEC logs.	Modified the code to find the type of request and determine if it is a direct request from RAMP so that external authentication failure logs are not recorded in *.SEC logs. **Workaround:** None
SBX-134460	SBX-134281 (10.1.6)	2	SBC changes tlsProfile->cipherSuite from rsa-with-aes-128-cbc-sha to tls_ecdhe_rsa_with_aes_128_cbc_sha during an upgrade from 10.1.5R3 to 10.1.6R0 **Impact:** TLS calls dropped after an upgrade due to the default cipher change. **Root Cause:** The new default cipher was set to tls_ecdhe_rsa_with_aes_128_cbc_sha when it used to be rsa-with-aes-128-cbc-sha after the upgrade. **Steps to Replicate:** Upgrade SBC while using rsa-with-aes-128-cbc-sha cipher suite as the default choice and verify if TLS calls stay running post-upgrade.	Reverted the default cipher to rsa-with-aes-128-cbc-sha. Customers can reconfigure the three cipher options manually after the upgrade if they wish to add a more secure cipher suite. **Workaround:** Manually configure rsa-with-aes-128-cbc-sha as the cipherSuite1 in all TLS profiles for which the SBC displays rsa-with-aes-128-cbc-sha as the 1st cipher suite before the upgrade.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134547	SBX-134249 (12.1.3)	2	The SCMP cored. **Impact:** The SCMP has cored due to an attempt to dereference a NULL pointer. **Root Cause:** The code checks for a flag in a Packet Service Profile that does not exist for a call. The SBC cores when attempting to dereference a NULL pointer because the stream's PSP pointer is NULL in this call scenario. The code should be checking the flag in the peer PSP, instead of the stream's PSP. **Steps to Replicate:** This bug was found by code inspection. The exact call flow that triggered it is unknown. After the fix, Engineering will run a full regression of the code.	The code is modified to check the flag's value in the peer PSP instead of the stream's PSP. **Workaround:** There is no clean workaround. A possible workaround is to enable relayUnknownAttrsForAudioTranscodeCalls in the trunk group. This prevents the core, but will most likely cause some attributes to drop and other unexpected consequences for the call. Therefore, it is not recommended.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134558	N/A	2	SLB Deployment: OOD INFO 200 OK not relayed to the Ingress **Impact:** The SBC does not forward the 200 OK of INFO in a deployment with multiple SLBs and SBCs. **Root Cause:** The SBC logic to remove the _ck from the response is incorrect. For example, the SBC includes logic to remove the character in a tag after the first occurrence of _ck before forwarding the response. This impacted deployments where multiple instances of "_ck" are present in the response (For example, gK1ae-SID00001S-gK0ae-SID00004S-1045106SIPpTag001_cK5bfc0700_cK24a6a50f). The SBC should remove only the last "_ck" (which it would have added in the request). **Steps to Replicate:** 1. Configure a setup for UAC --> SLB1 --> SBC1--> SLB1 --> SLB2--->SBC2--->SLB2--->UAS. 2. Send an INFO message from the UAC that reaches the UAS. 3. The UAS sends a 200 Ok successfully after receiving INFO. 4. The SLB2 forwards the INFO to SLB1. Expected results: The SLB1 forwards the 200 OK to the UA.	The code is modified to remove just the last "_ck". **Workaround:** None

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134590	N/A	2	CNF: Source IP used for DNS/DS interfaces by the SG container is the same even if there are different IPs configured **Impact:** The source IP used for DNS/DS interfaces by the SG container is the same, even if different IPs are configured. **Root Cause:** The configured IPName is not associated with the configured LIG. So XRM was not aware of these IPnames and assigned the primary IP in response to the DS Module's "XMR allocate" request. **Steps to Replicate:** Configure two IPv6 names in the SG network segment table. Example results: % show system networkSegmentTable SG_PKT0 networkSegmentType SG; networkInterfaceName pkt0; prefixV6 64; ipNameV6 SGPKT0V6_01 { ipList [240b:c0e0:101:2f1e:2a38:2:11:1] ; } ipNameV6 SGPKT0V6_02	Modified the code to remove the ipName configuration from the DS since only sigPorts are configurable with non-LIF IPs (These are plumbed as "Logical addresses" to the nearest LIFs). This feature is not extended to DS/DNS because it is unavailable on VNF. **Workaround:** The following is recommended: 1. Delete the IP Name configuration from "policyServer globalConfig". 2. Delete system policyServer globalConfig ipv6Name. 3. Delete the non-LIF IP from the "Network Segment Table" (For example, delete ipName "SGPKT0V6_02" from the segment table "SG_PKT0").

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134633	SBX-134535 (10.1.x)	2	SBC 5400 - ScmP Cored **Impact:** The Peer responds to SIPREC with only one SRTP m line, causing the SBC core. **Root Cause:** The SBC expected the peer to respond 2 m lines with SRTP. The second m line was AVP and triggered SBC to access an invalid address. **Steps to Replicate:** 1. Configure SIPREC and enable SRTP. 2. Have A call B. 3. The SBC sends SIPREC to SRC with 2 m lines in SRTP. 4. The SRC responds 1st m line SRTP and the 2nd one is AVP.	The SBC is enhanced to validate the address before accessing and treating it as an SRTP m line. **Workaround:** Disable SRTP for SIPREC.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134739	SBX-132793 (11.1.3)	2	PesProcess coredumps on 9.2.3R5 and 11.1.0R1 **Impact:** PesProcess core dumps on 9.2.3R5 and 11.1.0R1 **Root Cause:** The IP Peer object is shared across multiple threads during call processing. The reference count is maintained to keep track of the object usage and is decremented after use. A call to delete can only be done if the reference count is zero, and only then does the object get destroyed. In a call flow, the reference count is not decremented at multiple places, causing it to increment for each call. When it reaches its limit, it goes to zero, and the object is destroyed even though the IP peer was not deleted. A core occurs if the IP Peer object is accessed for a subsequent call. **Steps to Replicate:** 1. Setup SBC is basic call flow. 2. Run the calls continuously, which should determine the ingress IP peer. 3. A core will occur once the ref count reaches its unsigned integer limit.	Modified the code to properly increment and decrement the reference count. **Workaround:** None. You can restart the SBC to reset the refCounter.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134792	SBX-134475 (12.1.3)	2	One of the OAM containers remained in a startingStandby state in the SBC cluster **Impact:** The serf process, which manages HA status, went down during SBC startup, causing subsequent events to not get processed and the status to remain startingActive. Serf continues processing stale messages and tries to connect to IPs that have already left the cluster. **Root Cause:** The message queue created by serf was not clearing upon the serf stop action. On a container restart, the serf processes the stale messages from the queue and tries to connect the IP that left the serf pool. **Steps to Replicate**: The probability of replicating this issue is unlikely. 1. Try deleting a pod from the HA setup to free up the IP address. a. Note that it will still be present in another pod's serf configuration. b. If another pod from a different deployment picks up this free IP address, it may result in an unusual cluster formation between the two deployments. 2. If the pod or container is restarted while/before processing event messages from the message queue, the serf reads stale messages. a. View the serf logs to verify.	The code is modified to clear the message queue when the serf is stopped, ensuring that the IP is removed from the pool when a member leaves or fails. Stale messages are also removed from the serf queue. **Workaround:** Restart the container or delete pods to restore the correct states.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134853	SBX-134471 (12.1.3)	2	Policy server status is down between SBC Staging-1 deployment and PSX-Replicas (deployed in Staging-1 and Staging-2 clusters) **Impact:** The policy server status went to "down" when the start UDP media range changed from 1024 to 10000. **Root Cause:** The DS still uses the previously configured UDP media port as the source port, even when the base port range is changed. The system does not recognize the new port, and the old port is no longer configured. **Steps to Replicate:** 1. Open the IP interfaces. 2. Update the UDP base media port from 1024 to 10000. 3. Enable the IP interfaces.	Modified the DS to release the acquired port and use the value of the new UDP media port range. **Workaround:** N/A

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-134876	SBX-134287 (10.1.6)		If the dnsGroup is configured in a certain order, the SBC will not do DNS lookups. **Impact:** The DNS request is not sent to a configured DNS server when the DNS server is configured before configuring an Interface for Dnsgroup. **Root Cause:** When a server is created initially without a Dnsgroup interface, the DNS server IP address is not added to /etc/resolv.conf file which is required for DNS Request to be sent to DNS server. **Steps to Replicate:** Configure the SBC in the following order (configure the DNS server, commit, and then the interface for the DNS Group:	Updated code to add the DNS server IP when configuring the DNS server and then the interface for a DNS Group. **Workaround:** Bounce the DNS server state.

Issue ID	Original Issue	Sev	Problem Description	Resolution
			set addressContext default dnsGroup DNS_GROUP_DEFAULT server DNS1 state enabled recursionDesired true ipAddress 10.54.80.240 transportProtocol udp tcpFallback disabled priority 0 weight 0 recordOrder priority dscpValue 0 commit set oam snmp users user authKey f7:ce:f2:11:c8:a3:6d:af:79:5c:84:61:47:73:44:51:d5:d5:cc:6f privKey f7:ce:f2:11:c8:a3:6d:af:79:5c:84:61:47:73:44:51 authProtocol hmacsha group admin privProtocol aes128 commit set oam snmp trapTarget MEMS_FED fqdn mems-snmp.pro.ringcentralgov.com port 162 targetSecurityLevel authPriv targetUsername user trapType v3 state enabled commit set addressContext default dnsGroup DNS_GROUP_DEFAULT type mgmt transport udp interface mgmtGroup useConfiguredDnsServer enabled ednsSupport disabled rcodeErrorMonitorTimer 0 negativeDnsCacheSupport enabled negativeDnsCacheTimer 60 dnslookupTimeoutTimer 10 commit Without the fix: A tshark from SBC to DNS server shows the SBC is not sending a DNS request (tshark -n -i any -f"host 10.54.80.240" -t ad)	

Issue ID	Original Issue	Sev	Problem Description	Resolution
			With the fix: A tshark from SBC to DNS server shows the SBC sends a DNS request (tshark -n -i any -f"host 10.54.80.240" -t ad)	
SBX-134894	N/A	2	SBC may behave unexpectedly after an upgrade to 12.1.2R0 (or higher) **Impact:** For SBCs upgraded to 12.1.2R0 (or higher), the /run filesystem becomes full and causes abnormal behavior. **Root Cause:** When adding the 'nodev' option to run mount during the upgrade, the /etc/fstab is updated with a hardcoded size, which differs from a freshly installed SBC, causing the space issue. Also, during bootup, a change to the persistent volume / home was done before properly mounting it causing the applications to flood the /run partition. **Steps to Replicate:** 1. Perform an upgrade from any version to 12.1.4 (fix version). 2. After the SBC comes up, check df -h and verify the space allocated for /run. 3. Cross-check the value with a freshly installed 12.1.4 instance.	Modified the code by updating the /etc/fstab to take the default size set by Debian during installations and upgrades. Created an override configuration for systemd-journal-flush.service to set mount points as dependencies. **Workaround:** Manually modify / etc/fstab and remount. 1. sed -i '/^tmpfs \/run tmpfs/ s/,size=[0-9]*k//' /etc/fstab 2. mount -o remount,rw,nosuid,nodev,relatime,mode=755 /run

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-135161	SBX-134553 (11.1.3)	2	The SBC may return two different SIP cause codes (404 and 503) when all PSXs are unavailable or unreachable while only the 503 SIP cause code is appropriate. **Notes Root Cause:** The SBC throttles the sending of the "NO_SOFTSWITCH_AVAILABLE" logging event between internal subsystems to avoid excessive logging. The SIP 503 cause code was generated only for calls for which the event was not throttled. **Steps to Replicate:** 1. Configure an SBC to use an external PSX. Make sure that the PSX status shows as "active". 2. Simulate a network failure, for example by bringing down all mgt interfaces on the active node. If the link detection is configured, disable it to avoid a switchover. 3. All calls shall now fail with a SIP 503 cause code, the SIP 404 code shall not be present at all.	A code fix was added to correctly set the call disconnect cause, irrespective of whether the logging event was throttled or not. **Workaround:** None

Resolved Issues in 12.01.03R002 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134966	N/A	1	In 12.01.03R000, a new field was added to the STOP record at the end (field #301) to record the 'Minimum Recording Sessions' value. This was added as part of feature SBX-127000 / SBX-131075 added in V12.01.03R000. If your billing mediation system has an issue with this field, then this build is available with just the single change that will only include this data if you configure via CLI to include this in the STOP record. **Impact:** The STOP record may get rejected or errors logged from the Billing mediation server if an exception hits due to this additional unexpected field. **Root Cause:** A new field, added to the CDR record (STOP # 301) without incrementing the CAM VERSION, dropped records by some billing mediation platforms. **Steps to Replicate:** Review the STOP record for inclusion of field # 301 based on current accounting settings.	The issue is fixed by putting the logging of this parameter inside a wrapper that will check if cdrPatch is >= 1. This is set via CLI command. Refer to New in SBC 12.01.03R002 for additional information. **Workaround:** N/A

Resolved Issues in 12.01.03R001 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134400	SBX-133734 (10.1.6)	1	After a switchover, call hold/ unhold fails since the SBC is not able to send any in-dialog SIP messages to the registered endpoint. This break happened between 10.1.4R3 and 10.1.5R1 **Impact:** After a switchover, call hold/unhold fails since the SBC is not able to send any in-dialog SIP messages to the registered endpoint. A refresh register routine then occurs, and the SBC may allocate a new port after the switchover. **Root Cause:** Call Control Block (CCBPTR) was not updated with the correct values from the updated RCB. **Steps to Replicate:** This issue is easiest to replicate when the endpoints use TCP and TLS transports. Do the following in an HA-Pair: 1. Register an endpoint from the IP/Port. 2. Initiate a basic call from the endpoint. 3. After the switchover, the endpoint should re-register from a different IP/port (other than earlier). 4. The registrar endpoint will send a SIP Notify and then Re-INVITE from the UAS to the endpoint. 5. The SBC will send the a Re-INVITE message to the new destination port .	Modified the code to update the IP/Port for the new Connection from the Address of Record (AOR) block to the Call Control Block. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134152	SBX-133608 (12.1.4)	1	SBC services do not come up after enabling FIPS mode. **Impact:** The SBC services were not coming up after enabling FIPS mode. Users received a "libcrypto does not support 'sha-512'" error message. **Root Cause:** As part of the confd upgrade, some setcaps were added to confd-related binaries, which work in non-FIPS mode, but give the above error in FIPS mode. **Steps to Replicate:** 1. Open the latest build. 2. Perform a FIPS configuration. 3. After enabling FIPS, SBC services should come up fine.	The code is modified to fix this issue. **Workaround:** N/A
SBX-134193	N/A	1	CNF: Not able to resolve FQDN for IPPEER post-upgrade from 12.1.2-R001 to 12.1.3-123 build **Impact:** IPPEER FQDN resolution started failing after a couple of hours when running at 10 cps. **Root Cause:** The SBC DNS Client internally Toggle's sockets every 100 minutes, at which time a new socket with a different source port gets created. This is used to send DNS queries. When toggling, the socket fails, and thus the DNS queries fail. **Steps to Replicate:** 1. Create a DNS group. 2. Run a call with 10 cps call continuously for more than three hours. The expected result is that the call continues after three hours, but the actual result is that the calls are running continuously after three hours.	Updated the code to toggle sockets so that a new socket gets created properly after 100 minutes. **Workaround:** Delete and recreate the DNS group.

The following severity 2-3 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132165	N/A	2	Enabling FIPS on 12.1.1Rx SBC makes it impossible to log in to the EMA. **Impact:** After enabling FIPS mode and adding certificates for the EMA, logging into the EMA Web GUI fails and gives a 'Service Unavailable' error message. **Root Cause:** In SBC release 12.1.1 onwards, the hostkey ssh-rsa is disabled in FIPS mode. The EMA uses the ganymed-ssh2 library to connect to the backend through NETCONF, and version 263 of this library wasn't supporting non-rsa hostkeys resulting in the issue. **Steps to Replicate:** 1. Enable FIPS mode from the CLI or EMA. 2. After a reboot, add apache2 certificates for EMA to come up. 3. Log in to the EMA. The login fails giving a 'Service Unavailable' error message.	The ganymed-ssh2 library version was updated to 264, which support ECDSA hostkeys for SSH. The EMA is now able to connect to the backend and work as expected. **Workaround:** Manually enable the ssh-rsa as hostkey algorithm in /etc/ssh/sshd_config_2022 and do a service ssh-netconf restart.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134249	N/A	2	The SCMP cored. **Impact:** The SCMP has cored due to an attempt to dereference a NULL pointer. **Root Cause:** The code is checks for a flag in a Packet Service Profile that does not exist for a call. The SBC cores when attempting to dereference a NULL pointer because the stream's PSP pointer is NULL in this call scenario. The code should be checking the flag in the peer PSP, instead of the stream's PSP. **Steps to Replicate:** This bug was found by code inspection. We are not sure the exact call flow that triggered it. SVT will run full regression on the code with the fix.	The code is modified to check the flag's value in the peer PSP instead of the stream's PSP. **Workaround:** There is no clean workaround. A possible workaround would be to enable relayUnknownAttrsForAudioTranscodeCalls in the trunk group. This would prevent the core, but will most likely cause some attributes to be dropped and other unexpected consequences for the call. Therefore, it is not recommended. The best solution is to upgrade to a version with this fix.
SBX-134728	SBX-130861 (12.1.4)	2	SBC fails to connect to the CDR server over SSH with non-RSA keys **Impact:** The SBC is not able to use the CDR server with non-RSA keys, and the SBC is accepting the keys that it doesn't support. **Root Cause:** The libssh package needs updating, and there is no proper validation for the acceptance of the keys. **Steps to Replicate:** Request oam accounting cdrServer admin primary loadPrivateKeyFile fileName dsa	Updated the libssh package to add support for ssh-ed25519, ecdsa-sha2-nistp521, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp256 keys. Proper validation of keys is available, allowing the SBC to reject the key it does not support. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134654	N/A	2	SBC CNF: Sequence Numbers are appended as a suffix to the ACT record file, creating an issue in the CDR billing server. **Impact:** The global sequenceNumber for an ACT filename was causing issues. **Root Cause:** The global sequenceNumber for ACT filename was improperly coded. **Steps to Replicate:** 1. Configure a cdrServer 2. Perform a rollover on ACT files	Moved the global sequenceNnumber from the end of the filename to before the pod-specific sequenceNumber. **Workaround:** N/A
SBX-134219	N/A	2	The SBC CNF has a defined Ephemeral Storage Request/ Limit, and a SizeLimit for EmptyDir volumes. **Impact:** Few containers in SBC CNF deployments don't have an ephemeral storage request/limit set, nor a set EmptyDir sizeLimit. **Root Cause:** If the ephemeral-storage request/limit or the EmptyDir sizeLimit is not configured with a value, the local disk usage is unlimited and the application will consume more space from the local disk. The local disk attached to the worker node will then misbehave, resulting in the worker node evicting the pods from that node. **Steps to Replicate:** Deploy the SBC CNF solution and check the ephemeral-storage request/limit for each container, and also check the EmptyDir sizeLimit by executing "kubectl describe pod <pod_name>".	The code is modified to set the ephemeral-storage request/limit and EmptyDir sizeLimit to a valid value applicable for that container/pod. **Workaround:** Since the changes are in Helm charts, the ephemeral-storage request/limit and EmptyDir sizeLimit can be updated manually in the Helm charts that are used in customer deployment.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127302	N/A	3	SwitchOver after closing SSH putty window using CTRL-C **Impact:** If a confd session gets killed abruptly using ctrl-c, while running 'show configuration' or 'show status' commands with a large amount of data, the SBC application is going for restart. **Root Cause:** A Cpx process is intentionally aborted before confd completes a "Got error callback on non existing user session fd#" error. **Steps to Replicate:** 1. Configure the SBC with some of the ERE related configurations. 2. Run show configuration from the CLI. 3. Kill the user session being associated with CLI, while the command is being process by confd.	Downgraded confd to 7.3.2 version where this issue is not present. **Workaround**: Do not forcefully kill CLI sessions while data is being fetched from DB.
SBX-134471	N/A	2	Policy server status is down between SBC Staging-1 deployment and PSX-Replicas (deployed in Staging-1 and Staging-2 clusters) **Impact:** The policy server status went down when the start UDP media range is changed from 1024 to 10000. **Root Cause:** The DS still holds on to the previously configured UDP media port as the source port even when the base port range is changed. The system does not recognize the new port, and the old port is no longer configured. **Steps to Replicate:** 1. Open the IP interfaces. 2. Update the UDP base media port from 1024 to 10000. 3. Enable the IP interfaces.	Modified the DS to release the acquired port and use the value of the new UDP media port range. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134475	N/A	2	One of the OAM containers remained in a startingStandby state in the SBC Staging-2 Cluster **Impact:** The serf process which manages HA status went down during SBC startup causing subsequent events to not get processed and status to remain startingActive. Serf continues processing stale messages, and tries to connect to IPs which have already left the cluster. **Root Cause:** The message queue created by serf was not being cleared on the serf stop. On container restart, serf processes the stale messages from the queue and tries to connect the IP that left the serf pool causing the issue with serf. **Steps to Replicate**: The probability of replicating this issue is unlikely. 1. Try deleting a pod from the HA setup to free up the IP address. a. Note that it will still be present in another pod's serf configuration. b. If another pod from a different deployment picks up this free IP address, it may result in an unusual cluster formation between the two deployments. 2. If the pod or container is restarted while/before processing event messages from the message queue, the serf reads stale messages. a. View the serf logs to verify.	The code is modified to clear the message queue when the serf is stopped, making sure the IP is removed from the pool when a member leave or a member fail is called. Stale messages are also removing them from serf queue. **Workaround:** Restarting container or deleting pods will restore the correct states.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134559	N/A	2	The OAM application status is displayed as startingActive in SBC Staging-2 **Impact:** The OAM status continuously as startingActive after doing dockerstop/ dockerstart from the Connexip sHelml. **Root Cause:** The serf process that manages HA status fails during an sbx startup, causing subsequent events to not process correctly and the status remains as startingActive. **Steps to Replicate:** 1. Install SBC CNe. 2. Open the OAM pods. 3. Check sbxstatus/swinfo	The serf message-queue was modified to ensure that the serf start process correctly generates the queue, and is deleted when serf stops as part of dockerstop. **Workaround:** Restart the container or delete the pod to restore the correct states.
SBX-132330	N/A	2	IPsec functionality is not working on a CNF non-root setup. **Impact:** IPsec functionality is not working on CNF non-root setup. **Root Cause:** The PF Key interface between the application and the kernel needs root permission. **Steps to Replicate:** Run IPsec as non-root.	The PF Key interface between an application and a kernel has been replaced with a Netlink interface. The netlink interface works even in a non-root setup. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134761	SBX-133684 (12.1.4)	3	SBC CNF (12.1): CSAR creates Python scripts that produce incorrect TOSCA.meta file contents. **Impact:** The CNF CSAR creates Python scripts that produce incorrect TOSCA.meta file contents. **Root Cause:** The TOSCA.meta file contents were incorrect due to a logical error while populating the images and scripts paths, due to typos in "Created-By" and "Entry-Scripts" entries. **Steps to Replicate:** Generate CSAR, and check the TOSCA.meta file contents.	Corrected the logical error for populating images and scripts path, and corrected the typos in the "Created-By" and "Entry-Scripts" entries. **Workaround:** N/A
SBX-134759	SBX-134083 (12.1.4)	3	SBC CNF (12.1.2): CSAR creates Python scripts that generate incorrect image paths in the TOSCA.meta files. **Impact:** CNF CSAR creates Python scripts that generates incorrect images paths in the TOSCA.meta files. **Root Cause:** The image path given while generating TOSCA.meta files was inserted one directory level above the actual path. **Steps to Replicate:** Run the CSAR script, and check the image path in TOSCA.meta file.	Fixed the code by providing the correct image path when generating TOSCA.meta file. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134760	SBX-133832 (12.1.4)	3	SBC CNF (12.1): CSAR creates Python scripts that fail when running the Cluster Readiness Checker tool. **Impact:** CSAR creates Python scripts that fail when running the Cluster Readiness Checker tool. **Root Cause:** An array that was defined to hold the Helm chart name was instead hardcoded to only accommodate the SBC Core Helm chart name. **Steps to Replicate:** Validate for SBC Helm charts, and validate for cluster-readiness charts.	The code is modified to allow flexibility in the SBC Core Helm chart name. **Workaround:** N/A

Resolved Issues in 12.01.03R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132182	N/A	1	[CNF_NONROOT] Stats are not getting generated on "RunAsAnyUser" **Impact:** Statistics are not getting generated in the /home/sftproot/evlog/statistics directory when the security context is set as "RunAsAnyUser" even though the configurations are enabled in fileStatisticAdmin to generate the performance statistics, **Root Cause:** The Ustar archiving format has a limited range for User IDs (UID) and Group IDs (GID). When the system was run with a larger GID, it ultimately failed to create the tar file containing the data. **Steps to Replicate:** With the security context set to "RunAsAnyUser," enable the fileStatisticAdmin configurations to generate performance statistics and check for stat files in the /home/sftproot/evlog/statistics directory.	To resolve the issue with UID restrictions, the code is modified to change the archive formatting from Ustar to pax (restricted). This adjustment ensures that the system can handle larger UIDs and GIDs without failing to create the tar file. **Workaround:** None
SBX-132195	N/A	1	[CNF_NONROOT] PKT IPs are not getting plumbed to the SC Active Pod with "runAsAnyUser" **Impact:** When the setup is configured with Basic call Configs, the SC's PKT IPs are not getting assigned to the SC pod. **Root Cause:** The NS pod that assigns IPs to the SC pods is unable to access the NSAT JSON files and the shared config XML files due to: `Permission denied: '/mnt/gfsvol1/1.xml'` **Steps to Replicate:** Configure the SBC with call configuration and check the IP assigned to SC pods by running 'ifconfig' on respective pods.	Corrected the read+write permission so that the NS can access these file groups when once they are created. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132675	SBX-132269 (11.1.1)	1	Performance: Observing "0xFFFFFFFF-SipFeRcbUpdateMicroFlowForStableRegTimer' MAJOR Logs while running IMS-AKA Reg with Multiple AORs. **Impact:** Observing "0xFFFFFFFF-SipFeRcbUpdateMicroFlowForStableRegTimer' MAJOR Logs while running IMS-AKA Reg with Multiple AORs. **Root Cause**: The log level for this particular log was set as Major instead of Debug. **Steps to Replicate**: Run IMS-AKA Registrations with Multiple AORs.	Modified the code so that these MAJOR logs for multiple AORs are reported as INFO. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132973	N/A	1	Observing PfeApp coredump while triggering automation during restore revision **Impact:** When the OAM issues a configuration rollback revision, the PfeApp restarts continuously instead of deleting existing configurations and restoring PDP to specific required configurations, leading to a core dump. Hence, it fails to restore PDP to previous required configurations. **Root Cause:** 1. When the PfeApp receives a restore revision request from OAM, it deletes all current configurations, goes for restart and checks if PDP is pristine. 2. If PDP is pristine, the PfeApp configures it with specific configurations. Otherwise, it causes PDP to restart and come up fresh. At this point, if the PDP contains previously configured configurations, it should reply to PfeApp as "Not pristine." But instead, the PDP replies with "pristine." Thus, when PfeApp tries to configure the PDP, it replies that duplicate configurations are supplied and PfeApp issues a core dump. This all happened because the PDP was implemented earlier to only reply "not pristine" if and only if the interface was created. If not, it was programmed to reply "pristine." **Steps to Replicate:** Issue a rollback command from OAM. Expected: 1. PfeApp deletes all existing configurations then goes for restart.	The PDP is updated to check if any resources are present (interface, IP address, flow table and forward table). • If yes, it now replies to the PfeApp with "not pristine". • If no resources are created, it replies back with "pristine." **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. After PfeApp comes up, it sends a "Helmlo request to PDP asking whether PDP is pristine. PDP should reply as "pristine" if there are no configurations. Otherwise, it should reply "not pristine". 3. If the PDP is "not pristine", the PfeApp should trigger a PDP container restart. 4. After the PDP freshly comes up, the PfeApp configures the PDP with specific restore revision configurations.	
SBX-133168	N/A	1	[ASAN] [11.1.1R7] LeakSanitizer: detected memory leaks in CpxAppProc /src/confd_internal.c **Impact:** A memory leak exists in CpxAppProc. **Root Cause:** The structure was not getting freed after it was called. **Steps to Replicate:** Run a show command on a table to display the values. Example: > `show table oam localAuth userStatus`	Removed the structure since it was not required. **Workaround:** None
SBX-133520	N/A	1	Non-OAM confd pods were stuck on an old configuration revision **Impact:** Non-OAM confd pods were stuck on an old configuration revision. **Root Cause:** In some conditions, managed confd pods were not restarting to restore the new configuration. **Steps to Replicate:** 1. Perform an upgrade and rollback. 2. Restore a configuration of an older software release.	The code is modified to cause the managed confd pods to auto-reboot when they detect the managing pod performing a restore of a new configuration revision and a reboot request. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133694	N/A	1	Enhancement required in artifacts.json file to remove PRSM related configuration and to have a default configuration to download and tar all images in CSAR **Impact:** The artifacts.json sample configuration file that generates the CNF CSAR needs updating to remove the PRSM-related configuration and include a default configuration to download and tar all the images in the CSAR. **Root Cause:** The CNF CSAR was initially included as a reference that same CSAR script could be used for packaging PRSM images and associated Helm charts. The artifacts.json file was a sample file for the user to edit it and include all the image names that are required for the customer's deployment. **Steps to Replicate:** Verify that CSAR generated with default artifacts.json config file contain all images required for the SBC deployment and does not contain additional unnecessary images and files.	Updated the artifacts.json sample configuration file to remove PRSM images and add all default image names that are required for the SBC cluster deployment. **Workaround:** N/A
SBX-133753	N/A	1	[CNF-CSAR] Empty image tar files are getting created when image download fails in 12.1.2-R00-310 **Impact:** Empty image tar files are getting created in CNF CSAR when docker image download fails. **Root Cause:** Handling for docker image download failure was not implemented. **Steps to Replicate:** Test download failures with wrong credentials, invalid image path and tag.	The code is modified to include the handling of docker image download failures. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133782	N/A	1	[CNF]: NS Pod do not go for a restart on new config from RAMP **Impact:** In the SBC CNe, the NS container does not restart with the latest configuration when the RAMP issues a Connection Restore operation (i.e., when the RAMPDownloadConfig flag is toggled). **Root Cause:** The RAMP's Connection Restore scenario (resulting in the downloading of a new configuration from RAMP) was not implemented in the NS. **Steps to Replicate:** In a non-PFE SBC CNe deployment, when the RAMPDownloadConfig flag is toggled from RAMP, other containers of the SBC CNe (that make use of the RAMP/OAM configuration) perform a restart, but the NS container does not, resulting in the NS retaining the old configuration.	Added support of the Connection Restore operation to the NS. **Workaround:** None

The following severity 2-4 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128919	N/A	2	Failed to verify that the SBC sends OOD NOTIFY for 100 Trying for Monitoring CUCM User and PSTN User **Impact:** After a Refer msg, the SBC sends INVITE with the same number in the To and From header resulting in the NOTIFY validation failure. **Root Cause:** Changes were added to a different feature that is supposed to add Redirecting Original Number and Redirecting only when the feature flag is enabled that affects the To and From header of the INVITE after a REFER, it includes them for all the REFER cases. **Steps to Replicate:** 1. Subscribe the designated APP to WebRTC Gateway and initiate a call to PSTN User-B and answer the call on PSTN User-B 2. a. Intitiate a transfer call to Cisco User-A using the designated APP/ REST API b. The SBC sends a refer for Cisco User-A 3. Send OOD Refer from Kandy Link having Refer-To header with method = BYE, valid Target-Dialog header and Request-URI points to SBC for Call Termination of PSTN User-B before answering the call on Cisco User-A 4. Ensure Call Notifications from SBC sent to WebRTC Gateway 5. Save the CDR file and verify the parameters	Modified the code to only include Redirecting Info and Original Called Number when the control is enabled. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129085	N/A	2	Modify sbcDiagnostics to enable root access when a valid list is present **Impact:** On the public cloud, where the SBC is not able to start up, the root can not be enabled because a license has not been installed. **Root Cause:** The ability to enable the root user is not available **Steps to Replicate:** 1. Bring up a cloud SBC. 2. Install a license. 3. Log in as root. 4. Run the following commands: `gbin` `mv CpxAppProc CpaAppProc.save` 5. Copy a valid node locked license to /opt/sonus/external 6. Use the licenseFileTool delete function to delete the installed license 7. Run `sbxrestart` 8. Log off the SBC. 9. Run `sbcDiagnostic.sh -e <license name>` 10. Verify that you can logon on as root.	With this modification, if there is a valid node locked license matching the host, then root will be enabled, even if the SBC is not up. **Workaround:** None
SBX-129211	N/A	2	SonarQube Vulnerability: common/platformservices/cryptography/src/PsCryptography.cpp **Impact:** SonarQube vulnerability in CPP file PsCryptography.cpp **Root Cause:** SonarQube issue in PsCryptography.cpp use a stronger cipher algorithm **Steps to Replicate:** SonarQube scan must not report the weak algorithm vulnerability in PsCryptography.cpp	Updating PsCrypt to use EVP_aes_128_gcm instead of EVP_des_cbc **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130848	N/A	2	CS SWO: Deviation in unpermitted-list behavior using retryAfterMethod **Impact:** There is a deviation in the unpermitted-listing behavior when using the blkListAlgRetryAfterMethods configuration. In the defined test cases, specific SIP methods were expected to be unpermitted-list and rejected with a 503 response. However, after performing a CS SWO, only some methods were rejected, indicating an inconsistency in the unpermitted-listing functionality across cases. **Root Cause:** The unpermitted-listing mechanism for retry After SIP methods was inconsistent after performing a CS SWO. The unpermitted-list entry persisted across CS, RS, and SC, but the rejection behavior did not align with the configuration post-SWO. **Steps to Replicate:** 1. Configure blkListAlgRetryAfterMethods to include sip-publish, sip-message, and sip-info. 2. Send PUBLISH, MESSAGE, and INFO requests from the same endpoint. 3. Confirm that all methods are rejected with a 503 response. 4. Perform a CS SWO. 5. Send the same requests (PUBLISH, MESSAGE, and INFO) from the same endpoint. 6. Verify that all methods are still rejected according to the unpermitted-list configuration	The issue was resolved by modifying the ArsSendBlklistEvtToCs function to properly pass the blkListMethod argument. This ensures that the correct unpermitted-list methods are enforced consistently after a CS SWO. **Workaround:** No known workaround is currently available for this issue at the moment. The problem is resolved by applying the fix.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131144	N/A	3	The PAI/FROM URI userpart is truncated at the first instance of the letter **Impact:** The userpart of the FROM header URI is truncated at the first instance of the letter in an outgoing INVITE message **Root Cause:** When an incoming INVITE message is processed, the userpart of the FROM URI is truncated based on E.164 while saving the calling party URI and Calling party number. **Steps to Replicate:** 1. Make a Basic A - SBC-B call setup 2. Set numberGlobalizationProfile on both legs. `set profiles signaling ipSignalingProfile <IPSP_name> egressIpAttributes numberGlobalizationProfile DEFAULT_IP` 3. Set privacy to PAI at the egress leg. `set profiles signaling ipSignalingProfile <egress_IPSP> egressIpAttributes privacy privacyInformation pAssertedId` 4. Make a Basic A to B call. 5. Send the following URI in the FROM header in the incoming INVITE:	A new function is introduced which validates Userpart of FROM header URI. It validates: • If the Userpart is in E164 format and • The length of the Userpart. If the Userpart is in E164 format and length is maximum of 31 characters (after stripping off delimiters and visual characters), then the Userpart is considered in Calling Party Number, otherwise it is considered in Calling Party URI. **Workaround:** Transparency profile for FROM header

Issue Id	Original Issue	Sev	Problem Description	Resolution
			`Incoming INVITE:` `From: sipp` `<sip:198e3e18-4e57-4ae4-8c3d-b4e098975471@test.com>;tag=2811366SIPpTag001` 6. FROM header Userpart is truncated, and so is the PAI ad Contact header. `From: "sipp" <sip:+198@10.52.20.10>;tag=gK0000018b` `P-Asserted-Identity: "sipp" <sip:+198@10.52.20.10:5060;user=phone>`	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131271	N/A	3	CLI login error banner after upgrade to 11.01.01R00 **Impact:** Nonessential message is displayed to the user **Root Cause:** Case 1 : Failure status of a command (script) being displayed from pam module. Case 2 : Lack of permission to change to home directory for a user. **Steps to Replicate:** Case 1 : Step 1 : Enable both localAuthentication and externalAuthentication. Step 2 : Login as a local user. Expected result : No error message as seen this the description is displayed to the user. Case 2 : Step 1 : Enable externalAuthentication. Step 2 : Configure an externalAuthentication server. Step 3 : Login as external user. Expected result: On successful login , the banner message as seen in the Jira description is not seen.	Case 1 : Added a quiet utility provided by pam to suppress the exit status of a command (script). Case 2 : Provided the user with a home directory with appropriate permission to change directory. **Workaround:** N/A
SBX-131469	SBX-110555	2	Observing PrsProcess memory leak while running 300 CPS 30K calls in PFE setup **Impact:** Prs process memleak was being reported in call load. **Root Cause:** Since the RTM_FBS message type was not handled in MRM, ICM free was not happening, leading to this memleak. **Steps to Replicate:** Run the call load and monitor memory utilization graph	RTM_FBS message type are added in MRM ActiveMsgProcessing **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131685	N/A	2	SIPREC Metadata, 27th parameter of 4 => RECORDING (SRS3 - Egress) is not present in CDR File , whereas present in remaining RECORDINGS **Impact:** SIPREC Metadata(27th Parameter) is not updated in CDR if a SIPREC Recording fails to create a recording session for first available SRS. **Root Cause:** SipRec metaData information was not maintained for retry scenario where initial recording fails and SIPREC session is tried with next available SRS. **Steps to Replicate:** 1. Configure the SBC to handle all type of calls. 2. Configure three SRS Group Profile table (PSX) with: • SRSGRP1 - FQDNA IPV4,TLS,SRTP SRV Query • SRSGRP2 - FQDNB IPV4,TLS,SRTP A Query • SRSGRP3 - FQDNC IPV4,TLS,SRTP AAAA Query	Initial SIPRecording session may fail in case of SRS not available or SRS FQDN DNS query fail etc. In this scenario SBC tries to connect with the next available SRS where SIPREC MetaData info was not maintained for later Sessions However we may not Observe the Missing of data if call is refreshed with a RE-INVITE. Code is updated to Maintain SIPREC MetaData for SIP Recording retry scenarios. **Workaround:** NA

Issue Id	Original Issue	Sev	Problem Description	Resolution
			• SRSGRP4 - FQDND IPV6,TLS,SRTP A Query 3. Configure the SRS SRS Group Cluster Profile table (PSX) and attach all four SRS Group Profiles to it. Also configure Call Recording Criteria table (PSX). 4. Configure Siprec Metadata profile as below in SBC: `set profiles services sipRecMetadataProfile PROFILE version 1` `set profiles services sipRecMetadataProfile PROFILE sipHeader request-uri sipToXmlTagName gRequesturi` `set profiles services sipRecMetadataProfile PROFILE state enabled` `set addressContext default zone $SiprecIngZone sipTrunkGroup $SiprecIngTG services sipRecMetadataProfile PROFILE` 4. Enable siprec Recording CDR as below in the SBC: `set oam accounting admin generateSipRecordingCdr enabled`	

Issue Id	Original Issue	Sev	Problem Description	Resolution
			5. Configure packet capture for SIPREC. Procedure: 1. Make an A to B call using the external PSX. 2. The DNS A query will fail initially for the third recording and the SIPREC session will be connected for AAAA query for the same FQDN. 3. After SIPREC all four sessions established UAC sent BYE.	
SBX-132104	N/A	2	Calls with 60K PDUs are failing **Impact:** Calls failed when the SBC received a SIP call request had a packet size equal to 60kb. **Root Cause:** The connection manager buffer size was overshooting the max allowed limit that caused the packet drop instead of processing it. **Steps to Replicate:** From the UAC, send a SIP INVITE with a total size of packet equal to 60kb.	The connection manager buffer size limit was increased to next level so that it can accept a 60kb packet and process it successfully. **Workaround:** none
SBX-132143	N/A	2	A top2 core dump occurred on the system **Impact:** A core dump issue was reported on the Active node, specifically related to the top2 utility. **Root Cause:** Investigation revealed that the top2 core dump occurred shortly after the sbxPerf service was initiated. Sysdump logs confirmed that sbxPerf was not running or stopping correctly, with improper handling of the sbxPerf service's start/stop process via logrotate directly causing the core dump. **Steps to Replicate:** Install a fix build and run the command `systemctl status sbxPerf` and then determine if sbxPerf is active.	Changes were made to resolve log compression failures in the sbxPerf logrotate configuration. The configuration was also updated to use systemctl for managing the start/stop process, improving reliability. Additionally, the sbxPerf script was modified to generate individual logs for each execution. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132216	SBX-131729 (10.1.5)	3	SBC import failed on M-SBC due to congestion configuration **Impact:** The config import on the congestion container was failing due to the mode field in levelMC container when set to inService. Operators must make the mode before applying configs to levelMC containers. **Root Cause:** The mode field within levelMC containers was set to inService in the exported data. **Steps to Replicate:** 1. Configure levelMC containers with mode inService and export the configurations. 2. Run clearDB for clearing the configs and then try importing the configurations.	The on-node extension handler is added at the level MC containers to make the mode to outOfService before applying configs and then bring back to inService later. The backend code changes are done for handling the case. **Workaround:** Not Applicable

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132379	N/A	3	The SBC accepts and relays PAI headers with an invalid SIP syntax. **Impact:** The SBC accepts and relays PAI headers with an invalid SIP syntax **Root Cause:** The SBC parser accepts user=phone as a header parameter and processes it. **Steps to Replicate:** 1. Set up a basic SIP-SIP call with PAI transparency. 2. Run the call and determine if the SBC accepts the INVITE with PAI header and relays it to the egress side even the URI parameter (user=phone) comes outside of the angular bracket. 3. When fixed, the SBC should return 400 Bad Request for PAI header, where user=phone comes outside of angular bracket. 4. Check with different combination of PAI headers where user=phone is used inside and outside of angular bracket.	Code changes are updated as per ABNF for PAI header. **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132385	N/A	3	The SMM is not able to use a CR LF in a string to replace the matched regexp string in EMA. (CLI does not have this issue.) **Impact:** In EMA when and \r are entered they get stored as \ and \\r **Root Cause: "**\n" was treated as two separate characters ("\" and n") instead of a single chracter "\n". Similarly "\r" was treated as two separate characters instead of one. Due to this, "\" gets escaped with another "\" and gets stored as "\\n" and "\\r". **Steps to Replicate:** 1. Login to EMA 2. Create a SMM with \n and \r. It should get stored as it is in CDB	Code changes have been made to consider and \r as a single character using its ASCII value **Workaround:** No workaround

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132499	N/A	3	An SmPr core occurred on Standby node **Impact:** A Segmentation fault in SmProcess when processing a request for CPU statistics for a CPU number which is higher than the max number of CPUs on the system. **Root Cause:** The system fails because the operator uses an out-of-range array index to access an array. Each array entry contains data for a single cpu. The cpu number is used as the array index. If the cpu number is larger than the number of array entries, the SBC attempts to access invalid memory which will result in a Segmentation Fault. The code does already have a range check – but the check is incorrect because it doesn’t account for the fact that operators access the array with a 0-based index. **Steps to Replicate:** This issue is not reproducible because in most cases the system finds a 0 in the array entry (even when the array index). This was a rare case in which operators found a non-zero value which resulted in a Segmentation Fault.	The fix is to correct the range check. **Workaround:** Do not't request CPU statistics for with a CPU number that is larger than the number of CPUs on the system.
SBX-132621	N/A	2	DBM Logging observed on VNF **Impact:** DBM Logging observed on VNF **Root Cause:** No presence of DBM_PATHCHK thread in the non-CNF environment and the system continually attempts to send ICM message to it. **Steps to Replicate:**	Restrict sending messages to DBM_PATHCHK thread in non-cnf environment. **Workaround:**

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132628	SBX-132338 (10.1.6)	2	The SBC handles double quotes in the PANI header incorrectly **Impact:** The SBC sends a syntax error in P-Access-Network-Info(PANI) header. Also, if transparency PANI header is enabled in the outgoing profile the SBC sends duplicate PANI headers. **Root Cause:** When SBC received PANI header with parameter operator-specific-GI value within double quote string, it did not strip off double quote characters for CAI. **Steps to Replicate:** 1. Configure JJ9030 feature. 2. Incoming has PANI and operator-specific-GI value is within the double quote string. 3. The SBC sends an Invite with PANI and syntax error for operator-specific-GI value	The SBC removes double-quote characters before copying to CAI. Turn off PANI transparency, if the SBC already created it. **Workaround:** Use SMM to remove the double-quote characters in operator-specific-GI value

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132653	N/A	3	Penetration test revealed "Insufficient Privilege Separation" issues in the EMA. **Impact:** The EMA improperly validates user privileges. Some actions were available in the Graphical User Interface (GUI) only to an Administrator user, but the action was performed when the same request was sent to the user with an Operator or Guest role. **Root Cause:** Workspace-based authorization was not implemented, so a user who doesn't have access to a workspace could access configuration entities defined in the workspace. This vulnerability is not directly exploitable from the EMA UI. To exploit it, a person must create a specific CURL request. **Steps to Replicate:** As an Operator or Guest user, operate unavailable in the GUI. The operation should fail with a 403 error.	The code is modified to implement workspace-based authorization, which means that a user who does not have access to a workspace cannot access configuration entities defined in the workspace. **Workaround:** Perform the action from the UI rather than directly through CURL.
SBX-132670	SBX-129713 (10.1.6)	2	SBC 7000 SNMP V3 engine boot counter issue **Impact:** After an upgrade alarms are not working as expected. **Root Cause:** During upgrade the SNMP engine state data is not retained which causes issues after upgrade. **Steps to Replicate:** Configure SNMP v3 trap target and perform an upgrade. With fix build, alarms should work as expected. Make sure global.data file being retained as part of upgrade by checking upgrade logs.	The file global.data, which contains snmp engine state/ bootcount, is being retained during upgrade to resolve this issue. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132699	N/A	3	The overloadRejects count unexpectedly increases **Impact:** The SBC overloadRejects counter increments when there is no overload. **Root Cause:** This increment is due to the receipt of congestion (cause 42 Equipment congestion) from the remote peer since the cause matches. During the disconnect treatment, the SBC checked the cause and increased the overloadRejects count without validating whether or not the congestion is raised locally. **Steps to Replicate:** Basic configuration for SIP call (UserA to UserB): 1. Save the overloadRejects counter for Congestion. > show status system systemCongestionIntervalStatistics 2. User A calls User B. 3. User B rejects the call with 503 and reason code 42 in the reason header. 4. Calls get disconnected. 5. Check the Congestion Statistics for overloadRejects is not incremented.	The code is modified to ensure the counter is incremented only if the congestion is set internally by the SBC **Workaround:** NA

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132739	N/A	2	Download failed for the files listed under Back Trace in EMA PM. **Impact:** Download failed for the files listed under Back Trace in EMA PM. **Root Cause:** When a file is downloading, clicking on the same file multiple times for download throws error message. **Steps to Replicate:** 1. Login to EMA. 2. Navigate to Troubleshooting → Call Trace/Logs/Monitors → Log Management. 3. Click Back Trace. 4. Click the download button for any of the files listed. You will be able to download the files without error messages.	When a file is downloading, clicking on the same file multiple times for downloading is prevented until the first download is complete. Also downloading icon is shown when download is in progress. **Workaround:** No workaround
SBX-132748	SBX-132504 (10.1.6)	3	The SBC sends a PRACK twice against an 18x response **Impact:** The SBC sent a PRACK twice in response to an 18x response. **Root Cause:** When e2e Prack is enabled, the SBC sometimes sends a PRACK twice for an 18x response. **Steps to Replicate:** 1. Enable e2e Prack, transcode free, sdpAttributesSelectiveRelay is enabled on both Ingress and Egress. 2. The incoming call is handled for late media passthrough. 3. The Egress responds with an 18x with SDP to the Ingress. 4. The Ingress sends a Prack with SDP relay to the Egress. 5. After OA completes, the SBC internally attempts to trigger the Offer and ressend a Prack.	The internal ICM message relay from Ingress to Egress was issued twice. Added logic to clean up the internal ICM message relay from Ingress to Egress to prevent a duplicate 18x response. **Workaround:** Disable e2e Prack.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132844	SBX-131702 (10.1.6)	3	Adding/configuring a SIP Param Filter Profile from the EMA GUI does not work **Impact:** Cannot create/configure a SIP Parm Filter Profile via the EMA GUI. **Root Cause:** The Profile requires that the user creates at least one header before saving the configuration. **Steps to Replicate:** From the EMA GUI, try to create a SIP Param Filter Profile without creating a header filter.	Relaxed the code to allow the user to create a SIP Param Filter Profile without a header. **Workaround:** Use CLI.
SBX-132867	N/A	2	Media Loss is observed towards the Mediation Server when PCSI LI is enabled on the Egress leg (PCSI header sent in an 18x/2xx) **Impact:** Packet loss occurs in the Mediation Server from the downstream leg recording via snooping in TCP LI over IPsec. **Root Cause:** In a TCP LI over IPsec scenario, the NP Snoop packet alloc request sometimes gets the mbuf memory block used by the IPsec decrypted packet. The NP only clears the required flags in the mbuf for snooping, but the dpkt_info->IPsec flag used in the xmit process is not cleared in the DS snoop, resulting in unwanted paths in the code (i.e., a snoop does not happen from those packets). The US Snoop has this fix already; hence, it works fine as expected. Only the DS requires fixing. **Steps to Replicate:** None since the custom replication steps are customer-specific.	The code is modified for a DS snoop to clear all required flags from packet mbuf allocation (including dpkt_info->IPsec) and update them as per snooping requirements. **Workaround:** There is no workaround when TCP LI over IPsec is required.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132914	N/A	2	CE_2N_Comp_ScmProcess_0 / terminated with signal SIGSEGV **Impact:** The ScmProcess cored while processing an INVITE, which contained a History-Info header that did not contain a HostName. **Root Cause:** SIP encountered a Segmentation Fault due to a NULL pointer access. • The INVITE being processed contained 2 History-Info headers. • The first History-Info head contained a Hostname, but the second one did not. This occurred while the code attempted to compare the Hostnames in the two History-Info headers. Because the second History-Info header did not contain a Hostname, the pointer to the hostName in the code was a NULL pointer. The code did not have a NULL pointer check before attempting to compare the hostnames in the two headers. This produced a Segmentation Fault. **Steps to Replicate:** Send an INVITE containing at least two History-Info headers. At least one of these headers should contain a Hostname, and another should not.	Added a NULL pointer check to prevent the code from attempting to access low memory. **Workaround:** Do not send an INVITE with multiple History-Info headers when one or more History-Info headers contain a Hostname and one or do not. Alternatively, disable "acceptHistoryInfo" in the sipTrunkGroup->signaling configuration.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-132985	N/A	2	SBC 12.1.2 call load packet loss occurred **Impact:** Packets loss observed for a 82599 NIC. **Root Cause:** The Intel 82599 NIC occasionally dropped packets due to a lack of DMA resources and a growing count of interface rx_no_dma_resources on the Host. **Steps to Replicate:** Bring up and configure the SBC SWe instance with Intel 825LeakSanitizer leaks are detected in the SLB after a switchover **Impact:** LeakSanitizer leaks are detected in the SLB after a switchover in the SbcIntf process. **Root Cause:** The suppressed leaks were reported for the SbcIntf process because the ASAN environment variables were not set for this process. **Steps to Replicate:** Run the ASAN test to verify that sbcIntf has not reported a leak. Suspended leaks are logged into the associated sanitizer leak log file.99 VF to run passthrough call load.	Fixed PMD code to free pkt buffers with every packet transmission. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133037	SBX-133032 (12.1.2)	2	Non-root mode of SBC deployment failure occurred **Impact:** When the SBC Helm is deployed in a non-root mode, containers that use logrotate undergo continuous crashes and restarts. **Root Cause:** When the container is run in the non-root mode, the container run-time doesn't append the user's /etc/passwd file for which the container is instructed to run (using runAsUser). Hence, the logrotate fails with the following error message: `error: Cannot find logrotate UID (1004) in passwd file` **Steps to Replicate:** Launch the SBC Helm deployment in non-root mode. The containers undergo continuous crashes and restarts.	Created a new config-map to populate the default users and requested container (non-root) user. This config map was mounted to /etc/passwd path of all containers to ensure the logrotate functions on the expected lines. **Workaround:** None
SBX-133115	N/A	3	User password change via RESTCONF API fails **Impact:** Cannot change the password of the newly-created user using RESTCONF API. **Root Cause:** The symlink socket for action command is re-used for each action with the same user name. **Steps to Replicate:** 1. Create a new user through RESTCONF API. 2. Try to change the password of the new user with a temporary password through the RESTCONF API.	The symlink socket for action command will be updated for every session with the user session details. **Workaround:** N/A

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133216	N/A	2	[IMS-AKA] After the switchover, the SBC fails to send messages to the UE. **Impact:** On a cloud SBC after a switchover, the SBC fails to send SIP messages to the UE over an AKA connection (when there is bind failure for AKA port on standby). **Root Cause:** One server (port-s) and two client ephemeral ports (port-c) are allocated for each SSP on the Active SBC. In order to achieve redundancy, the same ports must be allocated on the Standby as well. In rare scenarios, the Standby SBC fails to allocate/bind the same port(s) because they are taken by some other processes/ applications on the SBC. When the Standby SBC fails to allocate the same port as the Active SBC, the SBC fails to send SIP messages to the UE over a secure AKA ports after a switchover. **Steps to Replicate:** 1. Perform IMS-AKA registration. 2. Run a stable call. 3. Perform a switchover and check that the SIP messages for the call are sent to the UE after the switchover.	The SBC is modified to avoid this AKA port bind failure issue on the Standby by using fixed/ reserved ports for the IMS-AKA. Using reserved ports guarantee that the ports are free on the Standby. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133270	N/A	3	http->https auto-redirection for PlatformManager is missing, causing a flagged issue in the security scan **Impact:** http->https auto-redirection for PlatformManager is missing, causing a flagged issue in the security scan. **Root Cause:** An auto-redirect from http://ip:444 to https://ip:444 was not configured in Apache. **Steps to Replicate:** 1. Access the Platform Manager using http://ip:444. 2. Auto redirection to https://ip:444 should occur.	Modified the code in the Apache configuration to redirect from http://ip:444 to https://ip:444. **Workaround:** Access Platform Manager directly using https://ip:444
SBX-133303	N/A	3	SBC 12.1.2 : sbxPerf logs are not getting written **Impact:** The sbxPerf logs are not continuously written to the /var/log/sonus/sbxPerf directory, resulting in only a single log entry for each log file in the sbxPerf directory. **Root Cause:** The sbxPerf service is not starting or stopping correctly during the logrotate process. As a result, only a single log entry is created in the sbxPerf directory, while the sbxPerf service is stopped each time logrotate is executed. **Steps to Replicate:** 1. Issue the command "systemctl status sbxPerf" and check if sbxPerf up and running. 2. Check that the logs are added to the /var/log/sonus/sbxPerf directory.	Changes were made to resolve log compression failures in the sbxPerf logrotate configuration. The configuration was also updated to use systemctl for managing the start/stop process, improving reliability. Additionally, the sbxPerf script was modified to generate individual logs for each execution. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133368	SBX-132456 (10.1.6)	3	ScmP cored under a high call load **Impact:** For an incoming call using an advance SMM rule where a preFix trunk group does not match the trigger, a core may occur. **Root Cause:** The memory allocation for the SMM rule deletes it twice. **Steps to Replicate:** 1. Configure an advance SMM rule and preFix TG. 2. The incoming call triggers a SIPS response 488.	The code is modified to delete the SMM rule only once. **Workaround:** Remove the preFix TG SMM rule or block the incoming call.
SBX-133478	N/A	3	An SC Container restart occurs due to a probe i/o timeout **Impact:** The container restarts due to the probe failure because the probe issues an i/o timeout error. Consequently, the client connection from Kubelet was unsuccessful. **Root Cause:** The server-side socket hung up, causing a connection close failure, which increased the client (Kubelet) connection queue stack at the server side. Once this stack reached the maximum limit, connections were no longer accepted, causing the probe i/o timeout error. **Steps to Replicate:** 1. Deploy the application, and check if prob listeners are running on each confd pods: "ps -ef|grep tcpProbeListener" "netstat -atnp|grep 4545" -----> probe ports in listening state (LISTEN) 2. Check for pod output descriptions. You should not see "i/o timeout" for the probe events.	Added a HealthCheck thread from the server probes listeners to continuously monitor form the server-side socket functionality and also a recovery mechanism within container in case of failure **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133496	SBX-132298 (10.1.5)	2	The SAM process is leaking memory **Impact:** The SAM process leaks memory when repeatedly running concurrent RESTCONF API status requests during a heavy call load. The combination of these 2 status requests triggers the leak: • https://<MGT IP>/api/operational/addressContext/default/ • https://<MGT IP>/api/operational/global/SipRecStatus/ **Root Cause:** The code that handles the SipRecStatus request overwrites a pointer to a buffer used in processing addressContext requests. As a result, the original buffer leaks. **Steps to Replicate:** Run the following RESTCONF API requests repeatedly while running a heavy call load: 1. https://<MGT IP>/api/operational/addressContext/default/ 2. https://<MGT IP>/api/operational/global/SipRecStatus/	Modified the code that handles the SipRecStatus request so it no longer overwrites the pointer to the buffer used in processing the addressContext request. **Workaround:** Do not run two previously mentioned requests at the same time.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133667	N/A	3	Call Trace setup has duplicated menu entry for "Level4 Trace Messages" **Impact:** The Call Trace setup includes a duplicated menu entry for "Level4 Trace Messages." **Root Cause:** "Level4 Trace Messages" appears twice because of code duplication. **Steps to Replicate:** 1. Login to EMA as admin. 2. Navigate to Troubleshooting --> Call Trace/Logs/Monitors --> Call Trace and Packet Capture --> Call Trace. Expected result: *"Level4 Trace Messages" is shown just once.	The duplicated code is removed. **Workaround:** None
SBX-133680	SBX-133348 (10.1.x)	3	The SBC sends multiple PAI instances that are not within angle brackets **Impact:** The SBC combines multiple PAI URIs into one header when angle brackets are mssing. **Root Cause:** SBC merges multiple URIs of the PAI header that are not within a pair of angle brackets ("<>") for each URI. **Steps to Replicate:** 1. Configure PAI transparency. 2. Set up an incoming call with multiple PAIs, where one of them is not within "<>" brackets.	The code is modified to ensure the SBC does not merge multiple URIs of PAI header if they each are not within angle brackets ("<>"). **Workaround:** Use SMM

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133683	N/A	3	SBC SWe on AWS v12 changes MTU to 9001 **Impact:** An SBC SWe on AWS instance launched with release 12.1.2 AMI has the MTU for all interfaces set to 9001, which causes problems with vim operations for an SSH connection. **Root Cause:** The DHCP response sets the MTU size to 9001 for all interfaces. **Steps to Replicate:** 1. Launch SBC instance with 12.1.2 release AMI on AWS. 2. Once the SBC application comes up, run "ifconfig" to observe the AMI set MTU size set to 9001 for all interfaces.	Updated the DHCP option configurations to avoid setting the MTU size on the AWS platform. **Workaround:** Once the SBC application is up, manually set the MTU size of the interface to 1500 using the command: `ifconfig <interface name> mtu 1500`. Example : `ifconfig mgt0 mtu 1500`
SBX-133958	SBX-133497 (11.1.3)	3	SamP cored on the Standby node **Impact:** Repeated SAM process cores on the Standby node. **Root Cause:** The cores are a result of either a HashInsert or a HashRemove setting in a recording hash table. Calls may get added to this hash table if they are "recordable" (media recording is configured on the Trunk Group) but are NOT of callType SIPFE_SIP_RECORDER_CALL: /ADDRESS_CONTEXT:/zone/ sipTrunkGroup/media/recordable A corruption in the hash table results from a freed call block that was never removed from the hash table. **Steps to Replicate:** This issue is not reproducible.	Code is added to ensure call block memory is removed from the hash table before freeing the call block. **Workaround:** Unfortunately, this issue may only be preventable by disabling media recording on all trunk groups.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133962	SBX-133780 (11.1.3)	3	ScmP cored when processing a SUBSCRIBE message with a NULL fromTag **Impact:** The SCM cored when processing a SUBSCRIBE message with a NULL fromTag following a previously-challenged Subscribe. **Root Cause:** The code is missing a NULL pointer check that causes a core when the fromTag in the incoming message is compared to the current "ingressRemoteTag" because the SCM attempted to dereference a NULL pointer. *NOTE: The incoming Subscribe is related to a "Challenged" request when the new fromTag is NULL.* **Steps to Replicate:** This bug was found by code inspection.	The code is modified to add a NULL pointer check to prevent a core when the fromTag is NULL. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-133969	N/A	2	OAM: Resolving LDAP Server FQDN based on the type of the IP family that is associated to OAM's mgmt interface **Impact:** The LDAP Server FQDN does not resolve based on the type of IP family associated with OAM's management interface. **Root Cause:** If the ldapConfigurationMode parameter set to advanced, the ldapServerAddress may also be specified as an FQDN. Only the first address returned from the DNS query will be used to connect to the LDAP server. If the first IP returned is not of the same type(IP family) as eth1(mgt0 for OAM), it results in issues with connecting to LDAP server. **Steps to Replicate:** 1. Enable externalAuthentication and set the type to LDAP. 2. Configur LDAP server with ldapServerAddress as FQDN. 3. Add IPv4 and IPv6 addresses to /etc/hosts to resolve the ldapServerAddress specified. Expected results : The first address returned is of the same IP family as that of mgtIp.	The code is modified to pass the IP family (AF_INET or AF_INET6) to the getaddrinfo call based on the IP type configured on mgmt interface. **Workaround:** Add IP addresses from the same IP family as the mgmt interface to the /etc/hosts file for address resolution.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-134058	N/A	3	EMA Home Page - Quick Helmp links point to the 6.2.x documentation **Impact:** On the EMA Home page, the Quick Helmp links point to the 6.2.x customer documentation. **Root Cause:** The Quick Helmp links on the Home page were not updated to future release versions after the 6.2.x release. **Steps to Replicate:** 1. Login to EMA and navigate to Home -> Dashboard. 2. Open the Dashboard setting. 3. In the Panels 'Quick Helmp' display, click on any link. Expected result: The quick links point to the correct version of the customer documentation.	The code is modified to point the Quick Helmp links to the correct version of the customer documentation. **Workaround:** None

Resolved Issues in 12.01.02R001 Release

The following severity 1 issues are resolved in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-131499	N/A	1	A re-INVITE from the carrier results in the SBC violating protocol in the SDP answer **Impact:** For session refresh INV/UPDATE, the PSBC violates protocol in the confirmation SDP answer when the number of codecs differs from the original request and is responded to locally. **Root Cause:** The Ribbon SBC responds to a re-INVITE SDP offer with an SDP answer that contains previously removed codecs (AMR-WB/AMR/PCMU). Some vendors interpret this as a protocol violation and expect the SBC to respond to the confirmation SDP offer with a confirmation SDP answer that contains only the previously negotiated codec. Depending on the behavior of the far end, the call may terminate. **Steps to Replicate:** Observe differences when running session refresh INVITE/UPDATE flows with the End2EndReInvite flag and End2EndUpdate flag enabled/disabled.	The code is modified to allow flags to control whether the SBC responds with a full or partial list. When the flags are enabled, and the number of codecs in a received SDP and SDP received in session refresh INV/UPDATE differ, the SBC shows the default behavior if End2EndReInv or End2EndUpdate is enabled. When the flags are disabled, the SBC auto-answers with the subset of codecs listed in the initial offer. **Workaround:** None.
SBX-133032	N/A	1	Non-root mode of SBC deployment failure in the customer's K8s platform **Impact:** On the customer K8s platform, when the SBC Helm is deployed in non-root mode, containers that makes use of logrotate undergo continuous crash and restarts. **Root Cause:** On the customer K8s platform, when the container is run in the non-root mode, the container run-time does not append the /etc/passwd file with the user with which container is instructed to run (i.e., runAsUser). Hence the logrotate fails with the following error message - error: Cannot find logrotate UID (1004) in passwd file **Steps to Replicate:** With the fix not in picture, launch the SBC Helm deployment in non-root mode on the customer K8s platform. The containers undergo continuous crash and restarts.	The code is modified to create a new config-map specifically on the customer K8s platform to populate the default users and requested container (non-root) user. This config map was mounted to /etc/passwd path of all containers. This ensured that logrotate functions on expected lines. **Workaround:** None.

The following severity 2-4 issues are resolved in this release:

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-132728	N/A	2	SBC CNe - need to populate actualCEName in the confd cli session **Impact:** The OAM displays identical CLI prompts (<user>@vsbc1) across different deployments. **Root Cause:** The OAM CLI and bash prompts were picking up the default name 'vsbc1'. **Steps to Replicate:** • Test CLI/bash prompts with AddHaIpSuffix set to true and false. • Also, test with eth0 configured for IPv6.	The code is modified to enable the CLI/bash prompts to contain the ActualCeName to match the node name displayed in RAMP. **Workaround:** None.
SBX-132869	N/A	2	The LIF interface should not contain an empty networkSegment and ipName value, or the SBC fails to assign an IP to the pkt0/pkt1 on a managed pod **Impact:** The LIF Interface CLI should not have an empty networkSegment name, ipNameV4/ipNameV6 **Root Cause:** Under the LIF Interface CLI, the SBC deleted the networkSegment name/ipNameV4/ipNameV6, resulting in a bad configuration due to the SBC's failure to allocate pkt0/pkt1 IP at the SG pod. **Steps to Replicate:** 1. Delete addressContext default ipInterfaceGroup IPIG_SG0 ipInterface IPIF0_SG ipNameV6. 2. Delete addressContext default ipInterfaceGroup IPIG_SG0 ipInterface IPIF0_SG networkSegmentName. The following error should appear: admin@vsbc1% commit Aborted: 'addressContext default ipInterfaceGroup IPIG_SG0 ipInterface IPIF0_SG networkSegmentName': Cannot delete ipNameV4/ipNameV6/networkSegmentName after the interface is created; you must delete the interface and create again to modify	The code is modified to generate an error when the CLI delete operation is called for networkSegment nameipNameV4/ipNameV6 on the ipInterface. **Workaround:** Do not delete the networkSegment nameipNameV4/ipNameV6 on the ipInterface.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-132888	N/A	3	Graceful handling of subprocess in Python Code **Impact:** A defunct process is created when the CLI command is triggered from a Python script. **Root Cause:** When the SBC executes any CLI command from a Python script, one process is created to execute the CLI command. After execution of the CLI command, the created process is not terminated unless the main process is terminated. **Steps to Replicate:** Not easily reproducible.	The code is modified to check if the created process is still alive after the CLI command execution, and if so, then the SBC gracefully terminates the process. **Workaround:** None.
SBX-133045	N/A	3	SAM keeps crashing after an upgrade to 12.1.2R0 **Impact:** The SamProcess cores periodically, which induces a switchover. **Root Cause:** The code cores when attempting to free a SIPCM_SESSION_APP_DATA_STR that is already freed. This occurs because the flag SIPCM_TLS_KILL_CONN_AND_SESS is set in socketPtr->tlsKillCode. **Steps to Replicate:** Run TLS calls under load.	The code is modified to remove a line of code that was setting the flag = SIPCM_TLS_KILL_CONN_AND_SESS and causing a double free. **Workaround:** None.
SBX-133242	SBX-12980 0 (12.1.2)	2	High disk usage because the 'warn' log file does not logrotate **Impact:** The 'warn' log continually grows, consuming the entire hard drive. **Root Cause:** The warn log under /var/log/warn does not delete the old files, which results in high disk usage **Steps to Replicate:** Install the build with the fix; the warn log should not consume more disk space.	The code is modified to add a warn log to rsyslog logrotate to delete old log files periodically. **Workaround:** None.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133243	SBX-132338 (11.1.1)	2	The SBC handles double quotes in the PANI header incorrectly **Impact:** The SBC sends a syntax error in the P-Access-Network-Info(PANI) header. Also, if the transparency PANI header is turned on in the outgoing profile, the SBC sends duplicated PANI headers. **Root Cause:** When the SBC receives a PANI header with parameter operator-specific-GI value within a double quote string, it does not strip off double quote characters for CAI. **Steps to Replicate:** 1. Config JJ9030 feature. 2. In-coming has PANI, and operator-specific-GI value is within the double quote string. 3. The SBC sends Invite with PANI and syntax error for operator-specific-GI value.	The code is modified to remove double quote characters before copying to CAI. **Workaround:** Use SMM to remove the double quote characters in the operator-specific GI value.
SBX-133244	SBX-132717 (10.1.6)	2	SEGV on unknown address in sipsCall.c **Impact:** The SCM cores in the forking feature. **Root Cause:** When SIPS tries to generate a message (for the forking feature), the message is created from local stack memory, which does not initialize properly. As a result, the SBC tries to access garbage memory. **Steps to Replicate:** Not easily reproducible.	The code is modified to initialize the local stack memory message properly. **Workaround:** Disable the forking feature.

Issue ID	Original Issue	Sev	Problem Description	Resolution
SBX-133380	N/A	2	Restore revision is failing on SBC **Impact:** The OAM fails to back up the configuration data to RAMP during the RAMP switchover. **Root Cause:** The issue was triggered due to an incorrect RAMP IP value in the /etc/hosts file on OAM. A RAMP switchover triggers an action request to OAM to update the configured parameters containing the username, password, and URL to access the object store service from RAMP. This also results in updating/etc/hosts with the new active RAMP IP (for the IPv6 communication). OAM uses FQDN (emsforconfigurator), which maps to the current RAMP active IP and is resolved via the entry in /etc/hosts. The script used to update the IP failed as /etc/hosts is a K8s managed file in a CNF deployment, resulting in the issue on alternate switchovers. **Steps to Replicate:** Ribbon tested the configuration backup during RAMP switchovers.	The code is modified to ensure the script updates the RAMP switchover IP correctly. **Workaround:** Editing the /etc/hosts file with the new active RAMP IP on a RAMP switchover.
SBX-133398	N/A	2	Avoid Container restart: Remove OAM, RAC dependency **Problem Description**: SBC Container restarts are observed. No container restarts should be seen during installs/upgrades. **Root Cause**: Upon installation/bring-up, SBC containers that need OAM-config may have to wait longer for it to become available if the OAM takes a long time. This causes a delay in creating the startup and liveness probes in SBC containers. Although SBC container pods have initialDelaySeconds configured for startup and liveness probes, it is sometimes not enough as the availability of OAM-config could take a long time. Even though it is not a failure scenario, kubelet would see the startup and liveness probes failing and restart the container. After the upgrade, the SBC container waits 10 minutes for the correct version of the config to become available. If the correct config is unavailable for 10 mins, it reboots the container. **Steps to Replicate:** 1. Install SBC CNF and verify that no container restarts are seen. 2. Upgrade from 12.1.2.R0 to 12.1.2R1; verify that no container restarts are seen.	The code is modified to create the startup and liveness probes immediately after startup instead of waiting for OAM-config to become available. This avoids the restarts caused by the delay in creating startup and liveness probes. **Workaround:** None.

Resolved Issues in 12.01.02R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Problem Description	Resolution
SBX-127843	N/A	CNe: SC policyServerStatus not coming active after new policy server configurations **Impact:** SG pod sends DNS queries to resolve PSX IP even after deleting the policy server configuration. **Root Cause:** The Timer handling DNS query is not deleted when the policy server is deleted. This is because the policy server name stored by the timer is appended with an index, which caused a failure in comparing server names. **Steps to Replicate:** 1. Spawn SBC CNe in 12.1.2 build 2. Configure PSX details using FQDN (the connection is now active). 3. Bring down the psx 4. Delete the policy server configuration in the SBC CNe. Expected result without fix: The SBC keeps sending DNS queries. Expected result with fix: The SBC should stop sending DNS queries.	The code is modified to compare the FQDN during timer deletion. **Workaround:** None.
SBX-131140	N/A	[12.1.1 CNe Deployment - Performance] SamProcess core observed in RS pod during REGISTRATION+Call load with Switchovers **Impact:** A high number of Reg entries (more than max allowed) were reconstructed after the RS pod switchover due to the RAC instance ID issue. This led to a crash in the RS pod. **Root Cause:** The instance ID fetched by the RS during reconstruction was incorrect, so there were almost twice the number of entries than the maximum allowed. **Steps to Replicate:** 1. Run 1200rps with AUTH and refresh reg interval of 3600 seconds. Number of registered clients: 450K. 2. Run 360 CPS CHT=100sec load. 3. Perform random switchovers on every pod for every one hour. A crash should not happen.	The code is modified to fix the instance ID issue in the RAC pod. As well, checks are added in the RS pod to construct only the maximum number of entries per pod. Finally, the reconstruction logic is changed to to a batch format instead of reconstructing all entries in one shot. **Workaround:** None.

Issue Id	Original Issue	Problem Description	Resolution
SBX-131249	SBX-129827 (10.1.6)	Frequent NP cores on SWe V09.02.04R002 **Impact:** Corrupt buffer management between NP and DSP Processes leads to NP and/or UXPAD and/or TPAD core dumps while running traffic, leading to a service outage. **Root Cause:** The incorrect tuning of the SWe VM impacts the buffer management between the NP and DSP processes. NP is slow in draining packets and releasing the buffers to the free pool, while DSP eventually runs out of buffers to transmit packets. The case of buffer unavailability isn't handled correctly in the TPAD DSP process, eventually resulting in the accumulated payload size running into a huge value. Whenever the buffer is available next time, the accumulated payload size worth of data is copied to the buffer, leading to corruption. **Steps to Replicate:** Run a G729A (Ingress) to G711U (Egress) transcode load with LRBT enabled on Ingress. • Without the fix, the NP and/or UXPAD and/or TPAD core dumps are observable. • With the Fix, no core dumps are observed.	The code is modified to drop the accumulated packet in buffer unavailability, and then the payload size is reset. **Workaround:** Ensure that the SBC VM is tuned correctly as per recommendations.

Issue Id	Original Issue	Problem Description	Resolution
SBX-131482	SBX-129099 (10.1.5)	DNS issue - The SBC is unable to send SIP ACK and BYE to MS Teams **Impact:** DNS queries may fail, causing calls or pathCheck to fail. **Root Cause:** The DnsProcess may send a DNS response containing the wrong dnsZoneId to the requesting Agent (causing the response to be lost). This timing-dependent edge case can occur when the DnsProcess simultaneously handles multiple DNS queries for the same FQDN from different DNS Agents and the dnsZoneId(s) differ. **Steps to Replicate:** Provision the SBC to support FQDN calls: 1. Create zone(s) without sipTrunkGroup(s). 2. Create DNS Group(s) and assign to zone(s). 3. Create FQDN ipPeer(s) in zone(s) 4. Create sipTrunkGroup(s) within the zone(s) [egress leg of call] (some use a dnsZoneId of 0 and others dnsZoneId of 1). 5. Create pathCheck profile 6. Assign pathCheck profile to FQDN ipPeer(s) 7. State enable pathCheck on the FQDN ipPeer(s) 8. Create routings to FQDN ipPeers through the set of sipTrunkGroup(s) 9. Run calls to the FQDN ipPeer(s) through the set of sipTrunkGroup(s) Call failures and/or pathCheck failures can occur within 12 hours.	The code is modified to enhance the DnsProcess to save the dnsZoneId contained in the DNS query. The DnsProcess sends the DNS response containing the correct dnsZoneId to the requesting DNS Agent. **Workaround:** None.
SBX-131541	SBX-126193 (11.1.1)	PesP core occurred on the server **Impact:** The PesProcess cored and caused an SBC switchover. **Root Cause:** The Pgresult object was declared static, causing a double-free issue to be seen and resulting in a segmentation fault. **Steps to Replicate:** You can recreate this while performing bulk updates on the toll-free prefix info table and simultaneously running calls.	The code is modified to change the pgresult object to nonstatic. **Workaround:** None.

Issue Id	Original Issue	Problem Description	Resolution
SBX-131865	N/A	Configuration and Profile Import/Export fails on SBC EMA/ CLI **Impact:** Config import is failing post upgrade to 12.1.2 because of an invalid trap entry present in 11.x DB ("sonusSWeVcpuAllocationDiffers Cnf"). **Root Cause:** Cnf trap names are generated from original trap names(sonusTrap.xml). Because of a trailing space present in original trap name, the Cnf trap name was getting generated incorrectly and this invalid entry was propagated to the newer release after upgrade, causing an import failure. **Steps to Replicate:** 1) Bring up set-up in 11.x version(where invalid cnf traps like "sonusSWeVcpuAllocationDiffers Cnf" are present). 2) Upgrade the set up to 12.1.2. 3) Try config export, clear DB and try importing the configuration. The post-upgrade config import should go through.	Removed the invalid trap during upgrade as part of CPX Upgrade code. Workaround: After upgrading, go to /opt/ sonus/sbx/tailf/var/confd/cdb and remove incorrect trap names if present in sonusTrap.xml/ sonusTrapCnf.xml, based on the type of deployment. Run $CONFD_LOAD -l -r sonusTrap.xml/ sonusTrapCnf.xml as per deployment.
SBX-131998	SBX-131289 (10.1.5)	Global Subscriber number causes call failure on the SBC **Impact:** The application cache cannot give the correct object when there are more than 6000 subscriber Entity objects. **Root Cause:** The logic during prefix matching was wrong, as we picked the Subscriber using the wrong key. **Steps to Replicate:** Add 6000+ subscribers and make a call with one subscriber as the called number. This picks the wrong subscriber object and, hence, use the wrong packet service profile.	The code is modified to fix the logic to pick the prefix from the right key. **Workaround:** Ensure the number of subscribers exceeds 6000.

Issue Id	Original Issue	Problem Description	Resolution
SBX-132015	N/A	The Ringback sound is not heard through the SBC Core **Impact:** In loopback flows, the ringback sound is not heard through the SBC Core. As a result, media is dropped internally in the SBC with undesirable ether header reasons. **Root Cause: The** NP PKT mbuf reach works used specific mbuf fields for storing VLAN information. In this call flow, Packet mbuf received on an enabled PKT interface is looped back using a non-VLAN PKT interface. Their vlan fields were not cleared, and such packets' LIF validations failed, causing the drops and no audio. **Steps to Replicate:** SBC loopback media call flows with a VLAN-enabled PKT interface for incoming media, and a disabled PKT interface for loopback media legs will reproduce this issue.	The code is modified to update the Packet mbuf header VLAN fields and clear them based on the interface (VLAN enabled/ disabled) used. NP LIF validations will see the expected values and relay the media now. **Workaround:** Disable VLAN on both interfaces to avoid this problem.
SBX-132727	N/A	CNe: config restore unsuccessful on SBC when performed from RAMP **Impact:** The SBC did not restart after attempting a restore revision from RAMP/CLI. A configuration restore was performed from RAMP to SBC, but it was observed to be unsuccessful. **Root Cause:** The restoreRevision action command is handled internally by SmProcess. It downloads the revision for which the restore is requested (if not present locally), replaces the corresponding cdb(database) files, and triggers a system reboot by invoking a script “reboot.sh.” This script internally invokes docDockerop if the environment is identified as CNe (and then the probes restart the container). The script uses “/proc/self/cgroup” to determine the environment and uses the presence of kubepods or docDocker to differentiate a KUBE_ENV from a DOCKER_ENV. Currently, the docker stop is only invoked for KUBE_ENV. The group file in the customer lab contains both KubePods and Docker, which results in an incorrect detection by the script and prevents it from calling DocDockerop. **Steps to Replicate**: To replicate this issue, launch the SBC instance in a Kubernetes environment backed by Docker CRI, ensuring that the group phrase includes 'kubepod' and 'docker.' Then, attempt to apply the revision.	The code is modified to refine the logic within the "reboot. sh" script to initiate the reboot process for Kubepods accurately and, specifically, correct the logic that ascertains whether the system is running as Docker or Kubernetes. **Workaround:** Trigger a docker stop/docker start on all the SBC pods (post restoreRevision) so that the pods can apply the restored revision

The following severity 2-4 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-122529	N/A	3	SBC not adding 3xx contact params in out of dialog scenarios **Impact:** SBC not adding 3xx contact params in out of dialog scenarios **Root Cause:** It is observed that its a day-1 issue i.e., SBC is adding the parameters of the contact header received in a 3xx message in an outgoing Subscribe message only with the local redirection that is when the force re-query flag is disabled. In all other cases like force re-query enabled or enhanced local redirection enabled, subscribe doesn't include the params from the contact. **Steps to Replicate:** 1. For the OOD scenarios such as SUBSCRIBE ---- 302 (contact has Party C(BatsIP) address and pkt 1 address) The issue will be recreated when force re-query enabled or enhanced local redirection enabled . In these cases, subscribe doesn't include the params from the contact. 2. Verify all the testcases with Force Requery enabled and Force Requery Disabled. In all the testCases, SBC should add the parameters of the contact header received in a 3xx message in an outgoing Subscribe message.	The scenario is implemented when the 3xx contact has maddr parameter(Epic No. SBX-4555) where as it is not implemented for 3xx redirection scenarios for Out Of Dialogue scenarios. So, the logic is been added for the required conditions. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125077	N/A	2	[CNe] SC pod scaling out by 1 pod while running bulk config **Impact:** SC pod scaling out by 1 pod while running bulk config. **Root Cause:** SC pod scaling out by 1 pod while running bulk config because CPU utilization is crossing threshold **Steps to Replicate:** 1. Bring up Setup in latest SBC build 2. Used OBS Image V1.2.3 3. Registered Setup to RAMP 4. Run bulk configurations 5. Check only scale out if avg of two hottest CPU crosses the Threshold.	While considering the CPU usage by HPA, only one hottest signaling CPU is considered for scale-up. Because of this when threshold is crossed SC pods were scaling out by 1. Now considering average of 2 hottest CPU's to calculate threshold. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128962	N/A	2	CNe_SG: Rx - Disconnect-Peer-Answer not received at SG POD **Impact:** When a diameter peer's state is disabled, a Disconnect-Peer-Request(DPR) AVP and TCP FIN is sent by SBC to disconnect the TCP connection. The Disconnect-Peer-Answer AVP response and FIN/ACK from the peer were dropped at SBC due to which SBC kept retransmitting FIN/ACK. **Root Cause:** This is a day 1 Diameter issue (on both the SBC CNe and other SBC platforms) where the DPR and the FIN for disconnecting the TCP connection were being sent by SBC back to back without waiting for the DPA or FIN/ACK response from the peer. This was causing SBC to delete the ACLs created for the diameter peer prematurely before any response was received and drop any subsequent response(diameter AVPs or TCP messages) sent by the peer and retransmit the FIN. **Steps to Replicate:** Create a diameter Rx peer. Enable the diameter peer and wait for TCP connection to be established successfully. Disable the diameter peer.	As part of diameter peer disable flow, the TCP socket closure and ACL deletion will be delayed till FIN/ACK is received from the peer. If FIN/ACK is not received from peer immediately, an internal timer would cause FIN/ACK to be retried and on timeout the TCP connection and ACLs would be cleaned up accordingly. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129062	N/A	2	[12.1 CICD] Rf-Diameter msg 271 Accounting Interim and Stop Records are not appearing after switchover, Rx-STR is not sent after switchover **Impact:** Diameter Rf: In a redundant SBC setup configured with Diameter Rf, ACR STOP AVPs were not being generated by SBC after switchover when an active call ended. Diameter RX: In a redundant SBC setup configured with Diameter RX, Session Termination Request(STR)AVP was not being sent by SBC after switchover when an active call ended. **Root Cause:** In redundant SBC setups(HA/N:1), the TLVs(variable length components) in the Diameter session control block(SCB) mirrored by the active SBC were being unpacked incorrectly by the standby/inactive SBCs. The packing logic used the size of the fixed components as the offset to start packing the TLVS, whereas the unpacking logic used the startOfData[] structure member as the beginning location to start unpacking TLVs. However, the SCB redundancy structure's fixed components were not word aligned causing them to encroach on the space meant for the variable length TLVs denoted by startOfData[]. As a result, after switchover, an SCB corresponding to the session ID for the active call was not found on the new active SBC.	The variable length components/ TLVs of the Diameter session control block are both packed and unpacked respectively starting from the offset equal to the size of the fixed size components of the SCB. The fixed components of the SCB structure are now word aligned. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			Steps to Replicate: Configure a HA VNF/Hardware setup (or) N:1 SBC CNe setup with diameter Rx or diameter Rf. Wait for TCP connection to be established with the diameter peer. Make a long duration call. Perform switchover after mirroring is successful(sync/mirroring status is complete) After switchover, after the active call ends, observe that ACR STOP AVP(in Diameter Rf case) or STR AVP is not generated on the new active SBC.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129525	N/A	3	SBC sends acct remote rsyslog server connection traps from standby SBC. **Impact:** when SBC is configured to send ACT logs to rsyslog server. SBC standby was triggering "Connection issue" traps. **Root Cause:** There was no code to prevent standby from triggering connection checks. **Steps to Replicate:** - Install an SBC. example SBC 11.1.1R2. - Configure SBC acct typeAdmin remote rsyslog RELP server: set oam eventLog typeAdmin acct fileWriteMode optimize set oam eventLog typeAdmin acct servers server1 syslogRemoteHost <rsyslog-server-ip> syslogRemotePort <server-port> syslogRemoteProtocol relp set oam eventLog typeAdmin acct syslogState enabled commit The SBC will start reporting the following trap every 5 minutes: `144 12142023 163002.316422:1.02.00.00225.MAJOR .SBCINTF: Connection issue to remote server with IP: 10.220.152.120. Connection state: UNKNOWN`	Avoided standby triggering connection issue traps by first determining whether it is standby before using the connection check method. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129544	N/A	2	CDR fields: [STO 279] ingress mosCq1 and egress mosCq1 are not printing any value when RTCPOptions is enabled **Impact: The** SBC was printing incorrect values for MOSCQ parameters in CDR **Root Cause:** The MOSCQ values are derived from the inbound R-Factor of the media streams and the r-factor was not taken into consideration which was causing the problem **Steps to Replicate:** Following configurations needs to enable to get MOSCQ values in CDR 1. set global system rFactorComputation enabled 2. set global qoeCallRouting mediaQosBasedRouting enabled 3. Run a call with media streams sent from both directsions. 4. Terminate the call and check the STOP record in the CDR file. 5. The MOSCQ values will be printed in the range "0 - 5.0"	The MOSCQ values are now derived from R-FACTOR only and printed in the ACT file STOP RECORD **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129561	N/A	3	SBC sends false acct remote rsyslog server 'Connection issue' traps when there are no CDRs to stream. **Impact:** When the SBC is configured to send ACT logs to rsyslog server it could send false 'Connection issue to remote server' traps, even if there are no connection errors. This condition occurs notable where a remote rsyslog server is configured on the SBC, but there is no TCP connection established to the remote rsyslog server. **Root Cause:** This is traps are generated when there is no activity between server and SBC, SS command will be empty, so the system triggers a trap. **Steps to Replicate:** 1. Install an SBC. example SBC 11.1.1R2.	when SBC is configured to send ACT logs to rsyslog server. we stop sending connection error traps when previous state is connection is UKNOWN.. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. Configure SBC acct typeAdmin remote rsyslog RELP server: `set oam eventLog typeAdmin acct fileWriteMode optimize` `set oam eventLog typeAdmin acct servers server1 syslogRemoteHost <rsyslog-server-ip> syslogRemotePort <server-port> syslogRemoteProtocol relp` `set oam eventLog typeAdmin acct syslogState enabled commit` The SBC will report the following trap every 5 minutes: `144 12192023 144502.745516:1.01.00.00276.MAJOR .SBCINTF: Connection issue to remote server with IP: 10.220.152.120. Connection state: UNKNOWN`	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129769	N/A	2	D-SBC XML Export/Import: Cluster nodes Playback processing errors with Dynamic MetaVars configured **Impact:** SBC nodes went into bad state after configuration import. **Root Cause:** metaVariableDynamic Table contents are not being imported, but metaVariableDynamic Table references were imported in other tables which caused configuration validation failure. **Steps to Replicate:** 1) Configure metaVariableDynamic table contents and export the configuration. 2) Clear the DB in the cluster 3) Use the exported configuration to import config Expected output: after configuration import metaVaribaleDynamic table entries should be imported.	imported metaVariableDynamic table contents during EMA/CLI config import is triggered. **Workaround:** Configure metaVariableDynamic table values prior to import configuration.
SBX-130068	N/A	3	SBC7K: new PSU: OUTPUT LED does not turn on even when the power is connected **Impact:** BMC failed to enable power supply, power supply inserted but power cable is connected after 10 minute delay. **Root Cause:** When new PSUs, PSA and PSB are inserted on SBC7000 and the power is connected, the BMC cannot recognize the PSB if the power is not connected before 10 times of "Failed to get Model for PS". Since BMC cannot recognize PSB, it instructed PSB to provide the output. **Steps to Replicate:** Insert the power supply, do not connect the power cable for 10 minutes. The system will flag a fault power supply.	Increased time delay to ~30 minutes to enable power supply. **Workaround:** Connect the power cable within 10 minutes of power supply insertion.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130073	N/A	3	SBC7K: New PSU: PSU fail alarms raised **Impact:** SBC 7K New PS triggered false power supply failure alarm. **Root Cause:** The BMC randomly failed to read input power, then it triggers power supply is failed. **Steps to Replicate:** Run SBC 7K with new PS for few days to see false alarms.	Raise an alarm if it failed consistently. **Workaround:** None.
SBX-130266	SBX-129705 (10.1.5)	2	SBC is failing the call with 503 for a particular scenario when final answer (200 OK) was received **Impact:** SBC is failing the call with 503 for a particular scenario when final answer (200 OK) was received **Root Cause:** The SDP received in PRACK from UAC causing SBC to move the call state into connected. So, when the final answer 200 OK (for INV) is received from egress, SBC treats it as unexpected event and terminating the call by sending 501. **Steps to Replicate:** 1. Call flow involves tone with RTP monitoring on egress leg. 2. There is early media (a=sendonly) answer in 183 3. Followed by new offer from ingress in PRACK(a=recvonly) and 2xx for PRACK (a=sendonly) 4. Followed by 180 Ringing starting the tone 5. Followed by SIP UPDATE from egress to change codec from AMRWB to G711 and dpm to sendrecv. This UPDATE gets answered. 6. Followed by 2xx for INVITE from egress	A code fix so that the SDP received in PRACK from UAC doesn't move the call state into connected state until the final answer from egress is received. **Workaround:** Disabling IPSP flag "End-To-End Re-INV" can make the call scenario work fine.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130311	N/A	2	ERROR: AddressSanitizer: heap-use-after-free on address 0x606000260480 at CE_2N_Comp_EnmProcessMain **Impact:** AddressSanitizer: heap-use-after-free on address reported while processing event log validation hash files memory that was allocated and deallocated, and then accessed again, which is invalid. **Root Cause:** The information passed back from the boost::regex_match routine was thought to be a copy of the information passed. However, when the routine returned, the memory pointed to was released. **Steps to Replicate:** 1. Run an asan build. 2. Turn on eventLog validation for the accounting log. 3. Rollover the accounting logs server times. 4. Observe that an AddressSanitizer: heap-use-after-free on address is not seen.	A change was made to make a local copy of the information before calling the boost::regex_match, so that the memory would persist till the returned memory was used. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130419	N/A	3	SBC Oam fails to register due to configuration database is locked by session **Impact:** SBC standby OAM is stuck in partially registered due to configuration database is locked by session 47 system ssh **Root Cause:** The config play-back files tries to apply before the OAM standby completely gets up. **Steps to Replicate:** 1. Login to the EMS. 2. Create OAM SBC cluster(MSBC OAM) and spawn the SBC for the respective cluster. 3. Check whether both OAM nodes coming up and registers with EMS.	A marker file added to check whether the instanceUp done so that the pb files gets applied after that. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130425	SBX-129335 (10.1.6)	2	The SBC is stuck in a routing loop after 302 is received. **Impact:** The call is stuck in a routing loop in multiple 302 redirection call scenario when domain based routing is used. **Root Cause:** Issue is observed due to code change done as part of SBX-112167 (10.1.0). A condition was added to free Original Message Info from SIPSG call control block only when its a Local Redirection or Force Requery flag is set. During processing of second 302, Original Message Info is not freed which results in feeding of domain URI of first 302 from Original Message Info to SIPSG call control block and later to CC. CC feeds this incorrect domain as Input Data to ERE. As its a domain based routing ,this results in routing to same target again and again. **Steps to Replicate:**	Reverting the changes done in SipSgProcessCurrentContact() done earlier as part of SBX-112167. Instead, code checks if msgIndex is incremented/added. When SBX receives a new 3xx message, msgIndex is a positive value and it frees up Original message Info (containing domain uri from previous 3xx). **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			1. Make a Basic A - SBX - B call setup. 2. A calls B, B sends 302 with 4 contact headers. First Contact carries domain URI with FQDN. 3. Since Force requery flag is set at egress TG, SBX does a ERE dip to find the target address. 4. Then, SBC sends re-directed INVITE to Party C. 5. SBX receives 302 from Party C with single Contact header with domain uri with FQDN. 6. SBX does a ERE DIP to find out the target address again. 7. In ERE log, in the input Data, Host under Called URI is the domain fqdn uri from first contact header of first 302 message instead of the domain fqdn uri from contact header of second 302. 7. In ERE log, ERE does a domain based routing on this incorrect domain fqdn uri resulting in call going to same Target address and call goes in routing loop.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130427	N/A	3	SBC allows an operator to configure invalid static routes. **Impact:** Invalid inputs for mgmtStaticRoute table is being accepted by SBC **Root Cause:** There was no validation for the input present while configuring mgmtStaticRoute table **Steps to Replicate:** Test Case for Replication: 1. Bring up the SBC after basic configuration. 2. Check show table system mgmtStaticRoute: `0.0.0.0 0 10.52.10.1 mgmtGroup mgmtIntf1 10` 3. Configure an invalid IP Prefix combination for example: `set system mgmtStaticRoute 172.18.177.43 18 10.52.10.1 mgmtGroup mgmtIntf1 preference 10` 4. Check show table system mgmtStaticRoute: `0.0.0.0 0 10.52.10.1 mgmtGroup mgmtIntf1 10` `172.18.177.43 18 10.52.10.1 mgmtGroup mgmtIntf1 15` <- This is an invalid address that should not have been added into table.	Added the validation for the inputs IPAddress and the Prefix during configuration. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130520	SBX-130286 (11.1.2)	2	EMA elasticsearch - bug in the main script **Impact:** When elasticsearch is started directly from cli, it results in abnormal behavior. **Root Cause:** When elasticsearch is started directly from cli, it is started with root user which results in abnormal behavior. **Steps to Replicate:** 1. SSH to SBC as linuxadmin user. 2. Switch to root user. 3. Change directory to /opt/sonus/ema/MonitoringTools. 4. Run ./elasticsearch start. Elasticsearch should be started with sonusadmin user	Code changes have been made to always start elasticsearch with sonusadmin user even if root user is trying to start it. **Workaround:** None.
SBX-130586	SBX-129775 (12.1.1)	2	Cache Proxy, Redis Cache and RAC pods fail to come up due to issue while parsing the interfaceName in Customers K8S Environment **Impact:** Cache Proxy, Redis Cache and RAC pods fail to come up in customer's K8S environment **Root Cause:** Script used at startup failed to parse the eth0 IPv6 address correctly in customer's K8S Platform **Steps to Replicate:** Found during Sandbox testing.	Fixed containerUtils.sh file to parse eth0 IPv6 address in Customer's K8S Platform. Fixed Liveness and Readiness probe for Cache and Cache Proxy. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130762	N/A	2	CNe: Observing Call failures when SC is scaling down **Impact:** Calls are rejected by SC pod when the HPA scale down was issued. **Root Cause:** During SC was scaling down, it goes into the dry up state and any new calls in this state are getting rejected. **Steps to Replicate:** 1. Spawn initially 1 SC and let it scale up based on the load. 2. Initiate 120 cps with 100 CHT load 3. Reduce the load to scale down the SC.	Delay the SC pod dry up by 2 seconds, which makes the SC pod to take up calls up to 2 seconds and meantime inform SLB about SC pod is going down so that SLB will not pump any new calls. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130778	N/A	2	SWe SBC XRM congestion alarm **Impact:** For SBCs that were recently upgraded to 11.1.1R1, the XRM congestion alarm gets triggered at midnight almost every day. **Root Cause:** Starting SBC 11.0, Debian11 OS is in use and cgroupv2 is enabled by default in debian11. In this version systemd defaults to the "unified" cgroup hierarchy. However, the SBC doesn't require it and you can override this setting by passing grub kernel option: systemd.unified_cgroup_hierarchy=false. When performing an upgrade from pre-11.0 to 11.0+ in SWE, and after rebooting via initrd, the user enables grub settings, updates software, and so on. Because the system is already booted by this time, kernel options for the current boot will still be same as pre-11.0 and "systemd.unified_cgroup_hierarchy=false" could be missing in /proc/cmdline. This causes unified cgroup hierarchy to be 'on' after upgrade and causes missing cpuset files. **Steps to Replicate:** 1. Install SBC version 9.2.x. 2. Perform an upgrade to the fix version. 3. After upgrade when the SBC comes up, the cpusets files shouldn't be missing and /proc/cmdline should have "systemd.unified_cgroup_hierarchy=false" set for 11.0+ versions.	Changed the upgrade code to do the grub update before rebooting to make sure the proper kernel options are present on the first boot with the new software. **Workaround:** Do an additional reboot after the upgrade.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130844	SBX-126929 (10.1.4)	2	SBC EMA LI API - unexpected delay in operation **Impact:** Unexpected delay in LI operation when performed through EMA LI API **Root Cause:** For any LI request, there are three operations performed by the API. 1. Authenticating the user. 2. Retrieving SBC LI license. 3. Performing the LI operation. Operations 1 and 2 are time consuming causing overall run time of 3 to 5 seconds. **Steps to Replicate:** Perform any LI operation and it should take take less than 3 seconds.	The code is modified to optimize operations 1 and 2 such that overall time taken to perform LI operation is less than three seconds. Please note in a freshly installed SBC or if SBC is restarted, the very first LI operation will take around five seconds (before the fix it used to take around ten seconds or more). Subsequently it will take less than three seconds. **Workaround:** None.
SBX-130906	N/A	2	SIP Digest w/TLS feature fails as REGISTER message is rejected with 421 extension required **Impact**: The SBC rejects a REGISTER with 421 when the sIPsecurityProfile is enabled with IPsec-3gpp and TLS security mechanism. **Root Cause:** Previously, the SBC did not reject a register when the security mechanism was IPsec-3gpp. But when the security mechanism was TLS, the SBC rejected the register even when all required headers (require, proxy-require, security-client) were present. **Steps to Replicate:** Not applicable.	The code is modified to not reject the register even when security mechanism is TLS. **Workaround:** Disable rejectSecUnsupportedRequest on the SIP Security Profile.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130974	N/A	2	CNe: The ACT.OPEN file should be closed when receiving the TRUE pod 'down 'alarm, regardless of the CDR configs configured. **Impact**: The ACT.OPEN files were not renamed to ACT a podDown occurred and the CDR server was not configured. **Root Cause**: The closing files scenario was not handled when the cdrServer was not configured. **Steps to Replicate:** 1. Perform a rollover of the ACT files and make sure the ACT.OPEN files are present. 2. Delete the sc or rs pod whic had ACT.OPEN file. 3. Verify the .OPEN file is now closed.	The code is modified to handle the scenario of closing files if cdrServer was not configured. **Workaround:** None.
SBX-131220	SBX-130058 (11.1.2)	3	TLS handshake failing with an 'Unknown CA' error **Impact:** Add a configuration to allow unknown peer TLS server's Root-CA/self-signed certificates to be accepted without validation **Root Cause:** The SBC in a SIP-TLS client role always verifies the peer's certificate. **Steps to Replicate:** 1. Disable or delete Root-CA certificate used by the peer SIP-TLS server. 2. Set the new configuration parameter peerCertValidate to true (default value), and test SIP-TLS call toward TLS server. The TLS handshake will fail with Unknown CA error. 3. Set the new configuration parameter peerCertValidate to false, and test SIP-TLS call toward TLS server. The TLS handshake will succeed after accepting the TLS server's certificates without validation.	The code is modified to add a configuration object, peerCertValidate, to accept unknown peer TLS server's Root-CA/self-signed certificates that are accepted without validation. The following EMA and CLI pages are updated to include this new flag: • TLS Profile - CLI • Security Configuration - TLS Profile **Workaround:** Configure the valid peer TLS server's Root-CA/ self-signed certificates on the SBC in SIP-TLS client role.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131295	N/A	3	Set oamproxy container log level to default log level "major" if LOG_LEVEL environment variable is not present **Impact:** The oamproxy container is exiting if LOG_LEVEL environment variable is not present. **Root Cause:** The oamproxy container is exiting if LOG_LEVEL environment variable is not present. **Steps to Replicate:** 1. Remove the LOG_LEVEL environment variable for oamproxy container and spawn pods. 2. Check logs of oamproxy container(/var/log/ribbon/ startOamProxy.log) for logs and /var/log/ribbon/ OamProxy.log to see if "major" logs are logged.	The code is modified to set oamproxy container log level to default log level "major" if LOG_LEVEL environment variable is not present. **Workaround:** None.
SBX-131317	N/A	2	UUID and pod details are missing in the sonusSbxNodeResourcesCallTrace HitGAPNotificationCnf alarm in sonusSbxNodeResourcesCallTrace HitGAPNotificationCnf **Impact**: The trace-related traps missed the pod details and parameters. **Root Cause:** The code to fill the pod-related details in the API for trace traps was missing. **Steps to Replicate:** Configure the call trace filters and run a call matching the filter; the trap will be seen.	The code is modified to fill the pod related details in the API for trace traps. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131442	N/A	2	uFlowStats not getting deleted immediately in SLB after deregistration **Impact:** The Microflow states were not recreated on RS pod pod switchover **Root Cause:** The reconstruction for microflow maps post switchover was not implemented. **Steps to Replicate:** 1. Send register using an SBC CNe setup, microflow entry should be present in SLB. 2. Performed RS pod SWO. 3. Send Refresh registration with expiry 180. 4. After expiry, the microflow entry should be deleted from SLB.	The code is modified to recreate the Microflow states after RS switchover. **Workaround:** None.
SBX-131500	N/A	2	[CNe] : Alternate IP configuration for SLB PKT0 is not working. **Impact:** Alternate IP configuration for SLB PKT0 is not working **Root Cause:** Multicast IP support not present for secondary IPs **Steps to Replicate:** Ping the Gateway IP using the secondary IPs, should be pingable	The code is modified to add mMulticast IP support for secondary IPs **Workaround:** None.
SBX-131501	N/A	3	NRMA: Unexpected Msg Type 0x20028 **Impact:** NRMA logged "Unexpected Msg Type 0x20028" in DBG logs. **Root Cause:** 0x20028 is NRM_AFFECTED_CALL_LIST_NFY. This message is only valid for active NRMA to report affected calls to NRM. The unexpected message was logged only from standby slot because standby SBC does not process it. **Steps to Replicate:** On 1to1 redundant SBC, simulate unsolicited call cleanup, then check the DBG log for message 0x20028.	The code is modified ensuring the standby NRMA message processing routine skips NRM_AFFECTED_CALL_LIST_NFY. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131519	N/A	2	Core on SBC 7000 upgraded to 12.1.1R0, failed over this morning. **Impact:** SIPFE cored. **Root Cause:** SIPFE cored because it was attempting to deference a NULL pointer. The code was writing a debug message to the log when this happened. This bug is triggered by a race condition in which the Registration Control Block is no longer available when SIPFE is sending an outgoing message. **Steps to Replicate:** This bug is triggered by a race condition in which the Registration Control Block is no longer available when SIPFE is sending an outgoing message.	The code is modified to tweak the SIPFE code to prevent it from attempting to deference a NULL pointer. **Workaround:** None.
SBX-131528	N/A	3	ASM-SGP-SBC01A is unacessible, SBC showing Network Connection Refused Error **Impact:** SBC01A responding with Network Connection Refused Error. Actual problem was EnmProcessMain crashed and when failure was detected for Enm, a switchover was invoked. **Root Cause:** EnmProcessMain crashes have been seen to happen occasionally, especially when running in a virtual machine. These healthchecks can happen in Enm and cause it to crash when Enm is doing a lot of disk i/o writes. **Steps to Replicate:** System call "poll" is added before writing to disk in EnmProcess. It checks if the socket is writable, and only then writes. Otherwise, return an error message. This will Helmp with ENM getting stuck on a wait and eventually hitting the timeout event.	The code is modified to add a system called "poll" before writing the EnmProcess to the disk and remove the container check condition from evmFileCompression.cpp since this fix is applicable for all platforms. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131549	N/A	2	[CNe] Prs Process core is observed for isbc container of SC pod **Impact:** Prs process core observed. **Root Cause:** The error handling was missing during NSC-NS communication. NSC was not handling all the error sent from NS. **Steps to Replicate:** Not reproducible.	The code is modified to handle all possible error sent from the NS pod to the NSC. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131673	SBX-131419 (11.1.1)	2	Calls failing using Samsung after reinvite to UE **Impact:** SBC is not calculating the correct b=AS value and hence causing a re-INVITE **Root Cause:** SBC was incorrectly calculating the bandwidth value due to a defect in the code.	The code is modified to resolve a syntax error in the calculation for each encoding type. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			Steps to Replicate: Configuration: 1. Configure SBC to play tone 2. Configure Egress TG with downStreamForking enabled. 3. Configure both zones with dialogTransparency enabled. Procedure: ======== 1. Send INVITE from UAC with multiple codecs, with AMR/AMR-WB also in it. Send b=AS:41 in the SDP 2. Receive 183 w/SDP from UAS, with PCMA. 3. Receive 180 w/SDP from UAS, with PCMA. 4. Receive 200 OK w/SDP from UAS with PCMA. Expected: ======= 1. INVITE send out will have all transcodable and passthru codecs. b=AS will have the value of the codec with highest bandwith. 2. 183 received and will be processed to UAC. Towards Ingress AMR-WB will be selected. b=AS:41 will be added and sent towards UAC. 3. 180 received and will be processed to UAC. Towards Ingress AMR-WB will be selected. b=AS:41 will be added and sent towards UAC. 4. 200 received and will be processed to UAC. Towards Ingress AMR-WB will be selected. b=AS:41 will be added and sent towards UAC. No re-INVITE should be seen after this due to b=AS parameter	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131669	N/A	2	SIP ladder under CDR viewer is not working on SBC-A **Impact:** The SIP ladder under CDR viewer is not working. **Root Cause**: In the HA setup, when the SBC performs switchover, the maintenance task that monitors the size and duration of Elasticsearch data is not started. Due to this, Elasticsearch is not able to handle the increase in the size of the data/ number of indices, causing the garbage collector to run frequently and thereby resulting in performance degradation. Hence, the sip ladder is not displayed. **Steps to Replicate:** 1. Log into the Active SBC. 2. Enable CDR Viewer and SIP Ladder. 3. Wait until there is around 7GB of Elasticsearch data. 4. Perform a switchover. 5. Wait for a few hours. 6. Log into the switched-over SBC and navigate to CDR Viewer screen. The Sip Ladder icon should display and the ladder diagram should appear upon clicking the icon.	The code is modified to ensure that the maintenance task is started during switchover. **Workaround:** Disable and re-enable the CDR viewer after performing switchover.
SBX-131699	N/A	3	EMA 'Perform Pre-Upgrade Checks' does not show any output. **Impact:** Pre Upgrade check does not show any output **Root Cause:** To display the output of Pre Upgrade Check, Platform Manager reads preUpgradeCheck.log file. However Platform Manager tries to read this file even before it is generated, hence causing the issue **Steps to Replicate:** Login to Platform Manager Perform Pre Upgrade Check The check should be successful and the logs should be displayed.	The code is modified to read the preUpgradeCheck.log only if it exists. **Workaround:** Use the CLI to perform pre upgrade check and to view the output.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131722	SBX-131557 (11.1.1)	2	SBC 11.1.1R4 Originated call takes 7s to leave SBC to CORE when CLIR is enabled. (Issue 96) **Impact:** Originated call takes 7s to leave SBC to CORE when CLIR is enabled. **Root Cause:** SBC fails to find RCB for INVITE when it is received and indicates anonymous user. As a result it sends AAR to PCRF for the PLMN ID and waits and after 6 seconds timer expiry - the call will then proceed. **Steps to Replicate:** Make anonymous call and verify 7 second delay in sending out Invite.	The code is modified to fix the logic related to finding the RCB when the call is received from anonymous user. **Workaround:** None.
SBX-131723	SBX-131338 (11.1.1)	2	SBC send wrong Flow Identifier for RTCP towards PCRF **Impact:** Flow-Number AVP was not populated correctly for the RTCP during audio only and audio+video call. **Root Cause:** P-CSCF was populating same value in the Flow-Number AVP for both RTP and RTCP for audio only and audio+video call. **Steps to Replicate:** 1. Enable RTCP support in the SBC. 2. Enable UE and AS send RTCP information in the SDP. 3. Run basic audio or audio+video call with Rx feature enabled. 4. Verify Media-Component-Description AVP for the audio and video in the AAR messages.	The code is modified to populate the correct value in the Flow-Number AVP for the RTCP for audio only and audio+video call. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131778	SBX-131184 (11.1.1)	2	SBC does not terminate Registration when IMS-AKA timer expires and IMS-AKA connection is deleted **Impact:** SBC does not handle new registrations from UE properly if there is already a registration on SBC with pending state. **Root Cause:** SBC does not terminate registration when it does not receive a REGISTER request with credentials within 10 seconds **Steps to Replicate:** 1. Send initial REGISTER from UE but do not send REGISTER with credentials from UE after 401 response. 2. Send fresh registration from UE after 40 secs. 3. Check that SBC will not send integrity protected parameter in outgoing register.	The code is modified so that the registration is terminated if the SBC does not receive a REGISTER request with credentials within ten seconds. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131841	SBX-131329 (10.1.6)	2	Alarm "sonusSbxNodeResourcesNoPacketsReceivedNotification" generated incorrectly in call hold **Impact:** During call hold, SBC wrongly generates NRMA media inactivity SNMP trap at the recvonly side. **Root Cause:** SBC generates NRMA media inactivity SNMP trap without validating whether its a sendonly or recvonly side. It only validates peerAbsenceAction and if it is set and media inactivity is detected by SBC after media inactivity timer expiry, it generates NRMA trap at the respective side. **Steps to Replicate:** 1. Setup: A --> SBC --> B. 2. Set mediaPeerInactivity inactivityTimeout to 20 secs. At Egress PSP, enable RTCP and peerAbsenceAction to peerAbsenceTrapAndDisconnect. 3. Party A calls Party B. Call is established. Party A puts the call on hold by sending a=sendonly. Party B responds with a=recvonly. 4. Call is put on hold for 1 min. 5. After call hold, call is completed gracefully. 6. NRMA media inactivity SNMP trap is generated by SBC after media inactivity timeout at recvonly (Party B) side. 7. SBC also prints NrmaPeerLossTrapGenerate() logs in info level dbg log.	The code is modified to add a condition for data path mode such that the NRMA peer loss trap is not generated at the recvonly side in a call hold scenario. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131842	SBX-131038 (10.1.6)	3	SBC is responding OPTIONS with 503 in specific condition with sips in CONTACT header **Impact:** SBC responds with 503 response to OPTIONS with SIPS URI in Contact header always during Dryup. **Root Cause:** For any request message where incoming request message is rejected due to dryup, request message is not pre-parsed and rejected, error response message always carries SIPS URI by default in Contact header. **Steps to Replicate:** 1. SIPp -> SBC -> SIPp Basic call setup 2. Run set command "set global system mode outOfService action dryUp dryUpTimeout 15" 3. Send OPTIONS message from Client side. 4. SBC rejects OPTIONS with 503 error with SIPS URI in Contact header	The code is modified to prevent the SBC from sending any Contact header in the error response when the incoming request message is rejected due to dryup. The Contact header is not sent because the RURI of the request message is not all parsed. **Workaround:** None.
SBX-131851	SBX-131513	2	After 11.1.1R3 to R4 upgrade reboots are seen, the EMA is not accessible and some CLI commands time out. **Impact:** After upgrading from 11.1.3R3 to a later version, CLI commands are getting stuck. **Root Cause:** SmProcess which is responsible for handling for some CLI commands was not responding as it was stuck. This was since a database commit API which was being run within a overridehealthcheck block was not responding. **Steps to Replicate:** None, its a rare issue which cannot be reproduced easily.	The code is modified to remove the override healthcheck for the database commit API, ensuring the SmProcess recovers. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131869	SBX-131573 (11.1.2)	3	Core SWe - OPTIONS crankback using wrong SIP sig port **Impact:** When the Primary egress peer doesn't respond and SBC sends to the secondary peer, it uses the same sport even when the secondary peer is in a different zone. **Root Cause:** After a crankback when the SBC finds the next route and then selects the tranport and sigport options, it is not checking for the correct sigport. The SBC just passes the same sigport used for the primary peer to select the transport and siport. **Steps to Replicate:** 1. Configure two IP peers in two different zones. Add these 2 IP peers to your routing label. 2. Send OPTIONS request from client script. 3. Run the server script for only the secondary peer. Without the fix: The SBC sends egress OPTIONS to the second peer with the same sigport used for the primary peer. With the fix: The SBC sends egress OPTIONS to the correctly configured sigport for the secondary peer.	The code is modified to fill pstRelayCb->usEgressSigPortId to 0 upon successfully finding a new route on crankbank so that when the function SipSgSelectTransportAndSigPort() is called, the SBC fills in sigport appropriately. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131913	SBX-128330 (10.1.6)	3	No audio after switching from direct media DM+ICE to pass-through **Impact:** No audio after switching from direct media DM+ICE to pass-through **Root Cause:** 1. the previous ICE media info was not cleared properly when switching 2. the ICE flags were not cleared when peer is ICE-lite. **Steps to Replicate:** With the correct configuration to make a direct media DM+ICE call: 1. Switch from direct media DM+ICE to pass-through call. 2. Switch from pass-through back to direct media DM+ICE call Ensure audio works in both cases.	The code is modified to resolve the issues with tjhe NRMA code. **Workaround:** None.

Resolved Issues in 12.01.01R001 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130397	N/A	1	Naming nomenclature for configMap and Service **Impact:** The customer requested a specific naming convention for configMap and Services, which was created as part of SBC CNe deployment. **Root Cause:** As part of SBC CNe deployment, the configMap and Services created by the SBC CNe have the deployment name prefixed before the configmap and service name, which is not compliant with the customer's naming nomenclature. **Steps to Replicate:** 1. Populate the configMap and the Service name in the values.yaml according to the customer's naming nomenclature. 2. Deploy the SBC CNe in the customer's cluster. 3. The configMap and Service deployed in the cluster should successfully deploy with the naming nomenclature recommended by the customer.	The code is modified to introduce the configmap and service naming nomenclature as part of the values.yaml file. Before deploying the SBC CNe, the user should populate the configmap and service names in the values.yaml file. **Workaround:** None.
SBX-131193	N/A	1	Include eth0 customer K8S platform-specific annotations for OAM pods **Impact:** The SBC CNe OAM Pod fails to identify the peer instance on the customer's platform. **Root Cause:** The network annotation parsing logic in the OAM doesn't account for the change in the network annotation obtained in a customer's platform concerning the eth0 interface after discovering the peer. **Steps to Replicate:** 1. Launch the SBC CNe on the platform without the changes. 2. The OAM standby pod fails to come up with its assigned role. The OAM standby pod is stuck in the peer-resolving operation. 3. With the fix, the OAM standby pod creates the assigned role and syncs with the active.	The code is modified to change the network annotation parsing logic to account for the pattern observed in the customer's platform. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131247	N/A	1	Remove the Virtual Memory (VM) related kernel parameters for SBC CNe solution **Impact:** In the customer's platform, there are a few Virtual Memory Kernel parameters (e.g., dirty_ratio, dirty_writeback_centisecs) that were set by the team with some values based on the type of disk attached to the Baremetal worker nodes. The Virtual Memory Kernel parameters are overwritten when the SBC CNe application is deployed. **Root Cause:** When the SBC CNe is deployed as part of the SBC application, the VM kernel parameters are overwritten. Because the VM kernel parameters are overwritten, the SBC slows down the disk read/write operation (IOPS), and the worker node goes into a NotReady state, evading the SBC CNe pods. **Steps to Replicate:** 1. Deploy the SBC CNe. 2. Make sure all the pods are up and running. 3. The pods should not terminate because Worker Nodes are entering the NotReady state (because of the Disk IOPS issue).	The code is modified to remove the VM parameter settings from the SBC CNe application code. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131257	N/A	1	SG, SLB, and SC containers (primarily the standby containers) are not in a Ready state while using eth0 IPv6 for interpod communication **Impact:** In the customer's platform, when eth0 is used as the interpod communication interface and the IP Address is set to v6, the communication between SC-SLB, Active & Standby SGs, Active & Standby SLBs, SC/SLB/SG/CS (oamproxy container)-OAM container is not successful. **Root Cause:** In the customer's platform, for the eth0 interface (the default interface), the network annotation does not have the interface name in it. The network annotation has the IP address and default parameter (with an accurate value). Since the SBC application is looking for an interface parameter while parsing the network annotation, the parsing fails, and the IP address is not returned. This results in the interpod communication failure. **Steps to Replicate:** 1. Bring up the SBC CNe with the interpod communication interface set to "eth0". 2. All the pods should come up running, and also the overall SBC CNe health status should display as "Healthy."	The code is modified to add conditions to check for the default parameter (and its value) along with the interpod communication value (eth0). If these conditions are met, the IP Address is fetched from the network annotation. Since the IP address was successfully fetched, the interpod communication worked fine. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131354	N/A	1	PCI Device environment variable parsing failure for PKT interfaces **Impact:** The PCI devices are incorrectly mapped to the PKT interfaces on the customer's platform, resulting in failure to communicate with the elements of the corresponding VLAN networks. **Root Cause:** Although the customer's platform provides an environment variable having PCIDEVICE_ as the prefix with the PCI slot addresses, this env variable does not guarantee the order in which the application uses the PCI devices, neither does it give the information about the interface (pkt0/pkt1) the PCI devices are allocated to. **Steps to Replicate:** 1. Launch the SBC CNe solution with port-redundancy enabled for pkt interface. 2. Verify the PCI device allocation to the PKT interface using the following commands: env | grep PCIDEVICE env | grep PCI_ADDR cat /opt/sonus/conf/swe/.port_map.txt 3. Please observe that the mapping for the pkt0p, pkt0s, pkt1p, and pkt1s are incorrect in their corresponding PCI slot IDs. With the fix, the output of the same command set mentioned above gives accurate mapping information.	The code is modified to use the customer's specific annotations rather than the PCIDEVICE environment variable, which is a standard across Kubernetes platforms, to parse the PCI slot IDs on the sriov interfaces. **Workaround:** None.

The following severity 2-4 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129775	N/A	2	Cache Proxy, Redis Cache, and RAC pods fail to come up due to an issue while parsing the interfaceName in the customer platform. **Impact:** In the customer's platform, when eth0 is used as the interpod communication interface and IP Address is set to v6, the Cache Proxy, Redis Cache, and the pods fail to come up. **Root Cause:** In the customer's platform, the network annotation does not include the interface name for the default eth0 interface. Instead, it only contains the IP address and default parameter (with a value of 'true'). Since the SBC application is looking for an interface parameter while parsing the network annotation, the parsing fails, and the IP address is not returned. Due to this, the Cache Proxy, Redis Cache, and RAC pods fail to come up. **Steps to Replicate:** 1. Bring up the SBC CNe with the interpod communication interface set to "eth0". 2. All the pods should come up running, and the overall SBC CNe health status should display as "Healthy."	The code is modified to add conditions to check for the default parameter (and its value) and the interpod communication value (eth0). The IP Address is fetched from the network-annotation if these conditions are met. Since the IP address was successfully fetched, the interpod communication worked as expected. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131216	N/A	2	Incorporate all PVC YAML with customer-specific annotations **Impact:** In the customer's platform, certain parameters are requested as part of the annotation: faultdomain: host, media: SSD, replication: 3. The above annotations are needed primarily in the customer's Staging and Production environment. **Root Cause:** In the customer's platform, the following parameters are added to the annotation: faultdomain: host, media: SSD, replication: 3. **Steps to Replicate:** Add the following annotations in the PVCs and make sure the PVCs are created successfully: faultdomain: host, media: SSD, replication: 3.	The code is modified to add the following parameters to the annontations: faultdomain: host, media: SSD, replication: 3. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-131246	N/A	2	Service Account Name is not populated in the HPA Deployment. **Impact:** Ribbon HPA is one of the microservices in the SBC CNe deployment. Its functionality is to support the autoscaling of the SC pods. The service account was set to default. If a non-default service account was configured for the SBC CNe deployment, HPA continued to use a default service account for any Kube API queries. This resulted in the Kube API queries failing and the HPA functionality not working as expected (i.e., autoscaling functionality). **Root Cause:** The HPA deployment's service account was set to default. If a non-default service account was configured for the SBC CNe deployment, The HPA continued to use the default service account for any Kube API queries. This resulted in the Kube API queries failing, and the HPA functionality (i.e., autoscaling functionality) was not working as expected. **Steps to Replicate:** 1. Deploy the SBC CNe with a non-default service account. 2. Check the HPA behavior when the service account was set as default (Kube API query should fail). 3. Update the HPA deployment to include the service account field explicitly. 4. Perform some Kube API queries and make sure that they are successful.	The code is modified to add the service account to the HPA deployment. Whenever the Kube API query is performed, the service account configured in HPA deployment is considered instead of the default service account. This resulted in the Kube API query to succeed. **Workaround:** None.

Resolved Issues in 12.01.01R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-124236	N/A	1	SamP process cores during bulk provisioning of an IP Address on a SBC 5400 for system limit check **Impact:** Configuring full range IP and port combination leads to a Process core. **Root Cause:** A combination of the full range IP and ports were consuming more memory that leads the system to an OOM state and a core. **Steps to Replicate:** Configure full range ports and alt media IPS.	The code is modified to limit the number of configured IP and ports so that system will not lead to an OOM. **Workaround:** Do not configure full range alt media IP and ports.
SBX-127165	N/A	1	Socket Creation Errors **Impact:** The SBC failed to create a socket. **Root Cause:** There is no retry mechanism for socket binding if it has failed. **Steps to Replicate:** 1. Configure single/multiple protocols in CLI. 2. Verify that if socket creation fails, the retry mechanism changes will work and that socket creation is tried again. 3. Also test by changing the SigPort state/ mode and LIF state/mode to disabled and outofService.	The code is modified enabling SIPCM to retry socket creation in case of failure. **Workaround:** None.
SBX-129635	N/A	1	No sig port to match transports 0;0;0;0 error is seen after CS SWO **Impact:** The SBC is not able to send an options msg out since the CS POD is not able to find the SIP signaling port **Root Cause:** The CS pod is not able to retrieve the signaling port config from the configuration **Steps to Replicate:** 1. Configure a peer with hostName. 2. Attach the pathchk profile. 3. The SBC will not respond to the options and all the peers are blacklisted. 4. SC & RS receive the blacklisted entries (the DB cache had the blacklsited keys) 5. Perform a CS SWO. With fix: options go out. Without fix: options do not go out.	The code is modified to remove the CS POD check from configuration which prohibits the SIP signaling information retrieval in the CS pod. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130118	N/A	1	Observed MAJOR logs "*MrmConnDeletedNfy: ResId is invalid for socket 31399. Not sending delete nfy" are flooded and switchover is observed on MSBC on build 12.1.1-86 **Impact:** Major logs are flooded in the MRM. **Root Cause:** If the BYE comes first before the MRM connection closes, it will clear the mres, causing the Mrm connection to not find the resource while deleting and printing the Major logs. **Steps to Replicate:** 1. Run a basic MSRP call. 2. UE should send BYE first before closing TCP connection.	The code is modified to add a check that sends "deleteNfy" to the Main only when the mres is valid. **Workaround:** None.
SBX-130573	SBX-130506 (10.1.6)	1	SBC is not able to send responses to reInvite/ Update request where the via ip/port from the request does not match the one from the wire. **Impact:** The SBC is not able to send a response message to a reInvite or Update when the packet received contains a VIA and the IP Port does not match that from the wire. **Root Cause:** The SBC finds the connectionId in local cache based on the source IP/Port from the wire, but then invalidates it when VIA Ip/Port does not match. It then tries to create a new connection to the IP/Port in the via to send the response. The message never gets to the right client, or the open request fails all together depending on protocol used. **Steps to Replicate:** Make a call and after call connect, the Egress sends a reinvite or Update to the SBC with different VIA IP/Port.	The code is modified allowing response messages to not need to have their source IP/Port compared against the sourceIP in the VIA and should just get sent on the same connectionId the request was received on. **Workaround:** None.
SBX-130669	N/A	1	Observed CcsP Core while running IMS-AKA load on SLB **Impact:** The CCS process cores in an IMS-AKA load run. **Root Cause:** The socket connect blocked the call, which led to a healthcheck failure and core. **Steps to Replicate:** Not applicable.	The code is modified to prevent the socket connect from blocking the call. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130994	N/A	1	The SBC discards SRTP packets as "authorization failure" after upgrading to 12.1.0R0 **Impact:** The SBC discards the SRTP packets as a "authorization failure" after an upgrade to 12.1.0R0 when (S)RTCP is enabled. **Root Cause:** The SBC NP Media flow SRTP decryption context gets overwritten by the SRTCP context due to a small oversight in how the dec_type handles the NP API for SRTP/ SRTCP. This was introduced from a new 12.1 feature. **Steps to Replicate:** Validate the SRTP media with PSP enabled (S)RTCP.	The code is modified to correct NP API handling for the updated dec_type fields to create valid SRTP and SRTCP decryption contexts to process the media. **Workaround:** Disable RTCP.

The following severity 2-4 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127741	N/A	2	FQDN not getting deleted from RS & SC from blacklisted entries **Impact:** The FQDN is not getting deleted from RS and SC when the disables pathcheck. **Root Cause:** The SBC is missing a hostname field in the recovery structure passed when it disables pathcheck. **Steps to Replicate:** 1. Configure a FQDN pathcheck profile. 2. Peers get blacklisted. 3. Disable pathcheck profile. 4. Check if the hostname is getting cleared on the RS and SC pods.	The code is modified to add the missing field and populate it with the correct value on the CS pod as well as retrieve the value and delete the hostname on the RS / SC pods. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128078	N/A	2	Domain name not getting listed as a blacklisted entry after pod deletion **Impact:** A domain name is not getting listed as a blacklisted entry after pod deletion. **Root Cause:** The FQDN entry was not sent by the CS Pod to SC /RS whenever the SBC syncs the blacklisted entries after the deletion of the pod. Hence, the SBC sends only the blacklisted IP. **Steps to Replicate:** 1. Configure the pathChk profile and attach it to the UAS. 2. Configure the DNS server to return two IPs. 3. Upon not receiving any response, the IPs and domain name are blacklisted. 4. Delete the SC/RS pod and see if it comes up with a domain name.	The code is modified to send the FQDN entry whenever the SBC syncs the blacklisted entries after pod deletion or pod restart. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128227	SBX-127878 (10.1.6)	2	minimizeRelayingOfMediaChanges FromOtherCallLegAll does not suppress certain re-INVITE messages from MS Teams after an upgrade from 10.1.1R3 to 11.1.1R0 **Impact:** In an RTP/AVP to SRTP/ SAVP call, if the egress peer updates the a=crypto SDP attribute by sending its new value in a re-INVITE, the SBC may send an unnecessary re-INVITE to the ingress peer although the minimizeRelayingOfMediaChanges FromOtherCallLegAll flag is enabled. **Root Cause:** The egress SG relays the new crypto attribute to the ingress SG. However, the ingress side is using RTP/AVP and therefore the SRTP crypto attributes are meaningless for the ingress side. The ingress SG is missing logic to suppress the re-INVITE. **Steps to Replicate:** 1. Set up a RTP/AVP to SRTP/ SAVP call flow. 2. Enable the minimizeRelayingOfMediaChan gesFromOtherCallLegAll flag on the ingress IP signaling profile. 3. Once the call is connected, let the egress peer send a re-INVITE with a modified a=crypto attribute. 4. The SBC will relay the media change to the ingress call leg and the SBC may send the re-INVITE out to the ingress peer.	The code is modified to add logic to prevent the SBC from sending the re-INVITE to the RTP/AVP call leg since the crypto attributes are meaningless for the RTP/AVP call leg. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128297	N/A	2	SBC cores while executing reset password curl command with response 500 Internal error **Impact:** The SBC Core was observed while running an action command to reset password. **Root Cause:** The issue was seen in the symlink handler code while processing the action command which would internally trigger an operational data. As the handler for action and operational data was same, it gets stuck in deadlock. **Steps to Replicate:** Tested the reset password request.	The code is modified to add a new thread to handle the action command requests under the symlink level. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128408	N/A	2	D-SBC XML Export/Import: Active OAM fails to send initial imported config & subsequent config changes to all cluster nodes **Impact:** The config import fails on the standby OAM and managed nodes, leading to subsequent config failures on these nodes. **Root Cause:** While applying the config /snmp/localEngineId on the active OAM node, the application callback function internally updates all the local references to localEngineId for other tables, which makes it way to the playback file used to replicate the config on the standby OAM/managed nodes. While replaying the pb files on those nodes, the callback function failed the validation when setting the localEngineId to the referenced tables due to incorrect logic. **Steps to Replicate:** 1. Export the config from the active OAM. Ensure that the /snmp/localEngineId in the cdb is different from the value in the seeded data file(/opt/sonus/sbx/tailf/var/confd/cdb/sonusSnmp.xml) This can happen for two cases: i) The system comes up with a config backup (which already has localEngineId config present), and then the config is exported from this system. ii) In a switchover scenario, wherein the export is taken from a peer box which has joined the cluster as a standby during installation. 2. Use this config to import on the new cluster, and validate that the config is applied successfully on all of the nodes.	The code is modified to validate if the new localEngineId is present in the db (for reference tables) before making any modifications; if the entry already exists, the SBC will pass the validation. **Workaround:** Remove the localEngineId config from the exported xml file before importing the xml file.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128416	N/A	2	SBC is not sending MESSAGE to UAS **Impact:** The SBC is unable to send MESSAGE to the egress leg because of a SCM Process core. **Root Cause:** The SBC was trying to access a pointer which was NULL. **Steps to Replicate:** Not applicable.	The code is modified to check if the pointer is NULL before accessing. **Workaround:** None.
SBX-128531	N/A	3	The SBC kept switching over **Impact:** Confd is crashing intermittently which cause the SBC to switchover. **Root Cause:** The customer set the SNMP version to v3, but did not set the authKey and privKeys; hence, SNMPv3 authentication failed while sending traps to the configured targets. The frequently occurring traps overloaded confd and it eventually crashed. **Steps to Replicate:** 1. Configure the SNMP users. 2. Set the SNMP securityLevel to authPriv/authNoPriv. 3. Set SNMP version to v3. Expectation: the system should fail the configuration as the snmp user's authKeys and privKeys are set as per the securityLevel.	The code is modified to add validations to make sure user's authKeys and privKeys are configured as per the securityLevel (authPriv, authNoPriv) when the SNMP version is set to v3. **Workaround:** Configure authKeys and PrivKeys for all SNMP users as per the securityLevel (authPriv or authNoPriv) if the SNMP version is v3.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128710	SBX-127682 (11.1.2)	3	Core generated on Server **Impact:** The CPX process goes down while processing a snmp bulk get request for global/system/nodeStatus (with default max-repetitions=10). **Root Cause:** The status response generated by the application contained incorrect data for one of the columns, leading to confd going down. **Steps to Replicate:** Tested the snmp bulk get command with ongoing calls on the system: snmpbulkget -c admin -t 10 -v 2c <SBC_ip> 1.2.3.4.5.6.7891.2.34.5.678	The code is modified to send back an empty response for call related status commands when no applicable data is present. As well, the code now hides the CNe related callStatus commands for non-CNe deployments for other northbound interfaces such as restconf, snmp, etc. **Workaround:** Recommend executing the get-bulk-request for global/system/nodeStatus with max-repetitions=3 (as there are 3 non-key fields in this list). Sample snmp command for nodeStatus with max-repetitions=3 : "snmpbulkget -c admin -C r3 -t 10 -v 2c <SBC_ip> 1.3.6.1.4.1.2879.2.10.3.114")

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128978	SBX-107984 (9.2.x)	2	The SMM adds extra CRLF at the end of SDP causing issue at remote **Impact:** The SMM adds extra CRLF at the end of SDP post SDP manipulation. **Root Cause:** The CRLF is getting added for each and every line of SDP when reformatting regardless of last line **Steps to Replicate:** 1. Configure the SBC for an A to B call. 2. Configure the SMM to modify the SDP and apply outputAdaptorProfile on egress TG or inputAdaptorProfile on Ingress TG. 3. Make a call with Invite SDP containing all parameters mentioned in SMM file criteria: sample SMM modify used to reproduce: rule 1 action 1 type sdpContent rule 1 action 1 operation delete rule 1 action 1 sdpContentSubType codecByName rule 1 action 1 from type value rule 1 action 1 from value "G722/8000" rule 1 action 1 to type sdpContent rule 1 action 1 to sdpContent streamType audio rule 1 action 1 to sdpContent streamInstanceId all 4. Contact TAC for more info if unable to reproduce.	The code is modified to add a check for the last line of the SDP to prevent the SMM from adding a CRLF at the end. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128987	SBX-127742 (10.1.6)	3	SBC sending SIPREC Re-Invite towards recording server without Multipart intermittently **Impact:** Metadata is missing in recording of the re-INVITE. **Root Cause:** Issue happens due to the timing of the SBC sending the ACK. If the SBC sends re-INVITE for the recording before the SBC sends out ACK towards the recording server, the SBC sees it is still not in the Connected state as ACK is not sent and does not send re-INVITE and instead sends BYE to the recording server. The working case is that the SBC is hitting a function to send re-INVITE for recording after it had sent out ACK. So, it is in CONNECTED state and able to send re-INVITE with metadata successfully. **Steps to Replicate:** 1. Configure the SBC with an example config. 2. The SBC should send an INVITE to recording server after receiving 183 with sdp. 3. The SBC sends re-INVITE to recording server once it receives 200 OK of INVITE from the Server and sends 200 OK to the client. 4. This is a timing issue. The SBC should start processing re-INVITE to recording server before it sends out ACK for initial INVITE. Without fix: The sent out re-INVITE does not have metadata. With fix: The re-INVITE has metadata.	The code is modified to update the sipRecflags to queue the re-INVITE upon getting the status "SIP_STATUS_REQUEST_PENDING" from the function. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129033	SBX-128548 (10.1.6)	3	An Incorrect Value is getting populated in CDR when PAI header contains Tel URI where display name contains a COMMA **Impact:** The SBC does not escape the COMMA present in the display name of PAI header containing a Tel URI. **Root Cause:** The code is not present to escape COMMA present in the display name of PAI header containing Tel URI. This results in an incorrect value getting populated in CDR sub-field 12 and the same incorrect value is overwritten in the next sub-field 13. **Steps to Replicate:** 1. Make a basic SIP call with the PAI header in INVITE listed below: P-Asserted-Identity: "Lamoda, Test" <tel: +1234567890;cpc=ordinary> 2. Send a 486 error response from server script. 3. Verify the ATTEMPT CDR field "Displayname of Tel URI PAI header" is properly updated with first 11 characters of display name. COMMA replaced with %2C. %2C is considered as single character.	The code is modified to convert COMMA with %2C. The %2C is considered as 1 character. **Workaround:** SMM rule to delete COMMA from Display name of PAI Header.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129074	SBX-123582 (10.1.1)	2	MRFP rejects the call with "Error=411" when the MOD message includes "CALLTRACE/TRACEACTIVITYREQUEST=ON" **Impact:** A call setup fails when the calltrace is turned on by customer for the call. **Root Cause:** When the customer sends ADD termination commands to MRFP with "CALLTRACE/TRACEACTIVITYREQUEST=ON", the MRFP sends ADD reply and then sends NOTIFY with calltrace status back to the customer. Sometimes, the ADD reply and NOTIFY reach the customer out of order. When the customer receives NOTIFY first, they could not locate the call context and trigger sending the SUBTRACT terminations command to delete the context/terminations in MRFP for the call. When the customer receives a re-INVITE, they send MODIFY termination commands to MRFP, but MRFP rejects the MODIFY commands with "Error=411, "The transaction refers to an unknown ContextID" since the context/terminations have been deleted already. **Steps to Replicate:** 1. Start a single call trace with Trace Scope of New call only. 2. Establish a 3pcc call matching the trigger condition of the single call trace. 3. MRFP rejects the call when the customer sends MOD message.	The code is modified to add a delay of 20ms for sending the NOTIFY calltrace status after ADD reply is sent in MRFP. This would make the customer receive the NOTIFY later than the ADD reply, such that when handling NOTIFY of calltrace status, the customer can correctly locate the call context/terminations. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129075	SBX-125866 (10.1.1)	2	RTP inactivity detection fails after switchover **Impact:** In a call hold/resume scenario, the MRFP stops RTP inactivity detection when the call is resumed after switch-over. **Root Cause:** An internal ID maintained in the resource manager module was changed from 0 to 1 upon switchover that caused the function to wrongly treat the call as in tone playing, and thus stopped RTP inactivity detection. **Steps to Replicate:** 1. Create a call and put it on hold. 2. Perform a switch-over. 3. Resume the call after switch-over.	The code is modified to fix the bug in the call redundant recovery function to keep the internal ID 0. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129076	SBX-127088 (12.0.0)	2	Call gets dropped after switchover **Impact:** A connected call can sometimes be dropped by the customer after a switchover occurred on MRFP. **Root Cause:** During the switch-over on MRFP, the new Active node will re-register with the customer by sending the customer a Service Change request with reason "Service Restore" for max number of tries = 2. Sometimes, due to the MRFP lower layer readiness for sending out or receive network packets to/from the customer, MRFP H248 stack may not receive the Service Request response, it start sending the Service Request with reason "Cold Boot". But once the customer receives the Service Request with reason "Cold Boot", by design, the customer treated the MRFP as a newly started node and started procedure to delete all the calls that's associated with the MRFP node. **Steps to Replicate:** 1. Create a call on MRFP. 2. Perform a switch over operation on MRFP. 3. Verify the call won't be dropped by the customer after the MRFP switch over.	The code is modified to increase the max number of registration retries from 2 to 10, which resolves the latency of the lower layer getting ready for send/ receive h248 messages and guarantees the successful registration with the customer with the correct Service Change reason code - "Service Restored". **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129178	N/A	2	IPsec SADB_ACQUIRE is selecting an incorrect ipv6 address when different IPs are used for ipInterfaceGroup and SipSignalingPort **Impact:** The SBC may select incorrect IPv6 addresses when an interface has multiple IPv6 addresses that can reach the IKE peer. **Root Cause:** The interface with IPsec-enabled has a IPv6 SIP signaling address different from the IPv6 address for IKE negotiation. IKE packets use an incorrect IPv6 SIP signaling address for IKE negotiation, causing the IKE negotiation to fail. **Steps to Replicate:** Reproduce the issue: 1. Configure multiple IPv6 SIP signaling addresses on an IPsec-enabled interface. 2. Observe that SBC selects an incorrect source IPv6 address in SADB_ACQUIRE when the packet was sent from the SBC towards IPsec/IKE remote peer. Test the fix: 1. Configure multiple IPv6 SIP signaling addresses on an IPsec-enabled interface. 2. Observe that SBC selects an incorrect source IPv6 address in SADB_ACQUIRE when the packet was sent from the SBC towards IPsec/IKE remote peer. Observe that IPsec tunnel was properly established.	The code is modified to filter out the signaling IPv6 address for the IKE source IPv6 address selection. **Workaround:** Configure an IPv6 SIP signaling address that is the same as the interface's address on an IPsec-enabled interface. At most, one IPv6 SIP signaling address is configured on the interface.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129201	SBX-129127 (10.1.6)	3	SBC User was created by system automatically (without clicking create user TAB) with dummy name **Impact:** An SBC User was created by the system automatically (without clicking create user TAB) with a dummy name. **Root Cause:** In the User Management screen of the EMA, when the Save button is clicked after editing user details, the UI does a base64 encoding of the username and sends it to the backend for updating of the user details. When the Save button is clicked again, the UI again encodes the username which is already encoded in base64 and sends it to the backend. The backend considers it as a new user creation request and ends up creating a new user. **Steps to Replicate:** 1. Log into EMA. 2. Navigate to User Management screen. 3. Edit user details and click submit button multiple times. 4. The dummy user should not get created.	The code is modified to prevent the re-encoding of the username. **Workaround:** Update the user details through the CLI.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129204	SBX-127080 (10.1.6)	3	The SMM RegEx displays incorrectly in EMA when using special characters **Impact:** Regex in SMM are not displayed correctly in the EMA. **Root Cause:** The special characters >, < and & were not encoded and decoded properly, causing them to display incorrectly in EMA. **Steps to Replicate:** 1. Through the CLI, create a SMM with regex for example <sip;><smm>. 2. Log into the EMA and navigate to SIP Adaptor Profile screen. 3. Regex <sip;><smm> should display as it is. 4. Update regex to for example <sip>;<sip;><smm>. 5. The update should succeed.	The code is modified to encode and decode >, < and & special characters. **Workaround:** Update SMM regex through the CLI.
SBX-129207	SBX-128766 (10.1.6)	3	Incomplete output from SBC GUI SMM 'View CLI' option **Impact:** The following value is not completely shown from SBC GUI SMM 'View CLI' option <sip: +112233445566@123.456.789.10:2345>;reason=unknown;privacy=off" **Root Cause:** The parsing logic to construct cli command ignored text after >; hence incomplete output is shown. **Steps to Replicate:** 1. Log into the EMA and navigate to the SMM screen. 2. Create a SMM with value <sip:+112233445566@123.456.789.10:2345>;reason=unknown;privacy=off". 3. Click the View CLI button. 4. The complete value should be shown.	The code is modified to fix the parsing logic **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129283	N/A	2	RTCP disabled when b=RS:0 but b=RR: non-zero **Impact:** The SBC disables RTCP when either of the bandwidth modifiers RS or RR are set to zero. **Root Cause:** Due to incorrect logical operators, the SBC disables RTCP when either of the bandwidth modifiers RS or RR are set to zero. **Steps to Replicate:** 1. Make a Basic SIP-SIP call setup. 2. Set PSP flags "enableRTCPForHelmdCalls" and "rtcp" to Enabled. 3. Send an initial INVITE with b=RS:2500 and b=RR:2500 in the SDP. 4. Send a re-INVITE for call hold with b=RS:0 and b=RR:2500 from the client side. 5. After the completion of the re-INVITE transaction, send RTCP packets from the server end. 6. The SBC receives RTCP packets from the server side and relays it towards the client side.	The code is modified to disabled RTCP only when both RTCP bandwidth modifiers are 0 (RR=0 and RS=0). **Workaround:** None.
SBX-129389	SBX-128844 (10.1.6)	2	The PrsP on AWS SWe active node cores **Impact:** PRS cores due to a Health check timeout while waiting on a semaphore lock. **Root Cause:** PRS hits a Healthcheck timout because XRM/CPS is waiting for a semaphore. There is code in an XRM error case which grabs the semaphore and never releases it. **Steps to Replicate:** This bug was found by code inspection.	The code is modified to release the semaphore in the edge/error case. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129431	N/A	2	Blacklisted entries not getting cleared after a specific number of CS SWO **Impact:** Entries in the cache for FQDN session are not getting deleted. **Root Cause:** A new session ID is associated after the disable and enable, hence after switchover the new session ID created on the newly active setup is different from the old keys. Hence, disabling the session on the newly active pod will not delete the keys which were stored in the cache because of the old active node. So these keys will remain there as garbage values. **Steps to Replicate:** 1. Configure a peer with hostName and attach the pathcheck profile. 2. The SBC does not respond to the options and all of the sessions are blacklisted. 3. Disable the pathcheck state. 4. Enable pathcheck again. 5. The SBC does not respond to the options and all of the sessions are blacklisted. Without the fix: The user will see a different key value than before in cache pod. With the fix: The user will see the same key value as was before. 6. Perform switchover and see that the session is retrieved by the newly active pod instead of sending the options again and blacklisting.	The code is modified to reset the session ID after a disable and enable so that the session ID associated with that peer is refreshed. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129437	N/A	3	Sysdump script is failing on a new SBC instance **Impact:** The sysdump script was failing while trying to collect sysdump from the EMA. **Root Cause:** The absence of directories caused the script to fail because the system began operations before verifying the existence of the directories. **Steps to Replicate:** 1. Install the new 12.1.1 build and create a core: kill -6 <SmProcess PID> 2. From EMA, Troubleshooting -> Troubleshooting Tools -> System Dump. 3. Run System Diagnostic Dump. The process should complete successfully.	The code is modified to add a checking condition before the directory operations are executed **Workaround:** None.
SBX-129448	SBX-129198 (11.1.2)	3	The EMA Helmp section is referencing wiki link instead of customer facing link for IPSP **Impact:** The EMA Helmp section is referencing a wiki link instead of a customer facing link for IP Signaling Profile. **Root Cause:** The Helmp URL of the IP Signaling Profile was not correct. **Steps to Replicate:** 1. Log into the EMA. 2. Navigate to the IP Signaling Profile screen and click on the Helmp link. 3. The correct URL should open in a new tab.	The code is modified to correct the Helmp URL for the IP Signaling Profile page. **Workaround:** None.
SBX-129512	N/A	2	NscLif.cpp bad use of sizeof **Impact:** Bad use of the parameter "sizeof". **Root Cause:** The parameter "sizeof" was incorrectly used. **Steps to Replicate:** Not applicable.	The code is modified to ensure that the structure is fully initialized. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129528	SBX-122410 (10.1.0)	2	Reopening SBX-122410 - Confd uses weak ciphers for encrypting the encryptedStrings fields **Impact:** Remove DES3 fields from YANG modules since its deprecated. **Root Cause:** Remove DES3 fields from YANG modules since its deprecated. **Steps to Replicate:** Try to add any new YANG fields with des3 encryption type and compile.	The code is modified to remove deprecated DES3 fields from YANG and add a validation script that checks for any new YANG field that is added with the des3 type during compilation. **Workaround:** None.
SBX-129556	N/A	3	Importing CLI configuration as a LDAP user fails with "Server returned HTTP response code: 401" **Impact:** Importing a CLI configuration as a LDAP user fails with a "Server returned HTTP response code: 401" error. **Root Cause:** The code was trying to get the usergroup of the LDAP user using a linux groups command which returned empty response, causing the 401 error. **Steps to Replicate:** 1. Log into the EMA as an LDAP user. 2. Navigate to the Configuration Script and Template screen. 3. Import a CLI file. 4. Import should complete successfully without any error.	The code is modified to ensure that when the user logs into the EMA, the usergroup is already retrieved from the cdb. The usergroup is now set in the header while invoking the API to import the CLI configuration. The API is further updated to retrieve the usergroup from the header and use it to check if the user is authorized to perform the import operation. **Workaround:** Import the configuration directly through the CLI.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129711	SBX-129569 (10.1.6)	2	E2E PRACK - SBC doesn't send PRACK for the 2nd 18x message if the 2nd 18x message comes before the 200 OK for the PRACK for the 1st 18x message **Impact:** In call scenarios with End-to-End PRACK enabled, SBC is not able to send a SIP PRACK for the second 18x response if the second 18x response was received before the 200 OK for the first SIP PRACK. **Root Cause:** The internal ICM message carrying the second SIP 18x sent to the ingress leg is not processed by the ingress leg yet. At the same time the received 200 OK for the first SIP PRACK caused the deleting of the ICM message. By the time the ingress SG processed the second 18x response, it does not have any ICM message indicating that it needs to relay the SIP PRACK to the egress leg. **Steps to Replicate:** 1. End-to-End PRACK enabled; 2. A calls B; 3. B answers with a SIP 183 containing Require: 100rel; 4. SBC relays the 183 to the ingress call leg, A sends a SIP PRACK and the SBC relays the SIP PRACK to B; 5. B sends the second 18x (180 or 183) and the 200 OK for the first PRACK (back to back).	The code is modified to prevent the SBC from deleting the internal ICM message when processing 200 OK PRACK on the egress call leg. The ingress SG is responsible for deleting the internal ICM message when it is done with all the processing. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129757	N/A	3	Add option to modify 'filePostfix' to standard CLI/GUI configuration **Impact:** The following command was only available after using the "unhide debug" command, but as the customer is using it they would like it available as a standard command: set oam accounting cdrServer admin primary filePostfix This field is defaulted to "TMP" and it contains the characters added to the end of the ACT filename while it is transferred from the SBC to the remote server. The "TMP" sometimes causes issues for the DSI and the customer might need to change it to "tmp" to avoid issues. As well, the command has a possible size of up to 255 characters. **Root Cause:** This field was previously only available when using the "unhide debug" option. **Steps to Replicate:** 1. Check that the control is visible without using "unhide debug" command. 2. Change the field from "TMP" to "tmp". 3. Transfer ACT files to a remote CDR server. 4. Check the files have the post extension of "tmp" while the transfer is happening.	The code is modified to make the command visible without using the "unhide debug" option. **Workaround:** The command is accessible in older releases using the "unhide debug" option on the CLI.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129764	N/A	2	AZURE : Observed high CPU usage in the instance **Impact:** When the SBC is running in Azure on vCPU, the SBC does not have idle time. This is specific to Azure and does not impact any other platform. **Root Cause:** Running the command "mpstat -P ALL 1" shows that vCPU 1 has no idle time. Running the command Htop shows the high CPU processes and the Microsoft Azure agent is running very high. **Steps to Replicate:** Install the SBC in the Azure cloud and run the command "mpstat -P ALL 1" to check that CPU 1 has idle time.	The code is modified to remove this faulty package, correcting the CPU usage issue (agreed upon following discussions with the Microsoft team). **Workaround:** None.
SBX-129777	N/A	2	Pkt interface with VLAN tag is displayed even after deleting the ipInterfaceGroup configurations in DSBC **Impact:** The PKT interface with the VLAN was clear even though VLAN was deleted. **Root Cause:** While deleting the LIF, SB was also not deleting the VLAN interfaces. **Steps to Replicate:** 1. Configure the SBC with VLAN. 2. Delete the LIF/.	The code is modified to prevent VLAN interfaces from also getting deleted. **Workaround:** Do not configure VLAN.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129855	SBX-129666 (10.1.6)	2	Standby node failed immediately after it was upgraded **Impact:** SAM process cores on the standby node due to a corrupted list. **Root Cause:** There is corruption in a list in SIPFE which caused a core on the Standby. The corruption results in an attempt to dereference a value that the code expects to be pointer - but is an IP address instead. The attempt to dereference a value that is not a pointer caused us to core. **Steps to Replicate:** This issue was triggered by a race condition and is therefore not reproducible.	The code is modified to resolve the bug where the code processed a timer expiration for an RCB (registration control block) without checking that the timerId matches the timerId stored in the RCB. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129866	SBX-129232 (10.1.5)	2	The sonusSbxNodeResourcesMediaPortRangeExhaustionNotification trap not generated when media->mediaIpAddress is configured at the sipTrunkGroup level **Impact:** The sonusSbxNodeResourcesMediaPortRangeExhaustionNotification trap is not generated when mediaIpAddress is configured on the sipTrunkGroup and all available media UDP ports are exhausted. **Root Cause:** The Alarm is raised based on a flag (XRM_XRES_ALLOC_PORT_RANGE_EXHAUSTED) which is set during media resource allocation. The alarm is raised based on this flag for a while-do loop only if the next attempt LIF is not found. Hence, in cases where we do not try for another LIF (V4 or v6), the alarm never gets raised, unless the LIF is NOT found. **Steps to Replicate:** Configure a media->mediaIpAddress on the sipTrunkGroup. Configure a small media UDP port range on the same sipTrunkGroup (to allow fewer calls to recreate the issue or else we may have to run 32000 calls to run out of UDP ports using a single IP address) and run calls such that we run out of UDP ports, ensure that the trap gets generated.	The code is modified to raise the alarm in multiple places before returning a failure trap. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129951	N/A	2	Register SIP PDU (for de-register) in not intercepted and LI server does not receive it **Impact:** The SBC is not intercepting all the messages when the "reQuery for refresh register" flag in IPSP is enabled for a SIP registration call. **Root Cause:** The SBC starts intercepting only after receiving the LI indication in policy response. In this case, the SBC is not going for a policy dip even when the flag "reQuery for refresh register" is enabled. **Steps to Replicate:** 1. Provision one DN as a target (use the same DN for SIP registration). 2. Make a registration call (send expires=300 in REGISTER). 3. Interception happens for all the SIP messages. 4. Send the Refresh register for the same call. 5. Since the expires value 300 is less than 3600 (default value), the SBC sends 200 OK response locally. It will not send Register to egress side. 6. The SBC will not go for policy dip even after enabling the flag "reQuery for refresh register". 7. At this stage, some of the SIP messages will not get intercepted.	The code is modified to intercept the SIP messages even when the SBC is locally responding with 200 OK for refresh register. **Workaround:** Use the default value "expires=3600" in SIP Registration.
SBX-129958	SBX-129065 (10.1.6)	3	ScmP Cores **Impact:** The SCM cores due to a memory corruption issue. **Root Cause:** A field in an internal structure was corrupted. The corruption resulted in an SCM core due to an invalid pointer reference. **Steps to Replicate:** This issue is not reproducible.	The core is modified to add a workaround which will validate the contents of the field before attempting to use it as a pointer, preventing a core. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130059	N/A	3	Post ISBC LSWU process, the active ISBC fails to send config revision changes to RAMP **Impact:** Post ISBC LSWU process, the active ISBC fails to send config revision changes to RAMP. **Root Cause:** The ISBC (latest build 10.1.5R1) and RAMP 23.12 keep getting the same negative results with "emsforconfigurator" not getting written to the /etc/hosts file (after switchover) on the newly Active A02 node. The SBC appears unable to support updating any other parameters in the heat template except the build details **Steps to Replicate:** Test LSWU process on 1:1 HA set up with latest RAMP version. Expected results: The RAMP registration should complete successfully. The SBC should upload new config revision to RAMP.	The code is modified to resolve the faulty setConfigStoreParams action command. When any action command is run on a 1:1 HA active node, the command is executed in on the standby server as well because of the Confd HA synching mechanism. A check was added to prevent this problem since this command need not run in Standby server internally. **Workaround:** None.
SBX-130135	PSX-43518 (16.1.1)	2	LI PSX target lookup for call forward - missing logic **Impact:** Interception failed for a single Diversion header due to some missing ENUM definitions in INTERCEPT_TYPE related to TEL_URI for DIV_REDIR, HIST_REDIR. **Root Cause:** If an INVITE message contains a single Diversion header mapped to DIV_REDIR, and there is no match in the LI target, the call will not be intercepted. **Steps to Replicate:** 1. Send an INVITE with a single diversion header. 2. Check that the information is mapped to DIV_REDIR. 3. Interception should be successful.	The code is modified to properly intercept a call containing a single diversion header. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130151	SBX-129872 (10.1.6)	2	SBC cores and performs switchover **Impact:** The SCM process cores while processing a header while using Filter Profiles. **Root Cause:** The issue is caused by a bug in the code that handles filtering of SIP headers. The bug sets the pointer to the internal structure using an invalid value. This results in a core when the code attempts to dereference this pointer. (In this scenario, the "default" SIP Filter Profile specified that the "P-Preferred-Identity" header should get filtered but this issue could happen with other filtered headers.) **Steps to Replicate:** 1. Configure ingress sip trunk signaling sipFilterProfile to "default". 2. Configure the default SIP Filter Profile to filter "P-Preferred-Identity" header: set profiles signaling sipFilterProfile default header P-Preferred-Identity enabled. 3. E2E reINVITE and ACK enabled. 4. Send an INVITE which includes a "P-Preferred-Identity" header. 5. Ingress sends an ACK and then sends re-Invite (P-Preferred-Identity) immediately.	The code is modified to set the pointer to the correct value. **Workaround:** Disable all headers in SIP Filter Profiles.
SBX-130263	SBX-129828 (10.1.5)	3	Adding changes for DSP2LE BRES is required **Impact:** NP's cmdErrCodeF0 count keeps growing. **Root Cause:** The fix SBX-122399 only fixed the LE2LE BRES case. DSP2LE BRES where BRM can still send disableRtcpRid = TRUE to NP when RTP RID is not ENABLED. **Steps to Replicate:** The issue is not reproducible.	The code is modified to add logic for DSP2LE BRES to set disableRtcpRid flag to false if RTP RID has not been enabled. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130269	N/A	2	OPTIONS is not getting sent when hostname is configured in the pathcheck profile over the egress side of ipPeer **Impact:** Options were not getting sent after the deletion of the hostPort and config of hostname. **Root Cause:** A modification on the active patchkprofile can result in unwanted behaviour such as when options were not sent. **Steps to Replicate:** 1. Bring SBC box up and running with latest version of SBC build. 2. Enable the pathcheck profile in the SBC: set profiles services pathCheckProfile TEST sendInterval TIME recoveryCount COUNT replyTimeoutCount TIMEOOUT_COUNT transportPreference TRANSPORT 3. Delete hostPort in the pathcheck of the Ippeer: delete addressContext ADDR_CONTEXT zone ZONE ipPeer NAME pathcheck profile TEST hostPort 4. Configure hostName in the pathcheck of the Ippeer as fqdn in egress: set addressContext ADDR_CONTEXT zone ZONE_NAME ipPeer IPPEER_NAME pathCheck profile TEST hostName HOST_NAME 5. In SBC the sipSigPort, configure only AAAA IP address. Expected Results: 1. The SBC should complete a SRV query for the hostName configured in the pathcheck profile. 2. OPTIONS should get sent to the port as well as the IPv6 obtained from the SRV query answer.	The code is modified to first disable the pathchk profile for any modification on pathchk profile. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			3. The sipArsstatus should not show any servers as blacklisted. 4. The sipArsstatus should show blacklist with Ipv6 address.	
SBX-130276	N/A	2	SYS ERR observed while executing suite **Impact:** While deleting the VLAN entry, NRS generates a core. **Root Cause:** The NRS was trying to delete a previously deleted VLAN entry. **Steps to Replicate:** 1. Configure LIF with the VLAN entry. 2. Delete the LIF.	The code is modified avoid a second VLAN entry deletion. **Workaround:** None.
SBX-130277	SBX-130063 (11.1.2)	2	SCM Core **Impact:** The SCM process cores after switchover. **Root Cause:** The SCM process cores after a switchover due to an invalid pointer reference. The root cause comes from a bug in the code that recreates Subscriptions after a switchover. This bug results in a non-pointer value being put into a field that should contain a pointer. **Steps to Replicate:** 1. Enable SUPPORT_REG_EVENT via IPSP. 2. A registers to B. 3. The SBC initiates Subscribe to B and sends Notify to SBC. 4. Execute switchover. 5. B sends Notify to SBC. SBC may core in this scenario.	The code is modified so that the process for recreating Subscriptions after a switchover no longer puts a non-pointer value into a field that should contain a pointer. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130420	N/A	2	InActivityMonitoringTimer not working for OOD REGISTER **Impact:** The inactivity timer is not working for register. **Root Cause:** For a register message, the SBC uses a different place holder to store values necessary to trigger the inactivity monitor. **Steps to Replicate:** 1. Complete the following pathcheck configuration: PathChk Config: sendInterval 20; InActivityMonitoringTimer 50; 2. Attach the pathcheck profile to the ingress peer. 3. Send the OOD REGISTER from the ingress PEER. 4. Send the OOD for REG. 5. Check if the option ping was stopped.	The code is modified to add a check which includes the register message place holder. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130426	SBX-129335 (10.1.6)	2	The SBC was stuck in a routing loop after 302 was received **Impact:** The call is stuck in a routing loop in multiple 302 redirection call scenarios when the domain-based routing is used. **Root Cause:** The issue is observed due to code change done as part of SBX-112167 (10.1.0). A condition was added to free Original Message Info from a SIPSG call control block only when its Local Redirection or Force Requery flag is set. While processing the second 302, the Original Message Info is not freed which results in the feeding of domain URI for the first 302 from the Original Message Info to the SIPSG call control block and later to the CC. The CC feeds this incorrect domain as Input Data to the ERE. As it is a domain based routing, this results in the SBC repeatedly routing to same target. **Steps to Replicate:** 1. Make a Basic A - SBX - B call setup. 2. A calls B, B sends 302 with 4 contact headers. First Contact carries domain URI with FQDN. 3. Since the Force Requery flag is set at egress TG, the SBC does a ERE dip to find the target address. 4. Then, the SBC sends a re-directed INVITE to Party C. 5. The SBC receives 302 from Party C with single Contact header with domain uri with FQDN. 6. The SBC does a ERE DIP to find out the target address again.	The code is modified to revert the changes made in the SipSgProcessCurrentContact() as part of SBX-112167. Instead, the code checks if msgIndex is incremented/added. When the SBC receives a new 3xx message, msgIndex becomes a positive value and it frees up the Original message Info (containing domain uri from previous 3xx). **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			7. In the ERE log, under the input Data, the Host under the Called URI is the domain fqdn uri from the first contact header of the first 302 message instead of the domain fqdn uri from contact header of second 302. 8. In the ERE log, ERE does a domain based routing on this incorrect domain fqdn uri, resulting in the call going to same Target address and creating a routing loop.	
SBX-130476	SBX-130088 (11.1.1)	3	SBC SWe as P-CSCF: SBC inserting "P-Access-Network-Info" with incorrect values **Impact:** The SBC inserts "P-Access-Network-Info" with incorrect values. **Root Cause:** When the accessType info is invalid or not supported by the SBC, the SBC still adds the P-Access-Network-Info: header with NULL string, and hence the remaining block will append the strings which are not following the ABNF notation for PANI header. **Steps to Replicate:** 1. Configure for PANI setup. 2. Configure the following AVP on Rx_scenario.xml <avp name="IP-CAN-Type" value="6"> </avp> <avp name="RAT-Type" value="1001"> </avp> 3. Send the SIP REGISTER Request. 4. The Egress REGISTER Message should not contain Header "P-Access-Network-Info:"	The code is modified to introduce validation for Invalid/ Unsupported accessType since the accessType is a mandatory header for PANI. The SBC will log the information and discard further processing of the PANI header. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130498	SBX-130185 (10.1.6)	3	ScmP core occurred on sbcswe-brln-de08 **Impact:** SCM cores due to an attempt to access memory that has already gotten freed. **Root Cause:** SCM cores due to an attempt to access memory that has already gotten freed. **Steps to Replicate:** In this case, accessing the memory after it was freed (which is rare) resulted in a core because the memory was inaccessible. This is a rare race condition that is not reproducible.	The code is modified to prevent accessing the structure memory after it has gotten freed. **Workaround:** None.
SBX-130519	SBX-130286 (11.1.2)	2	EMA elasticsearch - bug in the main script **Impact:** Abnormal behavior affects the SBC when elasticsearch is started directly from the CLI. **Root Cause:** Elastisearch starting from the CLI starts with the root user, causing the abnormal behavior. **Steps to Replicate:** 1. Configure SSH to SBC as linuxadmin user. 2. Switch to the root user. 3. Change the directory to /opt/sonus/ema/MonitoringTools. 4. Run ./elasticsearch start. 5. Elasticsearch should start with sonusadmin user.	The code is modified to always start elasticsearch with sonusadmin user even if the root user is trying to start it. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130558	SBX-130324 (13.0.0)	2	50004 port is NOT allocated for VTP Static XRES on SBC **Impact:** VTP Port (50004) is not getting allocated for VTP Static media Resource. **Root Cause:** A new API introduced as part of SBX-111365 (10.1.0) broke the existing logic to allocate 50004 for the static media resource. As a result, a no- VTP port got allocated to the static media resource. **Steps to Replicate:** Configure a SBC for a basic VTP to RTP call, and ensure that 50004 media port is allocated for the resource towards VTP side.	The code is modified to ensure that the 50004 port is allocated for static VTP media resources. **Workaround:** None.
SBX-130632	SBX-130431 (11.1.2)	2	SBC SWe as P-CSCF: Core in AMS SBC - PrsProcess **Impact:** The PRS process cores when an announcement file with an invalid format was replaced with an announcement file of the same name with a valid format. **Root Cause:** The PRS process cores when an announcement file with an invalid format was replaced with an announcement file of the same name with a valid format. There is a bug in the code that handles this scenario. This bug causes a divide by 0 condition which causes a core. **Steps to Replicate:** 1. Load an announcement file that has an invalid format. 2. Replace the invalid file with a valid file of the same name.	The code is modified to prevent the divide by 0 error condition. **Workaround:** Avoid loading an announcement file that has an invalid format and then replacing it with a valid file of the same name.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130656	N/A	2	Unknown SDP attributes of core audio stream is getting relayed to egress INVITE and ingress 18x or 200 OK when relayUnknownAttrsForAudioTrancodeCalls flag is disabled on ingress TG **Impact:** During a transcoded call, unknown audio attributes were relayed from one side to the other with the relayUnknownAttrsForAudioTrancodeCalls flag disabled. **Root Cause:** The audio stream's attributes length were calculated even when the relayUnknownAttrsForAudioTrancodeCalls flag was disabled. This made the SBC send out the unknown attributes to other side. **Steps to Replicate:** 1. Enable the sdpAttributesSelectiveRelay flag on both of the TGs. 2. Disable the relayUnknownAttrsForAudioTrancodeCalls flag on the ingress TG. 3. Send unknown SDP attributes in the core audio stream in the INVITE from ingress. 4. Send unknown SDP attributes in the core stream in the 18x or 200 OK from egress. Expected: 1. Unknown SDP attributes of core audio stream should not get relayed to egress INVITE. 2. Unknown SDP attributes of core audio stream should not get relayed to ingress 18x or 200 OK.	The code is modified to ensure the audio steam's attribute length are made "Zero" if it is a transcoded call and relayUnknownAttrsForAudioTrancodeCalls is disabled. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130674	SBX-130436 (10.1.6)	2	SMM leak in store SIP param rule **Impact:** The SMM leaks when rule configured operation to storeSipParam. **Root Cause:** Missing logic to free memory. **Steps to Replicate:** 1. Configure the SMM operation to storeSipParam. 2. Attach to input bound adapter. 3. An Invite coming in match the criteria and action on storeSipParam.	The code is modified to free memory when done. **Workaround:** Avoid using SMM rule action to storeSipParam.
SBX-130675	SBX-130120 (10.1.6)	3	The SBC doesn't send a SIP ACK to the egress call leg if ingress is configured for media NAPT and no media is received **Impact:** The SBC does not send a SIP ACK to the egress call leg if the ingress trunk group has media NAPT enabled and no media is received from the peer. **Root Cause:** The current logic on the ingress call leg prevents the sending of the connection status to the other call leg. **Steps to Replicate:** Configure media NAPT on the ingress trunk group and make sure that the SBC doesn't receive any media packets.	The code is modified to remove the restriction on the ingress leg in order to notify the egress call leg about the call connection so that the SBC can send the SIP ACK to the egress call leg. **Workaround:** Disable media NAPT.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130720	N/A	2	Refresh Register and DeRegister messages are intercepted even though their respective policy dip response does not have interception indication from PSX **Impact:** The SBC intercepts the SIP messages even though the target is deleted during the middle of the SIP registration call flow. **Root Cause:** The targets details are stored in the RCB and maintained throughout the SIP registration. The target's details in the RCB are not cleared when they are deleted in LI table. **Steps to Replicate:** 1. DN used for SIP registration is provisioned as target. 2. Make a SIP registration call. 3. Interception of the SIP messages starts after receiving the policy response. 4. Delete the previously provisioned target DN. 5. Send a Refresh register for the same SIP registration. 6. The SBC sends the policy query; since the target is deleted, LI indication is not received in the policy response. Without fix: the SBC will still intercept all the remaining SIP messages even after deleting the target.	The code is modified to not intercept SIP messages when the targets are deleted during the middle of SIP registration call. **Workaround:** Do not delete the targets during active registration calls.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130803	SBX-130642 (11.1.2)	3	Using incorrect filter to take tshark causes the process to become non responsive **Impact:** After starting a trace in Tshark, an error appears reading "Invalid filter value", but the trace continues running and the user is unable to stop it. **Root Cause:** The TSharkPID file was not being deleted. **Steps to Replicate:** 1. Log into EMA as admin. 2. Go to -> Troubleshooting -> Troubleshooting Tools -> TShark. 3. Type a invalid filter name. Here use filter as "tcp.port==2000". 4. Start the trace. 5. A popup should appear saying "Invalid filter value" and the trace is stopped successfully.	The code is modified to remove the TSharkPID file. **Workaround:** None.
SBX-130843	SBX-126929 (10.1.4)	2	SBC EMA LI API - unexpected delay in operation **Impact:** User noticed an unexpected delay in LI operation when performed through the EMA LI API **Root Cause:** For any LI request, there are three operations performed by the API: (1) Authenticating the user; (2) Retrieving SBC LI license; and, (3) Performing the LI operation. Operations 1 and 2 are time consuming, which causes causing an overall execution time of three to five seconds. **Steps to Replicate:** Perform any LI operation and it should take less than three seconds to complete.	The code is modified to optimize operations 1 and 2 such that overall time taken to perform LI operation is less than three seconds. Please note: on a freshly installed SBC or recently restarted SBC , the very first LI operation will take around five seconds (before the fix it used to take around ten seconds or more). Subsequently it will take less than 3 seconds. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130846	SBX-130741 (10.1.6)	2	Critical Vulnerability in postgresql-xx.x.x.jre.jar **Impact:** Customer identified CVE-2024-1597 Critical Vulnerability in postgresql-42.5.4.jar **Root Cause:** The postgresql-42.5.4.jar is vulnerable to CVE-2024-1597 **Steps to Replicate:** Verify the version of postgresql.	The code is modified to update postgresql to version 42.7.2 **Workaround:** None.
SBX-130912	N/A	3	ssreq page not working in the EMA **Impact:** User gets logged out of the EMA after clicking on the "Launch SSREQ" button. **Root Cause:** When the user clicks on the "Launch SSREQ" button, the CSRF token is not passed to the backed. This causes the backend to assume that the request is forged and immediately logs the user out. **Steps to Replicate:** 1. Log into the EMA and click the "Launch SSREQ" button. 2. User should not get logged out.	The code is modified to pass the CSRF token to the backend when the "Launch SSREQ" button is clicked. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130919	SBX-130913 (11.1.1)	2	DRBD partition sync issues (split-brain) if /dev/sdb deployed **Impact:** The Elastic Search tools not working after a switchover due to a disk corruption detected on the partition involving DRBD **Root Cause:** Due to a bind mount of /var/log/sonus/evlog to /home/sftproot/evlog, evlog shows up as mounted even after drbd is unmounted. This results in an unclear shutdown of the DRBD services on the active node when the active node goes down. As a result, the new active node DRBD detectd Splitbrains and assumes whatever data it has as 'UpToDate' and 'clean'. The new active node also sets itself up for FULL SYNC. On both sites if a switchover(sbxstop) is done on the active node, the kernel on the new active node detects corruption in the DRBD fs when the sync is about to start. The Elasticsearch/dataagent service keeps its state data in evlog and if this fs ends up corrupt, dataagent is unable to start. **Steps to Replicate:** This 1:1 setup was installed using OVA, has an additional disk - /dev/sdb setup for CDRs/elasticsearch indices, and VM disk(/dev/sda) is not used.	The code is modified to ensure the shutdown code flow checks for the drbd device name instead of the mountpoint path in /etc/mtab to make sure drbd is properly unmounted and ensure that the cleanup steps are run. **Workaround:** None.
SBX-130938	SBX-130636 (10.1.6)	2	SBCb node restarted **Impact:** The PrsProcess on the Standby cores in the ICE related code. **Root Cause:** The PrsProcess on the Standby cores in the ICE related code because the ICE code tries to free a structure that is already freed. **Steps to Replicate:** Issue triggered by a rare race condition that is not reproduced easily.	The code is modified so that whenever an ICE "Instance" is freed, the pointer to that structure is set to NULL. This prevents the code from attempting to free that structure more than once. **Workaround:** This bug can only happen for customers who are in "full ICE mode". It will not affect customers running in "WEBRTC" mode.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-130959	SBX-129554 (10.1.5)	2	Newly-created SIP trunk group doesn't pick up the dnsGroup from the zone level **Impact:** The dnsGroupId is not provided to the sipTrunkGroup(s) when the DNS group(s) are created and assigned to the zone(s), but before the sipTrunkGroup(s) are created. **Root Cause:** Check for zero sipTrunkGroups (within the zone) that prevented the dnsGroupId assignment to the zone. **Steps to Replicate:** 1. Create the zone(s) without sipTrunkGroup(s). 2. Create the DNS Group(s) and assign to zone(s). 3. Create the FQDN ipPeer(s) in the zone(s). 4. Create the sipTrunkGroup(s) with the zone(s). 5. Run the calls to the FQDN ipPeer(s). 6. Examine the DBG log, and see the message from DnsClientProcessLookupReq() "no zone Id specified, defaulting to x" - x = dnsZoneId which was returned by DnsGetAnyGroupId().	The code is modified to remove the check for zero sipTrunkGroups within the zone, permitting the dnsGroupId assignment to the zone. **Workaround:** Remove and reestablish the DNS Group(s) from the zone(s) after having created the sipTrunkGroup(s).
SBX-131181	SBX-130677 (10.1.1)	2	Unable to import p12 certificate in V12.01.00R000 **Impact:** Unable to import p12 certificates in SBC Core 12.01.xx. **Root Cause:** Certificates with weak PBE algorithms can not get imported in the openssl version 3. **Steps to Replicate:** 1. Launch the SBC 12.1.x. 2. Try importing a p12 certificate with strong PBE algorithm (sonuscert.p12). Certificate import should work fine.	The code is modified to use certificates with strong PBE algorithms and change CertPBE to AES-256-CBC and KeyPBE to AES-256-CBC for the default SBC certificate sonuscert.p12. **Workaround:** None.

Resolved Issues in 12.01.00R000 Release

The following severity 1 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-123003	SBX-119461 (10.1.4)	1	The IP ACL stats are available only for 2000 entries through the SBC GUI and EMS **Impact:** Only 2000 entries are available in the IpAclRuleStats performance statistics file. **Root Cause:** There was a hardcoded limit of 2000 entries when creating the IpAclRuleStats file. **Steps to Replicate:** 1. Create 2100 ACL rules. 2. Enable the IpAclRuleStats in the fileStatisticsAdmin table. The statistics file is written. 3. Verify that there are 2100 entries in the IpAclRuleStats file.	The code is modified so the 2000 limit is removed. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-124942	SBX-124840 (9.2.5)	1	Attacker can modify existing user Registration entry resulting call failures **Impact:** Calls from the registrar to an endpoint user may have the wrong sigport in the VIA/contact header. **Root Cause:** The sigport did not restore properly in RCB in memory after registration refresh while RCB was in a challenge state. **Steps to Replicate:** 1. Disable multipleContactsPerAor, and configure multiple sigports on the same zone. 2. Send A register from source address A through the sigport1 (success). 3. Send A register from source address B through the sigport2 in "challenge" state. 4. Send A refresh register through the sigport1 (still in "challenge" state and succeeds). 5. Send an AS call to registered end point (The INVITE has via/ contact of sigport2)	The code is modified to restore the RCB to correct sigport when processing received refresh registration while in a challenge state. **Workaround:** Enable the multipleContactsPerAor flag.
SBX-125176	SBX-123131 (9.2.5)	1	There is an SAM Process core **Impact:** The SAM process has encountered a Healthcheck Timeout while executing code in GWFE which has leaked some call blocks. **Root Cause:** GWFE has detected a call in an invalid state (the call is in the GCID Hash Table but is not in the CRV Hash Table). The code handles this call incorrectly, which can result in leaked call blocks. **Steps to Replicate:** This issue is not reproducible.	The code is modified to remove the call block if it is determined that the call block is in either of the CRV Hash Table and/or GCID Hash Table. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125294	SBX-125227 (10.1.5)	1	The SAM Process cores after a switchover following an upgrade to 10.01.03 **Impact:** The SAM Process on an SBC running version V10.01.03R001 received a CPC_OP_POLICY_VARIABLES_STR optional parameter in an invite message over the GW-GW link set from an SBC running version V09.02.xx. **Root Cause:** There is no support in V09.02.xx for encoding the CPC_OP_POLICY_VARIABLES_STR sent over the GW-GW link. The data is misinterpreted when the message is decoded on the V10.01.03R001 system, which does support the encoding/ decoding CPC_OP_POLICY_VARIABLES_STR. This results in the code thinking the length of the variable is over 3000 bytes instead of 13 bytes. The code overwrote the end of the buffer the message was decoded into, causing memory corruption. **Steps to Replicate:** Configure a flexiblePolicyAdapterProfile on the ingress TG of the ingress GW running software version less than 10.1.3R0. Create a variable and route the call to an egress GW running 10.1.3R0 or higher.	The code is modified to consider the version of the SBC in an INVITE message when decoding the CPC_OP_POLICY_VARIABLES_STR. If the INVITE message is from a version less than V10.01.03R000, the CPC_OP_POLICY_VARIABLES_STR structure does not go through any particular decode logic. The code is modified only to relay the flexible variables from the ingress to egress if instructed by the PSX. **Workaround:** Disable flexible variable SMM logic when working in a mixed network. For example: set addressContext defaultAddressContext zone <zone name> flexiblePolicyAdapterProfile <profileName> and set addressContext defaultAddressContext zone <zone name> sipsTrunkGroup <TG name> signaling flexiblePolicyAdapterProfile <profile name>

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125321	SBX-125239 (9.2.5)	1	Valid registered user cannot receive calls during malicious registration in the "challenge" state for the same AOR **Impact:** A call from the registrar is unable to send towards registered end point during the period in time while registration in the "challenge" state. **Root Cause:** The SBC was missing logic to support this issue. **Steps to Replicate:** 1. Disable MulitpleContactsPerAor flag. 2. Register User A to registrar. 3. User A sends refresh, registrar response 401. 4. Registrar tries to send call to User A.	The code is modified to allow a call to go through in this scenario. **Workaround:** None.
SBX-125474	SBX-125379 (10.1.5)	1	The SAM Process core occurs on the Server **Impact:** The SAM Process cores on the standby server as it transitioned to Active mode. **Root Cause:** The SAM Process cored because SIPFE erroneously tried to mirror data while still in Standby mode. The root cause is a very small window of time after a switchover where the functions that return the Active/Standby state may return inconsistent information. **Steps to Replicate:** The steps are not reproducible.	The code is modified to use a more reliable function to determine the Active/Standby state. This prevents the SBC from attempting to mirror data while still in Standby mode. **Workaround:** There is no workaround, but this is an extremely rare event.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125620	SBX-124419 (9.2.5)	1	The S-SBC sends 481 Call Leg/ Transaction Does Not Exists, instead of interwork 200 OK for UPDATE **Impact:** The SBC releases the call if the codec offer with EV mode empty and peer answer EV with mode is not empty. **Root Cause:** There is missing logic to check if the mode empty. **Steps to Replicate:** 1. Send A call to B 2. Send A a new offer EV with empty mode 3. B answers EV with mode not empty	The code is modified to accept the codec EV answer. **Workaround**: Use the SMM to delete the EV mode from the answer leg.
SBX-125818	SBX-125387 (10.1.5)	1	The Host name is requested in place of the system name **Impact:** In the LI - SOAP/XML API, the SBC expects the hostname instead of the system name where the API failed. **Root Cause:** The EMA uses the hostname to validate the input device name. If the hostname does not match the input device name, the EMA fails the operation. **Steps to Replicate:** 1. Invoke the XML/SOAP API with the hostname as the device name. 2. Verify that the API does not fail.	The code is modified so the EMA uses the system name from CDB to validate the input device name. **Workaround:** Use the hostname instead of the system name.
SBX-125821	N/A	1	The mainline build failed due to the Openssl **Impact:** The mainline build is failing due to the OpenSSL update in the Debian repository. **Root Cause:** The new OpenSSL package was available from Debian, and update the package to in the snapshot. **Steps to Replicate:** The steps are not reproducible.	The code is modified so the OpenSSL in the new snapshot and uploaded to the artifactory. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125994	SBX-125946 (10.1.5)	1	The SBC is repeatedly reporting sonusSystemNodeResourceCongestionWarningNotification alarm **Impact:** The SCM is leaking memory at a very slow rate. The Memory Leak related to SMMSipsMmActionGetHdrValue. The code was modified for SipsMmActionHdr() to free buffer in error case to prevent memory leak. **Root Cause:** There is a bug in SMM related code in which SIP is not freeing a SMM related buffer (SMMSipsMmActionGetHdrValue) in code that is handling an error condition related to an edge case. **Steps to Replicate:** The steps are not reproducible.	The code is modified to always free the buffer before returning from the function regardless of code path. **Workaround:** None.
SBX-126060	SBX-125531 (9.2.5)	1	Incorrect Contact header sent to registrar for valid registration during an attack **Impact:** Using the same AOR register from different SRC and different trunk routing causes access to an invalid parameter in Contact header when sending to the REGISTER. **Root Cause:** Currently, the SBC does not support changing trunk group for and AOR. **Steps to Replicate:** 1. Disable the multipleContactsPerAor flag 2. Send user A from source A route to trunk A and egress A', in challenge state 3. Send user A from source B route to trunk B and egress B' 4. Send a REGISTER with a Contact through the SBC from data from A and A'	The code is modified to reject the REGISTER coming from a different source IP, if the AOR is not authenticated. Only AOR from the same source IP can establish registration at a time. **Workaround**: Enable the multipleContactsPerAor flag.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126082	SBX-125887 (12.0.0)	1	SWe_NP cores observed during RTP to SRTP call **Impact:** On SBC SWe deployments, the NP process crash is seen when Ribbon Protect reporting is enabled and the system is handling SRTP calls. **Root Cause:** Root cause was identified as an incorrect typecast operation. **Steps to Replicate:** Configure the SBC SWe instance for Ribbon Protect reporting. Subject the SBC SWe instance to a load of passthrough calls requiring encryption/decryption(SRTP) functionality.	The code is modified to fix the incorrect typecast operation. **Workaround:** Disable Ribbon Protect reporting if the SWe instance is expected to handle SRTP passthrough calls requiring encryption/decryption.
SBX-126113	N/A	1	The CHM Process crashed on the SBC 5400 active node setup in V11.01.01-A004_275 build. **Impact:** A CHM core is generated at the start of upgrade on active node (due to data agent service taking longer to stop) if there is no connection between SBC and RA. **Root Cause:** At the start of the upgrade, the data agent service will is stopped as part of sbxstop. Service data agent takes longer to stop thereby causing a health-check failure and CHM core. **Steps to Replicate:** Launch the SBC HA, configure RA, and perform upgrade.	The code is modified to update the data agent service to the latest version so that it does not get blocked while stopping the data agent service. **Workaround:** Run the following commands to disable service data agent prior to the upgrade to avoid the CHM core: /opt/sonus/sbx/scripts/service.sh dataagent unmonitor /opt/sonus/sbx/scripts/service.sh dataagent stop

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126114	SBX-126062 (9.2.5)	1	A DTMF issue on V09.02.05R006 is not present on the V09.02.05R003 **Impact:** The DTMF has failures since R5 release. **Root Cause:** The root problem was that the initial SSN programmed in NP was set to a value > 0xfc00, which caused SSN to roll over quickly. **Steps to Replicate:** 1. Configure the SBC with "Reset Enc/Dec/ROC on Decryption Key Change" is enabled, but "SSRC Randomize For Srtp" is disabled in the PSP 2. Run SRTP regression call load for at least 60 minutes 3. Make a RTP to SRTP calls and play DTMF digits, 16 digits followed by 5 digits 4. Verify the DTMF digits on the receiver side. If no DTMF failures detected, repeat step 3 because the issue does not always occur.	The code is modified to exclude the encId zero in xres->secCfg when determining the initial SSN value. **Workaround:** None.
SBX-126185	SBX-126146 (10.1.5)	1	The SCM Process core occurred on the Server **Impact:** The SCM cores when setting up a call that involves ICE. **Root Cause:** The code mishandling an internal message parameter cast (as in, copied from one variable type to another) the message when completing an NRMA modification on the ingress leg. As a result, the code later tries to use an invalid pointer. **Steps to Replicate:** The steps are not reproducible.	The code is modified to cast the message correctly. The egress modify is correct, while the rare ingress code path is incorrect. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126426	N/A	1	The su root fails with the error "/opt/sonus/sbx/scripts/accountAging.sh failed" **Impact:** The 'su root' and sudo commands may fail with error "/opt/sonus/sbx/scripts/accountAging.sh failed" **Root Cause:** The issue exists on the customer's setup because the line where accountAging.sh is called in common-auth on the customer SBC was missing the seteuid. **Steps to Replicate:** During startup, add the changeOSAgingDate $SED part as "account expiry" without the seteuid option if the SBC restarts with $ACCOUNT_AGING_SH -A 0.	The code is modified to include the seteuid to the command line in common-auth. **Workaround:** From the EMA (login as admin user), configure **System > Admin >Account management > OSAccount Aging > OSAccount Aging Period**. The state must be 'Enabled', and if already 'Enabled', try to first set it to 'Disabled' and save, then set it to 'Enabled' again and save.
SBX-126573	SBX-126425 (10.1.5)	1	Logs under DBG, showing incorrect time slot under string "Diameter Command." **Impact:** The SBC does not print the current timestamp in the DIAMETER messages printed in logs when the config "dumpPdu" is enabled. **Root Cause:** There was an issue in the code where the SBC was continuously printing the wrong timestamp while dumping diameter messages in the DBG log. **Steps to Replicate:** 1. Configure the SBC to connect to the diameter server (Enable dump PDU flag in diamNode). CLI command to enable dumpPdu flag: set addressContext default diamNode Diam dumpPdu enabled 2. Check diameter messages like CER, CEA, DWR, and DWA. and its timestamp in the DBG log.	The code is modified to print the current timestamp while printing diameter messages. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126666	SBX-126629 (10.1.5)	1	While editing the Call Trace Filter, the name is not displayed. **Impact:** When trying to edit the call trace filter name in the EMA, the name tab does not display anything. **Root Cause:** The jquery selector could not display the name to edit, even though it was already disabled. **Steps to Replicate:** 1. Log into the EMA. 2. Navigate to the Call trace screen. 3. Select a record from the table for editing. 4. The name of the call trace filter is shown.	The code is modified to add a label to the jquery selector to write the filter's name and display it in the DOM (XML Document Object Model). **Workaround:** None.
SBX-126685	SBX-126166 (11.1.2)	1	Observed several cores while executing switchover scenarios and UxPad kills operations on VMWARE setup **Impact:** Several UXPAD cores were observed while running the GPU EVS traffic. **Root Cause:** Memory corruption due to the SBC allowing more than the permitted number of EVS channels on the UXPAD. **Steps to Replicate:** On a CPU with transcoding indices that translates to more than the permitted number of EVS channels (1024 channels), run 100% EVS capacity.	The code is modified to incorporate a check to allow only the permitted number of EVS channels (1024 channels) per UXPAD. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126738	SBX-125985 (10.1.5)	1	SLBs showing alarms "SLB is unable to forward a SIP message." **Impact:** Calls are dropped with a 500 error, even though there was no congestion on the backend SBCs. **Root Cause:** The calculation of the load distribution was wrong due to data overwrite when a particular SSP was added and potentially referenced a duplicate ID from some SBCs. This causes the 'no SBC found' error. **Steps to Replicate:** 1. Attempt to configure the SSP 0 and observe it shows out of range. 2. Attempt to configure the SSP 4097 and above, observe it shows out of range: the range is 1-4096 3. Add a new SSP in one of the SBCs and SLB while the load runs. Observe that it works fine after the fix. Before the fix, the No SBC found error was seen in logs often. 4. Update the SSP in one of the SBCs and SLB while the load ran. Observe that the "no SBC found" error is seen in logs.	The code is modified to use the same variable overwriting data for different SSPs in different Cnodes (SBCs). This variable now uses an array that uses SSP_id to save the sum value to calculate and balance the load. **Workaround:** None.
SBX-126798	N/A	1	An SCM Process cored on the S-SBC and M-SBC after creating the DSBC_HA **Impact:** A crash occurred while bringing up the HA systems, I-SBC and D-SBC **Root Cause:** A NULL check was missing while logging in to the guid. **Steps to Replicate:** Bring up a 1:1 I-SBC with HA. A crash should not occur.	The code is modified to include the guid in all logs, including reconstruction/Sync logic. Added the NULL check now before logging it in sync logic. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126890	SBX-126714 (10.1.5)	1	The SDP with "crypto:0" media attribute when a re-INVITE is processed locally **Impact:** Direct Media and multiple crypto lines may trigger the SBC response to keep-alive with the second line of crypto having invalid tag. **Root Cause:** A call offer with multiple crypto lines but egress answer with one crypto line. The SBC responds to keepalive with multiple crypto lines where the second line is invalid. **Steps to Replicate:** 1. Configure the direct media, egress, disable session keepalive. 2. Ingress offers multiple crypto lines; Egress answers with one crypto line. 3. Egress peer sends keep-alive, the SBC responds to multiple crypto lines, where the second one is invalid.	The code is modified not to send a crypto line with an invalid tag. **Workaround:** Enable e2e re-INVITE or use SMM to delete the invalid crypto line.
SBX-126914	SBX-126683 (12.0.0)	1	A single node upgrade failed from 12.0 to mainline in PM **Impact:** Unable to perform LSWU from 12.0 release to 12.1 release. **Root Cause:** In the newer version of PHP, if an array element does not exist then the SBC gives an error when trying to access the element, causing the upgrade to fail. **Steps to Replicate:** 1. Login to platform manager. 2. Perform LSWU. 3. The upgrade should be successful.	The code is modified to first check if the array element exists or not. If exists only then read the value. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126940	SBX-126426 (12.1.0)	1	The su root fails with the error "/opt/sonus/sbx/scripts/accountAging.sh failed" **Impact:** The 'su root' and sudo commands may fail with error "/opt/sonus/sbx/scripts/accountAging.sh failed". **Root Cause:** The issue exists on the customer's setup because the line where accountAging.sh is called in common-auth on the customer SBC was missing the seteuid. **Steps to Replicate:** During startup, add the changeOSAgingDate $SED part as "account expiry" without the seteuid option if the SBC restarts with $ACCOUNT_AGING_SH -A 0.	The code is modified to include the seteuid to the command line in common-auth. **Workaround:** From the EMA (login as admin user), configure **System > Admin >Account management > OSAccount Aging > OSAccount Aging Period**. The state must be 'Enabled', and if already 'Enabled', try to first set it to 'Disabled' and save, then set it to 'Enabled' again and save.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126954	SBX-126649 (10.1.4)	1	The SBC is switching over and core files generated **Impact:** The IM Process may core when mirroring or syncing X2 data after the mediation server goes unreachable in PC 2.0 LI. **Root Cause:** The LI code queues messages sent to the Mediation Server. These messages are queued off an LI call block. When the LI call block is mirrored, the queued messages are mirrored also. When there are many queued messages (because the Mediation server went unreachable), the CCB and messages may not fit into the 64KB buffer that was allocated for sending the Redundancy message to the standby. The code currently does not detect that the data does not fit into the buffer. As a result, the copy overwrites the end of the allocated buffer and causes memory corruption (of the memory beyond the end of the allocated buffer). **Steps to Replicate:** In the SBC HA setup, configure CDC with PC2.0 LI flavor: 1. Start the LI simulator, which accepts X2 data. 2. Provision the targets with wild card entry in EMS. 3. Make 10 Registration calls at a time with targets. 4. Once interception starts, stop the LI simulator. 5. Make additional interception calls. The SCM cores.	The code is modified to drop any CCB that has more than 64KB of pending data from the Mirror/ Sync messages. This fix prevents the core, which can happen when mirroring (or syncing). **NOTE**: A side effect of this fix is that the LI leg of the call is not mirrored and therefore is lost after a switchover. As a result, there is no Interception for this call after the switchover. This only applies to calls that have more than 64KB of data waiting to be sent to the Mediation Server and the SBC is attempting to mirror this call just before a switchover. A JIRA for release 12.1 was opened to improve the design to allow mirroring an LI CCB with more than 64KB. **Workaround:** Ensure that the network path to the Mediation Server is stable and connected/ up.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126991	SBX-126561 (10.1.5)	1	VoLTE-IMS Deployment SBC7K acting as PCSCF. PRACK with RAck: 1 0 header towards S-CSCF **Impact:** In a DLRBT and e2e PRACK scenario, the SBC may send invalid PRACK to the egress. **Root Cause:** Queueing an 18x may trigger an invalid relay of PRACK from ingress to egress after the RTP learning completes. The phone responds with PRACK using RAck: 679127 1 INVITE, but the RAck is 1 0 in the PRACK sent by the P-CSCF towards the S-CSCF. **Steps to Replicate:** 1. Enable the LRBT and e2e PRACK. 2. Send an 183 (prack) and 180 (no prack) through the egress peer. 3. After learning RTP, the SBC sends an additional 18x to ingress, and the peer sends a PRACK relay to egress.	The code is modified so PRACK is handled locally on ingress if the 18x is queued. **Workaround:** Disable the DLRBT.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127225	SBX-126648 (10.1.4)	1	Switchover and Application Restart **Impact:** The SCMProcess cores while processing a P_SVC_INFO header. **Root Cause:** There is a bug in the code resulting in the pointer to the P_SVC_INFO header getting copied to the wrong location. This results in a Segmentation failure since the SBC tries to read from an invalid location in the memory. **Steps to Replicate:** 1. Configure relay INFO. 2. Enable Transparency for P-Svc-Info header. 3. Enable Transparency for two other optional headers which will be sent in INFO message along with the P-Svc-Info header. 4. A calls B, A sends an INFO message to B which includes the P-Svc-Info header (and two other optional headers) **NOTE**: The INFO message should include a P-Svc-Info header and at least two other optional headers which precede the P-Svc-Info header.	The code is modified so that the SBC copies the P_SVC_INFO header properly, ensuring that the header pointer is stored at the correct location. **Workaround:** Use SMM rules. SMM rule on the incoming Trunk Group 1. Store the p-svc-info header to var. 2. Add new header A and store value from var. 3. Delete p-svc-info header. 4. Enable Transparency for unknown header (or A). SMM rule for outgoing Trunk Group 1. Store header A to var. 2. Add back p-svc-info header from header A. 3. Delete header A.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127282	SBX-124089 (10.1.5)	1	sipInternalCauseMappingProfile is not working after upgrade **Impact:** The assignment of the sipInternalCauseMappingProfile is not working after the upgrade. **Root Cause:** Observing after LSWU, the sipInternalCauseMappingProfile structure is not restored while creating Zone data from CDB (Configuration Data Base). **Steps to Replicate:** The issue is that the sipInternalCauseMappingProfile is not working after doing LSWU. 1. A new sipInternalCauseMappingProfile needs to be created using the below given commands. set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupOutofService sipCause 598 set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupOutofService sipCauseText "TG OOS" set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupOutofService includeReasonHeader none set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupOutofService insertCauseTextInSIPResposeTitle disabled set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupInDisabled	The code is modified for the following scenarios: 1. While restoring AddressContext-specific data from confd, zone data is created for each zone in the function SipSgCreateZoneDataFromDb(). But, InternalCauseMapProfile data from CDB is not restored. 2. To restore the InternalCauseMapProfile data from CDB, the function SipSgZoneInternalCauseMapProfile() is called in the function SipSgCreateZoneDataFromDb() so that InternalCauseMapProfile data is sent to the SIPSG_SIG_ZONE_STR. **Workaround:** Recreate and reapply the internalSipCauseMapProfile to the required zones.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			sipCause 597 set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupInDisabled sipCauseText "TG disabled" set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupInDisabled includeReasonHeader none set profiles signaling sipCauseCodeMapping internalSipCauseMapProfile VABF82_TEST causeMap TrunkGroupInDisabled insertCauseTextInSIPResposeTitle disabled set addressContext default zone ZONE1 sipTrunkGroup ACCESS_ZONE signaling causeCodeMapping sipInternalCauseMappingProfile VABF82_TEST set addressContext default zone ZONE1 causeCodeMapping sipInternalCauseMappingProfile VABF82_TEST 2. Before performing an upgrade, follow these steps in the CLI: set addressContext default zone ZONE1 sipTrunkGroup ACCESS_ZONE state enabled set addressContext default zone ZONE1 sipTrunkGroup ACCESS_ZONE mode outOfService. While trying to make a call, a "598 Server Failure" cause should be thrown. 3. Perform an LSWU. After an LSWU, while making a call, receive a "598 Server Failure".	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127385	SBX-126198 (9.2.5)	1	Call Fails to route the advance after the SBC receives a SIP Refer Message. **Impact:** This issue occurs when a trunk group in a 300 Multiple choice response exceeds the CAC limit. The call is cleared instead of going to the next TG. **Root Cause:** Route advancing is ceased if the call cleared due to CAC exceeded. **Steps to Replicate:** The Call Scenario/flow is: 1. A calls B. 2. B sends refer to the SBC. 3. The SBC does an ERE dip and finds three routes. 4. The call is established between A and route 0 or C. 5. C sends 300 Multiple choice with 3 TGs. 6. When trying to send the call to the 1st TG, it exceeds CaC limit and then tries to redirect the call to the next TG successfully.	The code is modified to add a check in the destination transfer case to handle the failure when the CAC limit is exceeded for a TG in multiparty call scenario. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127486	SBX-126469 (10.1.5)	1	VoLTE-IMS Deployment SBC 7000 acting as PCSCF. The ACK received is not being sent after a re-INVITE is sent towards the UE. **Impact:** The SBC sends re-INVITE without an SDP, which causes ACK not to get sent to the egress leg for an initial 200 OK. **Root Cause:** The issue is because the SBC uses an AMR codec to play tone on the ingress leg and switches to the EVS codec on the ingress leg for audio and PCMA on the egress leg for audio. This causes the SBC to send a re-INVITE to the ingress leg with EVS, but due to a delay in the PCRF response, newActivePsp is reset even before sending a re-INVITE to the ingress leg, causing the re-INVITE to go without SDP. **Steps to Replicate:** 1. UE-A sends AMR EVS codec to SBC. 2. The SBC sends AMR, EVS, and PCMA in INVITE to UE-B. 3. UE-B sends a 180 without SDP and a 200 OK with PCMA. 4. The SBC sends a 180 and 200 OK with AMR on the ingress leg. 5. The SBC sends a re-INVITE without SDP on the ingress leg.	The code is modified to avoid resetting the newActivePsp before a re-INVITE is sent to the network for the case where the user is waiting for a PCRF response. **Workaround:** This issue is not seen if the pcrfMode is set to asynchronous mode.
SBX-127517	N/A	1	Observed SamProcess core after configuring static route **Impact:** While running jenkins sanity, the user observed a SamProcess core after a static route config. **Root Cause:** Initialization of one member(XrmControlXresFsm *xrmFsmCtrlPtrChunkIPv6;) of a SigPort Struct Ptr was missed while coding. **Steps to Replicate:** Complete a Static Route config and verify that no core is generated,	The code is modified to initialize the member. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127533	N/A	1	On the hardware SBC 7000 setup (FIPS enabled), the standby node services are not coming up when upgrading from V10.01.03R002 to V12.01.00A002 **Impact:** When upgrading the SBC 7000 setup with FIPS-140-3 mode enabled from build V10.01.03-R002 to V12.01.00-A002, the services in the standby node are not coming up. **Root Cause:** The issue was due to improper OpenSSL configuration in a FIPS-enabled system. **Steps to Replicate:** 1. Install a 10.1.x build and enable FIPS. 2. Perform an upgrade to 12.1.x 3. The SBC should come up with FIPS-enabled. grep fipsMode /opt/sonus/conf/sbx.conf (enabled)	The code is modified to handle the OpenSSL configuration change while upgrading from a FIPS-enabled system. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127587	SBX-126722 (10.1.5)	1	No audio for media loopback calls that are established after a link detection switchover; stable media loopback calls that survived the switchover have two-way audio **Impact:** If the SBC switches over while there are stable loopback calls, one-way audio on newly established loopback calls are using altMediaIpAddresses results in stale MAC from a previously cached ARP entry. **Root Cause:** When a XRES (ethernet resource) with a resolved route is allocated in standby context, that route is added in the XRM's route cache. For the loopback route, the destination MAC address is the MAC address of the packet interface on active node. But on the SBC SWe platform, the standby packet interfaces have different MAC addresses as active packet interfaces. After a switchover, when the loopback route is assigned to the new loopback call, the previous active node's packet interface MAC address is used as destination MAC address caused by one-way audio. If XRM receives ARP change notification message from NRS, it updates all cached routes. But XRM is not guaranteed to receive ARP change message in this case. **Steps to Replicate:** 1. Configure LIFs with at least 2 altMediaIpAddresses, and use them as trunk group media IP addresses. 2. Make long duration loopback calls on SWe, ensure the loopback trunk has >= 2 altMediaIpAddresses. A switchover occurs on the standby node. 3. Check the call's audio.	The code is modified to the standby along with XRES data. When allocating XRES in standby context, XRM checks this flag for the SBC SWe. If loopback flag is true, XRM replaces the mirrored destination MAC address with the local packet interface's MAC address and saves it in route cache. **Workaround:** Use the LIF IP address as trunk group media IP address.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			4. Make new loopback calls. 5. Check new call's audio.	
SBX-127913	N/A	1	A SCM Process core dump is observed during the SBC automation run for random test cases. **Impact:** There was a core while running I-SBC test suites. **Root Cause:** The new logging enhancements done to add guid for non-INVITE had issues. **Steps to Replicate:** Run I-SBC test suites.	The code is modified with new NULL checks to the new logging enhancements. **Workaround:** None.
SBX-127967	SBX-126362 (9.2.5)	1	Frequent cores and split-brain messages, multiple SBC SWe KVM **Impact:** The SBC generates SWe_NP cores, and switches over when running SRTP calls. **Root Cause:** Buffer overwrite happens if the RTP header's "pad" bit is set but the RTP Pad Byte Count field is greater than the packet length. **Steps to Replicate:** Send a SRTP packet with the RTP header's pad bit set and the RTP pad byte count field set to 255.	The code is modified to correctly handle the improper pad byte count case when the SBC needs to strip the pad bytes. **Workaround:** Disable SRTP calls.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127988	N/A	1	SBC Core V12.0 - Stored XSS : Configure login banner **Impact:** The login banner in the platform manager's login screen is vulnerable to stored XSS. **Root Cause:** The login banner text was not html encoded, making it vulnerable to stored XSS. **Steps to Replicate:** 1. Log into the EMA. 2. Configure the login banner text with executable javascript code. 3. Log out of the EMA and navigate to the login screen of platform screen. Expected results: The login banner text shows as configured and the javascript code gets processed.	The code is modified to encode the banner text. **Workaround:** None.
SBX-128143	SBX-124611 (11.1.1)	1	SBC 5400 live upgrade to 11.1 is failing. **Impact:** LSWU to 11.x fails with pre-checks timing out whenever there are confd system queries being run in parallel during LSWU. **Root Cause:** The Pre-upgrade check times out because the SM process is processing the LSWU request causing all other system queries to wait, including the system command operation included in the appPreUpgrade check. Pre-upgrade check times out as the SM process would be processing the LSWU request and all other system queries being run will be waiting (including the system command run as part od appPreUpgrade check). **Steps to Replicate:** Perform LSWU to build 11.1.1R1 and ensure LSWU is successful.	The code is modified to remove the DB Query system command in the appPreUpgrade check. **Workaround:** Avoid running SNMP system queries during LSWU to prevent this issue.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128269	SBX-126698 (11.1.1)	1	Invite over 1500 MTU gets discarded **Impact:** IPsec packets (in tunnel mode) containing IP fragments are dropped. During call establishment, this results in failed call attempts. **Root Cause:** During reassembly of two fragments received inside the encrypted inner payload of an IPsec packet, if the IP payload of the reassembled packet is less than or equal to 1580 bytes, then the SBC fails to update the end of packet pointer correctly. This ultimately causes the packet to become corrupted and get dropped. **Steps to Replicate:** 1. Generate a SIP INVITE that will get fragmented into two packets, or will get fragmented into two packets once IPsec headers are added to the INVITE. The IP payload length of the INVITE must not exceed 1580 bytes. 2. Ensure that the SIP INVITE is routed towards the SBC through an appliance that will encrypt each fragment in its own complete IPsec packet. The outer IP header of the IPsec packet must not get fragmented. Algorithms tested must include encryption algorithm 3DES and MD5 authentication. 3. Verify that the SBC decrypts the IPsec packets, reassembles the decrypted fragments, and the INVITE is accepted and the call attempt succeeds.	The code is modified to ensure that the end of packet pointer for reassembled fragments received inside the encrypted inner payload of an IPsec packet is correctly updated. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128273	SBX-125865 (10.1.5)	1	One-way audio issues that come up after the IP gateway MAC address change and the SBC sending RTP packets to the old/ stale MAC address **Impact:** The XRM's existing route and gateway hash table can only handle one-to-one mapping between them. **Root Cause:** The cause is the original logic introduced in 7.2.x to support IP platform migrations on pkt ports (adjacent switch replacement). **Steps to Replicate:** The steps are not reproducible.	The code is modified to allow one-to-one mapping between the route and the gateway. Two new debug commands are also added to dump the first 100 entries of route and gateway hash tables. **Workaround:** None.
SBX-128440	SBX-125991 (11.1.2)	1	PrsP Core Occurs on Server **Impact:** This problem is found in the code for fingerprinting media which can Helmp assist in identification of spam (robo) calls. Processing of a certain kind of media (G722) caused the PRS process to crash. **Root Cause:** In the part of code that checks if 30 seconds of media is collected, a bug when the media buffer is exhausted causes the buffer to overflow and a PRS process crash. **Steps to Replicate:** This fix cannot be tested without a specific type of media with a combination of timestamp variations, packet sizes and silence gaps.	The code is modified to correct the problem with the 30 ms of buffered traffic when the buffer is exhausted. **Workaround:** Input the following CLI commands for Enabling and Disabling Fingerprinting. Since these are provisioning commands, they are persistent across reboot: set global callTrace sageFingerprint disable (workaround) set global callTrace sageFingerprint enable show details global callTrace

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128510	SBX-123260 (10.1.3)	1	When the port range setting is narrowed and port is not available, SBC adding port number "9" in Application M-line **Impact:** The SBC sends port 9 in the outgoing INVITE towards the egress leg when no TCP ports are available. **Root Cause:** The flag "EnhancedApplicationMediaSupport" that was introduced in 8.2 to prevent the SBC from sending port 9 in an INVITE when ports are not available, but instead to send a 488 to the ingress peer when ports are not available, does not function as designed. **Steps to Replicate:** 1. Configure TCP port range from 10000 to 10002. 2. Make 4 application media calls. The SBC should send port 9 in egress INVITE for 4th call instead of rejecting 4th call 488 response.	The code is modified for the SBC to send 488 response to ingress peer when TCP ports are not available for media. **Workaround:** Configure sufficient TCP port range based on expected TCP calls on the SBC.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128912	SBX-128029 (10.1.4)	1	Intermittent call failures on the SBC 5400 **Impact:** There is an intermittent one-way audio issue on the SBC. **Root Cause:** XRM used NP_MEDIA_FLOW_MOD_RTP_NAT_MATCH_FLAG option to ask the NP to re-learn and notify when an RTP packet did not match the srcIP, and the srcUDPPort passed down. NP_MEDIA_FLOW_MOD_RTP_NAT_MATCH_FLAG is used for secureNAT feature where prefix! = 0. When this flag is sent with prefix = 0, the NP did not set the part that informs the NP to re-learn and caused one-way audio. For the calls that are successful, there are multiple re-INVITEs that trigger the XRM to modify the flow, which overwrites the NP_MEDIA_FLOW_MOD_RTP_NAT_MATCH_FLAG option with NP_MEDIA_FLOW_MOD_RTP_NAT_NEW_FLAG (modFlag 0xC00 or modFlag 0x400) before the 1 second timer expires. **Steps to Replicate:** In a NAPT set up, after the SBC learned RTP packet and establishes the connection, use the following steps: 1. Send a re-INVITE to change RTP port to a different port than the one triggering the NAPT re-learning. 2. Send a few RTP packets from the old port and followed by RTP packets from the new port.	The code is modified to not use the NP_MEDIA_FLOW_MOD_RTP_NAT_MATCH_FLAG for the non-secure re-learn case. XRM now uses the NP_MEDIA_FLOW_MOD_RTP_NAT_NEW_FLAG and sets the srcIP and srcUDPPort to the old values. This code change sets the correct fields and notifies the XRM when an RTP received does not match the values passed in. **Workaround:** No workaround.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129220	N/A	1	During scale up of SC, the API is unable to fetch the current deployment count of SC/RS pods when the deployment kind is "rollouts" **Impact:** The application failed to scale up or down the SC pods on crossing the threshold range for the "rollouts" deployment kind. **Root Cause:** The API that provides the current deployment count of SC pods fails due to resource access, as the count is further used to make scaling decisions. **Steps to Replicate:** The steps are not reproducible.	The code is modified to update the resource access parameters for the "rollouts" deployment kind. **Workaround:** None.

The following severity 2-5 issues are resolved in this release:

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-121420	SBX-119575 (10.1.5)	2	The SBC sends an INVITE to an incorrectly registered client. **Impact:** 1. Sending a call to an incorrect registered user because of subsequent registrations resulting in overwriting connection details of the initial registration. 2. Sending an in-dialog message to a newly registered endpoint for the same user, with multipleContactsPerAor disabled. **Root Cause:** 1. While handling SIP registrations, the SBC internally creates and maintains a connection handle representing the registering user agent's socket. Due to design limitations, the handle may duplicate into one of the subsequent registrations if the network connection for the initial registration is closed. This resulted in a call to a registered party, going to a different unintended registered agent who registered later. 2. While sending an in-dialog message, the connection handle is picked up from the updated registration, which has the new IP/port and thus routes to a new connection, whereas the remote target for the dialog still points to the old IP/port. **Steps to Replicate:** Use the following steps for the first issue: 1. Using SIPp, establish the first set of 256 long-duration registrations over TCP for 256 different endpoints. a. Make sure to close the TCP connections for each registration.	The code is modified to detect a bad connection handle, which points to a different remote socket than requested by the SIP stack. If this is detected, the connection handle is cleared, resulting in the message going to the socket requested by the SIP stack. **Workaround**: None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. Using SIPp, establish a second set of 256 long-duration registrations over TCP for 256 endpoints (different from the first set). 3. Make calls to the first set of registered endpoints. Observe that some calls go to the second set of registered endpoints. Use the following steps for the second issue: 1. User opens a new connection T1(IP1/P1) on registering with the SBC. 2. Establish the call using the same T1 connection, with an INVITE having contact IP1/P1. 3. On the SBC switchover, the T1 connection is closed. 4. Opens a new TCP connection T2 from new socket (IP1/P2) on a re-registration. 5. Send a MESSAGE method to the SBC to be delivered in-dialog to the user and ensure it is sent to IP1/P1 and not to IP1/P2.	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-122431	SBX-121550 (10.1.5)	2	Video/Data stream was not relayed on the egress side in both bundled and unbundled scenarios **Impact:** In a bundled call with audio, video and data, the 'show status global callDetailStatus' command shows egressDtlsStream3 as DISABLED instead of RELAYED. Also, the fingerprint was missing in the INVITE SDP of the video and data stream. **Root Cause:** The issue occurs when the dtlsSrtpParams and the srtpParams are getting cleared due to a code fix in SBX-121550 in the 9.2.5R5 release. **Steps to Replicate:** 1. Run a call that sends the bundled media: audio, video, and data channel. a. Answer accepts bundling on all three. b. While the call is running, ensure that the command "show status global callDetailStatus" shows egressDtlsStream3' => 'RELAYED. 2. Verify the SBX-121550 fix using the steps below: a. Make an RTP to SRTP configuration. The set up should be HA. The RTP leg should not have any security psp attached. b. Configure the session timer, as the session expires for the SRTP leg first. c. Establish an A to B call and then perform a switchover. d. Wait for the switchover to occur.	The code is modified to revert to the changes in SBX-121550. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			e. Wait for the session timer to expire and see an INVITE towards the SRTP to successfully answer with a 200 OK. f. Wait for an INVITE towards the RTP side. Observed results: The SBC sends BYE. Expected results: The SBC sends INVITE to the ingress side.	
SBX-123230	N/A	5	The customer deleted the 'admin' user as the password aged. **Impact:** Deleting the "admin" user and rebooting the system failed to start the application. as SBC depended on the "admin" user for cloud initialization (AWS). **Root Cause:** The system restores SSH keys as part of the cloud_init startup process. but fails as a result of the deleted "admin" account. **Steps to Replicate:** 1. Restart the system in AWS after removing the "admin" user from the confd CLI. 2. Check whether the system starts successfully or fails.	The code is modified so if the admin account is deleted, the system does not attempt to restore the 'admin' account SSH keys. **Workaround:** None.
SBX-124852	SBX-125893 (11.1.1)	2	ISBC-HA : CpxAppProc dumps core on active node **Impact:** Standby Cpx cores and restarts. **Root Cause:** Moving the confd state back from slave to none in 1:1 HA. **Steps to Replicate:** None due to rare occurrence.	Removed the change to move confd state back from slave to none in 1:1 HA. **Workaround:** Restart the SBC.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125066	SBX-125060 (9.2.5)	2	Registration issues where calls were allowed from non-registered IP/Port **Impact:** With multiple registrations in the challenge state coming through the SBC and back-to-back INVITES, the SBC may allow a call from an unregistered endpoint. This occurs during a small window while the registration transits from the initiating to the challenge state. **Root Cause:** When receiving multiple registrations in the challenge from different sources, the SBC may receive a call from an unregistered endpoint. This is a result of the SBC not validating an authenticated end point source address correctly. **Steps to Replicate:** 1. Disable MultipleContactsPerAor and configure multiple SIP signaling ports in the same zone 2. Receive a register from source A address and send to signaling port A 3. Send refresh from A and in the challenge state 4. Attempt to register A from different source address, B to signaling port B (Registration is in initiating state). 5. Run A from source address B try to make a call	The code is modified to validate the authenticated endpoint source address. **Workaround:** Enable the Global Signaling flag "multipleContactsPerAor".

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125111	SBX-125078 (9.2.5)	2	The SBC sends an INVITE to non-Registered IP/PORT when the RCB in Updating/Terminated state **Impact:** The registrar server may send a call to the wrong IAD. This can occur if multipleContactsPerAor is disabled and the registrar server is unable to respond to the updated registration. **Root Cause:** The registrar server was unable to respond to the updated register, which causes it to send the call to the wrong IAD. The SBC registration is in the middle of updating/terminate state. **Steps to Replicate:** Disable the multipleContactsPerAor and multiple SIGport on the same zone. Case 1: 1. Run an A register success from sigport 1. 2. Run an A register from sigport 2, and receive call from registrar. Case 2: 1. Receive an A register success from sigport 1. 2. Run an A register from sigport 2, and wait for retransmit timeout. 3. Receive a call from registrar.	If the registration is in the updating state, reject the call. If the registration timeout and in terminating state, still allow the call to the correct previous authenticated contact. **Workaround:** Enable the Global Signaling flag "multipleContactsPerAor".

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125267	N/A	2	Import of confd XML with Media Port Range is failing **Impact:** Import can downgrade the interface, add media port range, and make the interface up in an ideal scenario. However, it was throwing an error when importing configs. **Root Cause:** The /addressContext/ipInterfaceGroup/IPInterface/state is "disabled," and the/addressContext/ipInterfaceGroup/ipInterface/mode is "outOfService". At the same time, importing media port range configs, and then it should come to the enabled state and "inService" mode, respectively. **Steps to Replicate:** 1. Add mediaPortRange configs by changing IPInterface mode to "outOfService" 2. Make IPInterface mode to "inService" mode 3. Export the configs 4. Clear the DB on the SBC 5. Import the same configs and, check the "ExportStatus" and ensure the import is complete.	The code is modified so the interface gets down while applying import configs. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-125709	SBX-122164 (10.1.3)	2	M-SBC acts as if enhancedApplicationMediaSupport was disabled although it is enabled **Impact:** The enhancedApplicationMediaSupport flag is not enabled when configured together with other "system->media" flags. **Root Cause:** MRM code returns a failure when an unrelated "system->media" flag is configured along with MRM related "system->media" flags. This is causing the CLI commit to fail. **Steps to Replicate:** Configure the mentioned flags below all at once, and enhancedApplicationMediaSupport will not be enabled: set system media enhancedApplicationMediaSupport enabled set system media tcpPortRange baseServerPort 10000 set system media tcpPortRange maxServerPort 65148 set system media dedicatedBWForNonRTPMedia 50 set system media mediaPortRange baseUdpPort 10000 set system media mediaPortRange maxUdpPort 65148 set system media mediaPeerInactivity inactivityTimeout 20 set system media policing spikeAction alarm bwOverloadAlarmTimer 300 commit	The code is modified to allow MRM to handle only MRM related flags and ignore unrelated flags. **Workaround:** Workaround is to commit steps 1. to 4. separately and 5. to 8. separately: 1. set system media enhancedApplicationMediaSupport enabled 2. set system media tcpPortRange baseServerPort 10000 3. set system media tcpPortRange maxServerPort 65148 4. set system media dedicatedBWForNonRTPMedia 50{{}} commit 5. set system media mediaPortRange baseUdpPort 10000 6. set system media mediaPortRange maxUdpPort 65148 7. set system media mediaPeerInactivity inactivityTimeout 20 8. set system media policing spikeAction alarm bwOverloadAlarmTimer 300 commit

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126003	N/A	2	Fix the IKE memory corruption issue caused during the printing of large logs **Impact:** In the IKE subsystem, when printing the logs of a size larger than 512 bytes, memory corruption occurs. This issue occurs when setting the the debug log level to info and using certificates for IKE authentication. **Root Cause:** The Buffer is overrun while printing the logs of size larger than the allocated buffer size of 512 bytes **Steps to Replicate:** The steps are not reproducible.	The code is modified so that only 500 bytes of the larger logs is printed, and there is no buffer overrunning. **Workaround:** None.
SBX-126048	N/A	2	T Password Expiry prompt is shown for a calea user for sso CLI provisioning **Impact:** The Password Expiry prompt is shown for a calea user for sso CLI provisioning. **Root Cause:** The password change prompt is seen because the password for a newly created user 'calea' has never gotten reset when the connection between the EMS and the SBC is delayed. **Steps to Replicate:** Test with a delayed connection between the SBC and the EMS. Block the OAM IP at RAMP when the OAM is coming up so that the connection is delayed.	The code is modified to reset the CALEA user password when the connection between EMS and SBC is delayed. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126079	N/A	2	The SWe_NP is not coming up for the SBC guest with eSXi host having OS version 8.0 Update 1. **Impact: The management** The interface of the SBC SWe instance of type 'vmxnet3' fails to come up with VMware ESXI platform 8.0. **Root Cause:** SWe_NP tries to configure a single RX queue and enable the RSS if the management interface is 'vmxnet3'. ESXI platform 8.0 is not permitting RSS, which is enabled with a single RX queue, resulting in RX queue configuration failure. **Steps to Replicate:** Bring up an SBC SWe instance with a management interface of type 'vmxnet3' on VMware ESXi platform 8.0. The management interface should be up, and the user can log in.	The code is modified to disable the RSS if the management interface is 'vmxnet3'. **Workaround:** None,
SBX-126105	N/A	2	Negative value reported for ORIG_CALLS in SipSigPortStatisticsStats **Impact:** A negative value is observed for ORIG_CALLS in SipSigPortStatisticsStats. **Root Cause:** ORIG_CALLS exceeded the max value that INT32 can hold. **Steps to Replicate:** Make ORIG_CALLS exceed what INT32 can hold (2,147,483,647).	The code is modified to change the ORIG_CALLS type from INT32 to UINT32 **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126152	SBX-125906 (12.0.0)	2	Both Active and standby servers are coming up as Active when reboot is done **Impact:** Both nodes are coming up in the active role when there is a switchover in the bond interface from one interface to another interface. **Root Cause:** Bond device switchover does not happen as it is using the 'ifenslave' command which is deprecated and not available in the bullseye release of Debian. **Steps to Replicate:** Bring up the SBC in HA mode and perform a switchover of the bond device by bringing down one of the active interfaces.	The code is modified to ensure that the 'ip' command is used to perform the switchover of interface for the bond device. **Workaround:** None.
SBX-126204	SBX-125816 (9.2.5)	2	Openstack VM SBC - crash on standby - SCM (SIPSG SG iter) **Impact:** SCM cores due to Healthcheck while the customer was making configuration changes to SIP Trunk Groups (when there are thousands of SIP Trunk Groups configured). **Root Cause:** Healthcheck encountered because the SIP code was taking too long to process a set of SIP Trunk Group related configuration changes. When making configuration changes to a SIP Trunk Group, a MAJOR level log message is printed for every configured SIP Trunk Group (in this case there were 4000+ Trunk Groups configured). Printing this log message 4000+ times affected the performance of the system. **Steps to Replicate:** 1. Configure 4000 TGs. 2. Make changes to 3 or 4 different TGs. 3. Commit changes.	The code is modified to no longer print a MAJOR level log message for every configured SIP Trunk Group when making configuration changes. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126366	SBX-126069 (11.1.1)	2	Observed a SipReg core during a failback with 256k subscriber data **Impact:** Observed a SipReg core during a failback with 256k subscriber data. **Root Cause:** During failback, the SBC crashes and a sipReg core occurs. **Steps to Replicate:** 1. Load the latest SBC build V11.01.01-A004-272 onto a HA 7000 SBC. 2. Complete the SipReg config and then load the 256k subscriber data. 3. Trigger failover and observe the sipReg core. 4. If no core is generated during failover, check the SBC sync status. Once the SBC is synced properly, complete the failback and check for the core.	The code is modified to ensure the sipreg subscriber profile load is phased out with timer, then RCB will sync to standby as it is phased out with the timer. **Workaround:** None.
SBX-126468	N/A	2	SIPREC Re-Invite after Switchover does not contain +sip.src extension in Contact Header **Impact:** Post SWO, When the SBC receives the re-INVITE from the endpoint, SBC triggers a Re-INVITE towards the SRS with missing SIPREC feature tag (+sip.src) in Contact URI. **Root Cause:** The control bit of SIPREC feature tag remains unset after the SWO. **Steps to Replicate:** 1. Set up the SBC for SIPREC for ingress recording. 2. Make a call between A to B. 3. Perform the switchover. 4. Trigger Re-Invite from the endpoint.	The code is modified to set SIPREC feature tag, Now SBC triggers a Re-INVITE with SIPREC feature tag in Contact URI towards the SRS on receiving the re-INVITE from the endpoint. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126578	N/A	2	The mgt0 IPV6 config is not applied **Impact:** The Ipv6 addresses are not getting displayed in the SBC Platform Manager Install/Upgrade screen. **Root Cause:** To retrieve and store IPv6 addresses from interfaces, the SBC software was using the 'ip -6 route' command which is deprecated in Debian 11. Due to this, no IPv6 addresses are returned to the Platform Manager Screen from backend. **Steps to Replicate:** 1. Install an SWE SBC and configure a IPv6 address for mgt0. 2. Log into Platform Manager and check the Software Install/ Upgrade screen. Without the fix, no IPv6 addresses are displayed. With the fix, the IPv6 address is shown under 'IP v6 addresses'.	The code is modified to update the OS command 'ip -6 route' to 'route -6' in the software. **Workaround:** None. It is a display-only issue.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126581	SBX-125587 (10.1.5)	2	The SBC does not send a SIP ACK to 200 OK for a re-INVITE in certain call flows **Impact:** The SBC is unable to send ACK to keepalive on the egress when the peer response 200OK is different SDP from previous one. There is a race condition when ingress received keepalive and send to egress, at the same time SBC internally send keepalive on egress. **Root Cause:** On egress, the response 200OK (SDP) for internal keepalive is accidently an answer for e2e re-INVITE on ingress. Later on the 200OK for e2e re-INVITE does not have e2e ACK. **Steps to Replicate:** Configuration: e2e Invite and Ack, Same keepalive value of ingress and egress trunk groups After a call connected 45 seconds later, the SBC sends keepalive on egress, at the same time received keepalive from the ingress.	The code is modified to not update the SDP of 200OK from an internal keepalive INVITE. Wait for the 200OK (SDP) from e2e re-INVITE to update the SDP. **Workaround:** Configure the session keepalive value on egress greater than ingress.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126608	SBX-125710 (9.2.5)	3	SBX-125710 - SBC wipes out dialog stateful variable after ignoring a SIP message by SMM action "ignore" **Impact:** The SMM's dialog variable is lost after ignoring the 18x message by the SBC. **Root Cause:** The dialogType in the transaction was set as invalid after ignoring the 18x. This results in the deletion of the dialog scope variable as part of the cleanup action. **Steps to Replicate:** 1. Set up a basic SIP-SIP call with a SMM dialog scope variable. 2. Send an 18x with SDP and then send an 18x without SDP. 3. Verify that the dialog scope variable exists even after ignoring the second 18x.	The code is modified to update the dialogType variable correctly to INVITE and check if it is a SMM generated PRACK, then do not delete the dialog scope variable. **Workaround:** None.
SBX-126613	N/A	2	Support for optional ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 **Impact:** Support ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384. **Root Cause:** The ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 is not supported by the SBC. **Steps to Replicate:** Configure the TLS profile to use the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, and run SIP-TLS calls. Ensure the selected ciphersuite for the TLS session is TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384.	The code is modified to provide ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 support. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126672	SBX-126428 (10.1.6)	2	The SBC 7000 is acting as P-CSCF. IMS AKA does not work when UE expects server-initiated authentication **Impact:** The SBC sends 488 when Register is received without Security Client header. **Root Cause:** This is a design issue, missed the requirement to send 421. **Steps to Replicate:** Send a Register without a security client header when IPsec-3gpp is enabled.	The code is modified to send 421 in this scenario. **Workaround**: Use the SMM to send 421 instead of 488. This fix works only when sbxSecMode is set to sbc-pcscf.
SBX-126750	SBX-124245 (10.1.5)	2	Force VoLTE subscriber deregistration if PCRF indicates Abort Session Request **Impact:** When the SBC receives an ASR (Abort Session Request) through the Rx interface from PCRF, only the Diameter RX session is terminated but does not force de-registration. As a result, the active registrations are torn down only when the registration timer expires which might end up being several hours or days later. **Root Cause:** There was no handling by the SBC to trigger a de-registration after the PCRF notifies ASR through the Rx interface. **Steps to Replicate:** 1. Configure the SBC as a P-CSCF and establish a diameter Rx session with PCRF. 2. PCRF notifies ASR (Abort Session Request) to the SBC through the Rx interface. 3. The SBC receives an ASR but does not force a de-registration and only terminates the diameter session.	The code is modified to handle the following actions when an ASR is received for the diameter Rx session: 1. Tear down any call(s) from the registered UE 2. Trigger deregistration towards the SBC core. 3. Log the correct disconnect reason and the expires value as 0 for the register STOP EVENT record. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126754	SBX-125326 (10.1.5)	2	The P-CSCF Rx interface support of Subscription of Notification of Signaling Path Status **Impact:** When the “provSignalingFlow“ flag is disabled, the SBC doesn’t include the Media-Component-Description AVP in the AAR (Authorization Authentication Request) message. As per standard, when provSignalingFlow is disabled, the SBC should send the Media-Component-Description AVP with the Flow-Number as “0”. **Root Cause:** There was no handling by the SBC to send the Media-Component-Description AVP in AAR when the “provSignalingFlow“ flag is disabled. **Steps to Replicate:** 1. Configure the SBC as a P-CSCF with the “provSignalingFlow“ flag disabled and establish a diameter Rx session with PCRF. 2. Observe the AVPs sent in the AAR. 3. The Media-Component-Description AVP is missing in the AAR message.	The code is modified to send the Media-Component-Description AVP in AAR with the Flow-Number as “0” and the Flow-Usage: AF_SIGNALLING. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126760	N/A	2	Output of the "show table/status system ethernetPort packetPortStatus <host_name> pkt0/pkt1" command is not proper. **Impact:** The "show table/status system ethernetPort packetPortStatus <host_name> pkt0/pkt1" command output is not proper **Root Cause:** The packetPortStatus hostname key uses the Actual CeName, and get_object implementation was expecting CeName as the key. **Steps to Replicate:** 1. Run "show table/status system ethernetPort packetPortStatus <host_name> pkt0/pkt1" command. 2. Verify the output.	The code is modified to allow the CeName/ActualCeName. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126856	SBX-125974 (10.1.5)	2	Creating duplicate sipTrunkGroup overwrites mediaIpInterfaceGroupName on the original sipTrunkGroup **Impact:** The EMA does not display any error when trying to a create a sip trunk group with a name that already exists and changes some but not all values in the existing one to defaults. **Root Cause:** The EMA uses netconf interface to create sip trunk group and the interface does not provide capability to differentiate between create and edit operation. As a result, if we try to create a SIP trunk group with a name that already exists then the netconf interface treats the request as an update request, which results in the modification of existing SIP trunk group. **Steps to Replicate:** 1. Log into the EMA 2. Create a SIP Trunk Group with name "STG-1" 3. Create another SIP Trunk Group with the same name "STG-1" An error message is displayed in the UI.	The code is modified to check if an entry already exists or not, if yes then an error message is displayed to the user. **Workaround:** None.
SBX-126953	SBX-126875 (11.1.2)	2	ScmP cores repeatedly **Impact:** The SCM cores while SIPSG is processing registration sub elements. **Root Cause:** The code was missing a NULL pointer check. **Steps to Replicate:** The root case was found by code inspection.	The code is modified to add a NULL pointer check to prevent the core. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-126974	N/A	2	The SBC/SLB Mgmt Client status is showing as "Configuration Failed" **Impact:** The SBC/SLB Mgmt Client status is showing as "Configuration Failed" **Root Cause:** In 1:1 HA, sometimes the instanceup notification is sent simultaneously from the LCA Registration and sbxCleanup.sh scripts. **Steps to Replicate:** Reported use-case.	The code is modified to drop the second notification attempt if the first one is in progress. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127017	N/A	2	The feature "Short-duration RTP inactivity timer for emergency calls " implemented is not working as expected in failover scenarios. **Impact:** Stable calls are torn down during an SBC switchover when "Media Peer Inactivity Timeout" is configured in less than 6 seconds. **Root Cause:** With inactivity timer values from 1 second to 5 seconds, during a failover, the media inactivity is detected by the SBC that is failing over. The media flow has switched to the new active SBC. However, the old active SBC is still not fully down and detects inactivity when the timer values are low. This leads to the call disconnecting on a switchover. **Steps to Replicate:** Configuration: 1. Bring up the SBC HA pair with a release running 10.1.x or later 2. Configure route PSP with "Media Peer Inactivity Timeout" as 1 second. 3. Configure route PSP with "Peer Absence Action" as "Trap And Disconnect". Steps: 1. Place call between two endpoints via SBC with both endpoints sending media packets.	The code is modified to disable the inactivity detection on the node applied earlier when going down. **Workaround:** Configure "Media Peer Inactivity Timeout" as 6 seconds or more.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. Once a call is marked as Stable, perform a switchover for the SBC using the CLI: request system admin <name> switchover Expected Behavior: • After a switchover, the call remains stable on the new active SBC. Actual Behavior: • After a switchover, the call is disconnected by the SBC.	
SBX-127065	SBX-122079 (11.1.1)	2	Ingress and Egress Last Measurement for Latency CDR values mismatch. **Impact:** RTCP measured roundtrip reporting couple of milliseconds (false) latency, where as network used, or the SBC media processing is not really causing that delays. **Root Cause:** DPDK TSC clock updates are lagging by few milliseconds per second, observable with RTCP gen seconds durations usage (otherwise not an issue/noticeable for small intervals use cases). RTCP DLSR measures missing the milliseconds are causing RTT latencies and false reports. This is observed after Linux kernel/ DPDK upgrades, which caused other performance issues also in this release. **Steps to Replicate:** Run RTCP termination/generation call flows, where SR, RR RTCP packets exchanged from SBC's computes and report RTT latencies in records.	The code is modified to use the Linux system clock for better accuracy, With this new clock source, RTT latencies computation is fine and no false latencies are reported. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127096	SBX-127070 (10.1.4)	3	Switchover occurred because of IM Process core **Impact:** The IM Process cores due to memory corruption while processing Lawful Intercept related data. **Root Cause:** The core was caused by memory corruption. The memory corruption was the result of the code copying into a buffer that was large enough. The code was re-using an existing buffer that was not large enough for the PDU that was copied into it. **Steps to Replicate:** The steps are not reproducible.	The code is modified to no longer reuse an existing buffer for storing the PDU. The code now frees the original buffer and allocate a new one (which is large enough for the PDU). **Workaround**: None.
SBX-127189	SBX-126663 (12.0.0)	2	High-level noise is heard on the G.711 leg of an EVS-G.711 call after packets stop arriving for a few seconds on the EVS leg. **Impact:** The SBC generates a high level of noise when no packets are fed to the EVS decoder when in non-DTX (Discontinuous transmission) mode which is considered as a lost frame. **Root Cause:** An error in the API layer of the EVS decoder results in the “Bad Frame Indicator” flag not getting set in case of lost frame. This results in the EVS decoder taking the CNG path instead of the PLC path. **Steps to Replicate:** 1. Run an EVS to G711 call. 2. Stream media with packet losses on the EVS leg. 3. Capture the media on the G711 leg. 4. The media captured on the G711 leg should not have any occurrences of a high level of noise.	The code is modified to xix the API layer such that the Bad Frame Indicator is set in the case of frame loss so that Packet Loss Concealment takes its place. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127256	N/A	2	An incorrect CEName reported by the SBC **Impact:** An iIncorrect CEName reported in some statistics. **Root Cause:** The RGM node name is reported in some statistics for CeName. The CeName is picked from interface metavariables (RGM node name). **Steps to Replicate:** Test the reported statistics.	The code is modified to properly populate actualCeName. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127394	SBX-127007 (10.1.5)	3	A Quick re-registration on an Alternate SIP Server when the Primary Server is down does not work if the TLS transport is used between the SBC and the registrar **Impact:** Quick re-registration on alternate SIP server when primary server is down (known as Registrar Recovery) does not work if TLS transport is used between the SBC and the registrar. Although the SBC blacklists the primary registrar once it becomes unavailable, the SBC never re-registers the users to the alternate registrar. The SBC does reply with a SIP 503 message to REGISTER refresh messages instead of re-registering the endpoints to the alternate registrar: eventually the registrations times out. **Root Cause:** The SBC uses the configured port number used for UDP/TCP transport (here 5060) instead of the port number used for TLS transport (here 5061) when the Registrar Recovery checks the registrar's availability. As a result, the Registrar Recovery feature cannot detect the unavailability of both registrars and considers the primary registrar as available all the time. **Steps to Replicate:** 1. Enable the Register Recovery feature in the IP signaling profile that is assigned to the trunk group between the SBC and the registrars. Enable SIP over TLS on this trunk group. 2. Once the endpoints are registered, create a condition in which the primary registrar is blacklisted (i.e. SIP OPTIONS pathcheck pings time out or fail).	The code is modified so the Registrar Recovery feature uses the port number used for TLS transport when checking for the registrars' availability. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			3. Upon the next internal registration refresh, the SBC is unable to detect that the primary registrar has been blacklisted and the SBC replies back with a SIP 503 message. The registration may time out afterwards.	
SBX-127476	SBX-127437 (10.1.0)	2	Federal_Phase_2_Consult_Transfer : Consult transfer call fails when REFER "with" replaces "is" received on the SBC **Impact:** The SBC is not able to correctly handle REFER with embedded information when there are extra attributes following the "from" tag: Refer-To: <sip:6132120002@uc.com:5061;user=phone;transport=tls;nt_server_host=172.29.29.114:5061?replaces=1b142f22a82e25c674745f13215184774b59e0f272%40172.29.29.114%3bto-tag%3dgK04808bb2%3bfrom-tag%3d999D6644-1118528D%3bnt_rid> **Root Cause:** The code to parse the "replaces" attributes was only expecting to have the callId, the from-tag, and the to-tag. The additional attributes were added to the end of whichever of these attributes was last parsed. **Steps to Replicate:** Make a SIP call and then send the REFER with an embedded "replaces" and confirm that the SBC is able to process it correctly.	The code is modified to correctly terminate the from-tag information when a semi-colon is found to indicate the start of a new parameter. **Workaround:** Use SMM to remove the extra embedded parameters following the from-tag.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127500	SBX-127177 (12.0.0)	2	IPv6 route entries are not displayed from the sHelml command "# ip -6 route" **Impact:** There were no entries shown from Linux SHelml command "# ip -6 route". **Root Cause:** The SBC 5.10 kernel was missing changes to handle the IPv6 route entries. **Steps to Replicate:** Use the "# ip -6 route" command, and check the displayed IPv6 routes.	The code is modified to allow the Linux 5.10 kernel to display the IPv6 route entries shown by the "ip -6 route" Linux SHelml command. **Workaround:** Use the "# route -6" Linux sHelml command to display the route entries.
SBX-127504	SBX-126724 (12.0.0)	2	BFD Switchovers during idle or traffic have increased with 12.0 **Impact:** Packet port switchover observed by customer due to BFD reply timeouts. **Root Cause:** The BFD daemon was not getting enough CPU cycles when it is pinned to the mgmt core. **Steps to Replicate:** The user should not observe any false packet port switchovers where the BFD is used for link monitoring.	The code is modified to change the BFD daemon CPU affinity set to signaling cores. **Workaround:** None.
SBX-127513	SBX-127267 (10.1.5)	3	There is an SBC switchover from A to B due to the SCM Process core **Impact:** The SCM process cored while processing an STI Response from Diameter. **Root Cause:** The SCM cored due to accessing a NULL pointer while processing a corrupt STI Response from Diameter. **Steps to Replicate:** The steps are not reproducible.	The code is modified to prevent NULL pointer access. A separate fix is added to investigate why the SCM has received a corrupt/misaligned STI Response from Diameter. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127547	SBX-126429 (10.1.5)	2	The current active SBC is slowly leaking memory in the SCM Process **Impact:** The SCM is leaking memory while processing a re-INVITE when the Rx feature is enabled. **Root Cause:** While processing a re-INVITE, PCRF related code is overwriting a pointer to a Packet Service Profile while allocating a new one. Overwriting the pointer prevents the structure from getting freed when the call is completed. **Steps to Replicate:** 1. Enable pcrfCommitment flag in SIP Trunk Group. 2. Run load with calls that involve a re-INVITE. 3. Check for memory leak.	The code is modified to avoid overwriting pointers that can lead to a memory leak. The code with now check that the pointer is freed before overwriting the pointer. **Workaround**: Disable the PCRF Rx Feature by setting pcrfCommitment flag to “none”.
SBX-127590	SBX-127086 (10.1.4)	2	No audio on media loopback calls after switchovers - the SBC uses an invalid destination MAC address on the media loopback call leg **Impact:** SWe only: If SBC SWe switches over, the new media loopback calls have one way audio. **Root Cause:** In the change done for SBX-126722, the destination MAC address was not always updated correctly in the route structure of the media loopback call leg. **Steps to Replicate:** In HA redundant setup: 1. Make two long duration media loopback calls and check the audio. switchover to redundant slot, and check the audio 2. The SBC should not deliver one way audio. 3. Make another set of media loopback calls, and observe one way audio.	The code is modified to correct the related code in XRM. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127617	N/A	2	RAMP is unable to display license usage since SBC generates delayed file **Impact:** RAMP was not able to display the license usage. **Root Cause:** RAMP shows the license usage by reading the pm stats file that OAM generates. OAM was delayed in generating the file, which causes the issue. **Steps to Replicate:** Register an SBC CNe deployment with RAMP and verify the license usage with calls.	The code is modified to unregistered the stubbed module from respective pod for stats. **Workaround:** None.
SBX-127783	SBX-127609 (10.1.5)	3	Syntax error is coming from the SBC when Userpart contains # and F **Impact:** The SBC treat userpart of SIP-URI with character E and F as syntax error. **Root Cause:** The Sipparser is not supported. **Steps to Replicate:** Run an incoming call with from header (SIP-URI) has character E and F in userpart.	The code is modified to support character E and F in userpart of SIP-URI. **Workaround:** None.
SBX-127828	N/A	3	The file does not generate on both config drives **Impact:** When running createConfigDrive.py using the file option and supplying an input file the script only creates the standby config drive **Root Cause:** Values for key 'haMode' from the input file do not match with the condition check in the script file. **Steps to Replicate:** The steps are not reproducible.	The code is modified to change values for the key 'haMode' in the script according to the input file values and for the CLI mode. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127839	SBX-126018 (9.2.5)	2	SBC 9.2.5R4 fail-over with Core **Impact:** The ScmProcess cores (9.2.5R004) and causes fail-over. When crankback calls were retried on the TLS trunk groups, because of repeating failures, the message was not sent and the SBC makes infinite retries. An internal structure was accumulating attempted route data in an unbounded way. **Root Cause:** There was no check in the code path on the number of attempts before adding and attempting subsequent routes **Steps to Replicate:** The issue is not reproducible.	The code is modified to add an internal limit of 10 applied to wherever calls are redirected or cranked back. This is now checked when adding the route to the list of attempted routes. If the issue occurs, the following log will appear with the GCID - "CcCrankBackCallStart: Attempted Route lists exceeded CPC_ROUTES_MAX" **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127851	SBX-125715 (11.1.2)	2	DSP Transcoding not initiated with different telephone-event PT bitrate call flow in SBC vV10.01.02R001 and above **Impact:** The SBC does not transcode the call for a difference in 2833 PTs when the codec in use (Opus) has a clock rate of 48000. **Root Cause:** The DTMF clock rates other than 8k and 16k are not handled under the "Different 2833 Payload type" flag-based transcoding logic. This results in the SBC setting up the call as a pass-through when 48k DTMF PT differs on both sides. **Steps to Replicate:** Configuration: 1. Enable transcoding for Opus-Opus along with other codecs. 2. Enable the following flag at Route PSP: packetToPacketControl -> transcode -> conditional -> conditionsInAdditionToNoCommonCodec -> different2833PayloadType enable	The code is modified to handle other DTMF clock rates and invoke transcoding if 2833 payload type is different. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			3. Configure PreferredRtpPayloadTypeForDtmfRelay as 101 on both route PSPs. Steps: 1. UAC sends INVITE to the SBC with the following SDP: m=audio 6000 RTP/AVP 107 8 0 18 9 96 101 102 103 a=rtpmap:8 PCMA/8000 a=rtpmap:0 PCMU/8000 a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no a=rtpmap:9 G722/8000 a=rtpmap:96 AMR-WB/16000 a=fmtp:96 mode-set=0,1,2; mode-change-capability=2; max-red=0 a=rtpmap:107 opus/48000/2 a=fmtp:107 maxplaybackrate=16000; sprop-maxcapturerate=16000; minptime=10; useinbandfec=1; maxaveragebitrate=20000 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=rtpmap:102 telephone-event/16000 a=fmtp:102 0-15 a=rtpmap:103 telephone-event/48000 a=fmtp:103 0-15 a=sendrecv a=ptime:20	

Issue Id	Original Issue	Sev	Problem Description	Resolution
			2. The SBC egresses out an INVITE with the following SDP (note that in egress, INVITE 102 is used for the 48k DTMF and 103 for the 16k DTMF) m=audio 1030 RTP/AVP 107 8 0 18 9 96 101 102 103 a=rtpmap:107 opus/48000/2 a=fmtp:107 maxplaybackrate=16000; sprop-maxcapturerate=16000; minptime=10; useinbandfec=1; maxaveragebitrate=20000 a=rtpmap:8 PCMA/8000 a=rtpmap:0 PCMU/8000 a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no a=rtpmap:9 G722/8000 a=rtpmap:96 AMR-WB/16000 a=fmtp:96 mode-set=0,1,2; mode-change-capability=2; max-red=0 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=rtpmap:102 telephone-event/48000 a=fmtp:102 0-15 a=rtpmap:103 telephone-event/16000 a=fmtp:103 0-15 a=sendrecv a=ptime:20 3. The UAS sends a 200 OK with the following SDP: m=audio 41678 RTP/AVP 107 102 a=rtpmap:107 opus/48000/2 a=fmtp:107 maxplaybackrate=16000; sprop-maxcapturerate=16000; minptime=10; useinbandfec=1; maxaveragebitrate=20000 a=rtpmap:102 telephone-	

Issue Id	Original Issue	Sev	Problem Description	Resolution
			event/48000 a=fmtp:102 0-15 a=sendrecv a=ptime:20 Without Fix: The SBC sets up the call as a pass-through and sends a 200 OK answer to ingress with the following SDP: m=audio 1028 RTP/AVP 107 102 a=rtpmap:107 opus/48000/2 a=fmtp:107 maxplaybackrate=16000; sprop-maxcapturerate=16000; minptime=10; useinbandfec=1; maxaveragebitrate=20000 a=rtpmap:102 telephone-event/48000 a=fmtp:102 0-15 a=sendrecv a=ptime:20 With Fix: The SBC sets up the call as a transcode and sends a 200 OK answer to ingress with the following SDP: m=audio 1028 RTP/AVP 107 103 a=rtpmap:107 opus/48000/2 a=fmtp:107 maxplaybackrate=16000; sprop-maxcapturerate=16000; minptime=10; useinbandfec=1; maxaveragebitrate=20000 a=rtpmap:103 telephone-event/48000 a=fmtp:103 0-15 a=sendrecv a=ptime:20	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127856	SBX-126680 (9.2.5)	2	REGISTER EVENT CDR with 488 response **Impact:** A sends register request to B. Before receiving 200 Ok for the register request, C sends a subscribe request for A. As the registration is still not stable, the subscribe request receives a 488 Not Acceptable here, this is expected behavior. But in the Event CDR, the event for SIP TXN Status 488 Not Acceptable Here is associated with REGISTER i.e., "REGISTER,488", when it should be for SUBSCRIBE. **Root Cause:** For the subscribe dialog when registration is unstable, the SBC invokes a registration event CDR instead of subscribe, as a relay CB (control block) is not available. **Steps to Replicate:** Set following: set oam accounting admin eventAcctState enabled set oam accounting admin eventAcctPsxInfoState disabled set oam accounting admin eventAcctMethods eventRegister enabled set oam accounting admin eventAcctMethods eventSubscribe disabled 1. A sends register to B. 2. Pause. 3. C sends subscribe for A, before A receives the 200 OK for register.	The code is modified to invoke the relay event with no CB, ensuring the event CDR is raised for SUBSCRIBE instead of registration **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			4. A receives 488 Not Acceptable here, as registration is unstable. Expected: no CDR event raised for 488 When Event Subscribe is enabled: set oam accounting admin eventAcctMethods eventSubscribe enabled Expected: Event CDR generated for SUBSCRIBE, i.e., "SUBSCRIBE,488"	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127883	N/A	2	Disallow unsupported algorithms/ encryption in the IKE/IPsec Protection Profiles as FIPS 140-3 complaint in the 12.1 build. **Impact:** Unsupported algorithms/ encryption in the IKE/IPsec Protection Profiles which should not get allowed after enabling FIPS 140-3. This functionality was not working as expected in the 12.1 build. **Root Cause:** The functionality was not supported in an earlier 12.1 build.	The code is modified so that the SBC will disallow unsupported algorithms/encryption in the IKE/ IPsec Protection Profiles. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			Steps to Replicate: The following code example will disallow the unsupported algorithms after FIPS is enabled: admin@lsbc1% set profiles security ikeProtectionProfile AesSha1IkeProfile algorithms dhGroup modp768 [ok][2023-11-07 21:57:42][edit] admin@lsbc1% co Aborted: 'profiles security ikeProtectionProfile': System is in FIPS mode, dhGroup can be set only to modp2048 and higher [error][2023-11-07 21:57:43][edit] admin@lsbc1% set profiles security ikeProtectionProfile AesSha1IkeProfile algorithms dhGroup modp1 Possible completions: modp1024 modp1536 admin@lsbc1% set profiles security ikeProtectionProfile AesSha1IkeProfile algorithms dhGroup modp1024 [ok][2023-11-07 22:00:57][edit] admin@lsbc1% co Aborted: 'profiles security ikeProtectionProfile': System is in FIPS mode, dhGroup can be set only to modp2048 and higher [error][2023-11-07 22:00:58][edit] admin@lsbc1% set profiles security ikeProtectionProfile AesSha1IkeProfile algorithms dhGroup modp1536 [ok][2023-11-07 22:01:08][edit] admin@lsbc1% co Aborted: 'profiles security ikeProtectionProfile': System is in FIPS mode, dhGroup can be set only to modp2048 and higher [error][2023-11-07 22:01:09][edit] admin@lsbc1% set profiles security ikeProtectionProfile AesSha1IkeProfile algorithms dhGroup modp2048 [ok][2023-11-07 22:01:40][edit] admin@lsbc1% co No modifications to commit. [ok][2023-11-07 22:01:41][edit] admin@lsbc1% co Commit complete. [ok][2023-11-07 22:01:46]	

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-127945	SBX-127939 (10.1.5)	2	ASAN error : heap-use-after-free observed in sanitizer log **Impact:** The code is reading from memory after it is freed. This issue exists when processing a 3xx message received on an egress GW and both the ingress and egress GWs are running 10.1.0 or higher code. **Root Cause:** The code maintained a pointer to an internal CPC data structure and was using this information to determine how much data is sent back across the GW-GW connection. Unfortunately, as the 3xx parameters are processed, the code reallocated the memory block where the CPC data structure is local due to adding more CPC structures and needed a larger memory block. While its unlikely that the old memory block is reallocated in this code flow, it is not good for the code to accessing this now invalid memory as could result in code reading the wrong size allowed for the GW-GW buffer and the 3xx may not process. **Steps to Replicate:** Make a GW-GW call where the 3xx message arrives with embedded contact headers.	The code is modified to take a local copy of the information to avoid accessing a pointer in a reallocated memory block. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128059	SBX-127084 (10.1.5)	3	There is different behavior of From header after FUP (V9 -> V10) **Impact:** The DM/PM rules on the PSX were not taking effect, when the calling party number was treated as anonymous. This resulted in the SBC setting the From Header to: From: <sip:anonymous@anonymous.invalid>;tag=xxxxx instead of the intended value passed down from the PSX From: <sip:Anonymous@Anonymous.invalid>;tag=xxxx **Root Cause:** As part of SBX-101165 feature changes in 10.0 the functionality was intentionally changed so the privacy profile took precedence over the DM/PM rules from the PSX when the calling party number was to be anonymized. **Steps to Replicate:** On the PSX configure DM/PM to do the following: 1. Delete "From Display Name" 2. Userinfo will be set to anonymous 3. HostPort will be set to anonymous.invalid Then send in an INVITE that contains Privacy: id Check that the outgoing INVITE has the From header set to From: <sip:anonymous@anonymous.invalid>;tag=xxxxx	The code is modified to revert the changes made in SBX-101165 to allow DM/PM rules to still take precedence when the calling party number is marked as anonymous. **Workaround:** Use the SMM to correct the contents in the outgoing FromHeader.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128164	N/A	2	The SBC fails to fork the call to all configured destinations if the call comes in over the TLS; only the first destination rings. **Impact:** The SBC fails to fork the call to all configured destinations. If the call comes in over TLS, only the first destination rings. **Root Cause:** The TLS flag coming from SIPFE has the same value as the forking flag in SIPSG. The check for native forking is failing and is not saving the data. **Steps to Replicate:** Configure the SBC with call forking. Send an INVITE to the SBC with transport TLS. Expected: The forking is successful, and the call is sent to all parties.	The code is modified to display the correct enumeration. **Workaround:** None.
SBX-128234	SBX-127848 (10.1.6)	2	The SBC removes the phone context from R-URI when TO transparency is enabled **Impact:** When the TO header transparency is enabled, the SBC does not include the Phone-Context in RURI. **Root Cause:** The current code prevents adding the Phone-Context in RURI if the TO header transparency enabled. **Steps to Replicate:** 1. Enable TO header transparency and configure a call with globalization. 2. Make a call. 3. Verify that RURI has phone-context parameter.	The code is modified to ensure the transparency headers are independent from other headers. As well, the code to allow adding a Phone-Context in RURI is removed. **Workaround:** Use SMM to remove the Phone-Context if needed.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128245	N/A	2	The SWe NP failed with mgt1 interface on a packet port redundancy KVM setup **Impact:** The SWe instance is unreachable with mgt1 interface and packet port redundancy. **Root Cause:** The SWe_NP fails because of the incorrect configuration populated by the startup script. **Steps to Replicate:** 1. Bring up SWe instance with mgt1 and packet port redundancy. 2. The SWe_NP fails to come up, and the instance is unreachable.	The code is modified to correct the startup script to populate the correct configuration. **Workaround:** None.
SBX-128271	SBX-128180 (11.1.2)	2	D-SBC Export/Import XML config file errors **Impact:** After an XML import into the "target" D-SBC Cluster, missing elements present on the SBC after validating the D-SBC XML export from the "source" D-SBC Cluster modify the XML for "target" D-SBC Cluster. **Root Cause:** The emaTarget snmp trapTarget object was getting partially exported which resulted in the import failing. The system congestion and overloadProfile were also not getting exported, so data was missing following the import. **Steps to Replicate:** Export a config and then import it - compare the elements configured.	The code is modified to improve import and export scripts to recognize when the seeded data is changed and to process all elements following a default element. **Workaround:** After exporting the configuration, the user can manually update the configuration to remove the partial emaTarget data to avoid import issues. The user can also manually add the congestion and overloadProfile data to the export file or to the SBC configuration following the import.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128277	SBX-126898 (11.1.2)	2	External Radius username not visible in audit logs v11.1.0 **Impact:** If a user logs into the EMA with a user validated via Radius, and that user is not a local user, then the username is blank for configuration changes in the Audit log. **Root Cause:** If a user logs into the EMA with a user validated via Radius, and that user is not a local user, then the session start notifications sent from confd to the ChmProcess do not contain the username. **Steps to Replicate:** 1. Enable Radius authentication. 2. Log into the EMA with a Radius user that is not a local user. 3. Make a configuration change via the EMA GUI. 4. View the current Audit log and ensure that the user and EMA client address is properly displayed. Ex: CHM: audit user: admin/00 12.345.678.90 port 12345 context: netconf /system/ policyServer/globalConfig/ reconnectTimeout: set to 102	The code is modified to display the proper username and client addresses for configuration changes in the Audit log. **Workaround:** None.
SBX-128305	N/A	2	Observing SYS ERR in hash.c while running CAC features **Impact:** A SYS_ERR observed in logs when the TG CAC feature suite was run. **Root Cause:** As part of the fix done for SBX-126339, IpHashRemove was replaced by IpHashInsert. Instead of removing the hash entry, the code tries to add an entry to the hash, thereby raising a SYS_ERR for duplicate entry **Steps to Replicate:** TG CAC feature test suite run.	The code is modified to replace IpHashInsert with IpHashRemove. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128309	N/A	2	IPsec IP XFRM policy is not getting replicated on Standby SBCs for N:1 upon first switchover **Impact:** Policy not replicated on Standby. **Root Cause:** The IPsec SPD was not getting updated in the standby SBC's context. **Steps to Replicate**: 1. Configure IPsec SPD in N:1 setup. 2. Perform a switchover. 3. Check the configured policy on newly active SBC with the following command: `/opt/sonus/bin/np/swe/IPsec-stat xfrm policy`	The code is been modified to update the SPD list in all the standby SBCs' contexts. **Workaround:** Disable and enable IPsec SPD state.
SBX-128341	SBX-124692 (10.1.6)	2	Add MAJOR level debugging for the error UasCallProgressCmd failed for callid=%s, gcid=0x%x, status= %d, ret= %d" **Impact:** SBC fails to send a status message in random cases. **Root Cause:** Unknown yet. **Steps to Replicate:** Not reproducible.	The code is modified to add more major logs where the message fails to send for further investigation. **Workaround:** None.
SBX-128462	N/A	2	Observed Prs process crash in MSBC while running load with 50cps of MSRP load on build 15309 **Impact:** The Prs Process cores due to a time cancel issue. **Root Cause:** The timer cancel was coded inside the expiry function of that timer, which is wrong as the expired timer does not need a cancellation, so a non set timer was used to cancel. **Steps to Replicate:** Run a load with 50cps of MSRP load.	The code is modified to remove the cancel timer code from the expiry function of that timer and marked the saved timer id as INVALID. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128508	SBX-127835 (10.1.6)	2	The SBCs are leaking UDP ports - calls and registrations failing after all ports are exhausted **Impact:** The UDP ports were leaked when usePortRange is enabled under registration failing case, which exhausts all call ports. **Root Cause:** There are 2 issues here: 1. The registration ID and usePortRangeFlag in SIPFE server RCB are updated by the SIPSG when the registration is completed. SIPFE checks usePortRangeFlag to determine whether to free corresponding PORT_RANGE_CNX_CB or not. If the registration fails, both the registration ID and usePortRangeFlag stay at zero and causes the PORT_RANGE_CNX_CB to not free and UDP port leaked in XRM. 2. With additional support added for SLB, a new field, egressSigPortId, is added before ulRegistrationId that causes the SipFeProcessPortRangeCnxCloseReq() to always send zero registration ID when trying to close the port range connection in non-SLB configuration. **Steps to Replicate:** 1. Enable the usePortRange in egress SIP TG. 2. Use XRM debug command to see the initial UDP port usage. 3. Send SIP REGISTER. 4. Reply with 403. 5. Wait for registration to timeout and free up. 6. Repeat Step 2 to see UDP port usage after registration is cleared. 7. Repeat Step 3 to 6.	The code is modified so: 1. The usePortRangeFlag works correctly when deleting the unstable registration. 2. The egressSigPortId moves after ulRegistrationId to ensure the registration ID is always the first field after the ICM header in the message. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128516	N/A	2	Observed MAJOR logs in the MSBC while running a load with 10 cps of MSRP load (64kb of message size) and 100 cps of Audio call load on build 15339 **Impact:** The MicroFlow and ACLs do not get freed even after the sockets is closed. **Root Cause:** While the Shutdown in progress, if BYE comes then the mres goes to the "free" Statefree so there was no code to free the microflow after the ACK or FINACK timer expires. **Steps to Replicate:** 1. Send BYE from PEER when the SBC is waiting for LAST ACK. 2. The Microflow should get deleted.	The code is modified to allow the expiry functions to delete the microflows in such cases. **Workaround:** None.
SBX-128537	SBX-128301 (10.1.6)	2	Running the regex for wildcard RCB lookup causes the SAM to crash. **Impact:** The SAM Process may core during memory free routine when wildcard is used in AOR. **Root Cause:** The SBC accesses memory using a NULL pointer. **Steps to Replicate:** Configure surrogate registrations and the answer from Registrar must contain multiple child registration AORs. The child AOR in the response contains a wildcarded AOR.	The code is modified to check valid memory before freeing it. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128578	N/A	2	[Burp Security Scan]: Password field with autocomplete enabled **Impact:** In the Radius Server screen, autocomplete is enabled on the password field Shared Secret. **Root Cause:** The autocomplete property on the password field Shared Secret is not set to false. **Steps to Replicate:** 1. Log into the EMA. 2. Navigate to the Radius Server screen. 3. Click on the Password field Shared Secret. 4. Autocomplete text should not get shown.	The code is modified to set autocomplete to false on the password field. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128608	SBX-128548 (10.1.6)	3	An Incorrect Value is getting populated in CDR when PAI header contains Tel URI where display name contains a COMMA **Impact:** The SBC does not escape the COMMA present in the display name of PAI header containing a Tel URI. **Root Cause:** The code is not present to escape COMMA present in the display name of PAI header containing Tel URI. This results in an incorrect value getting populated in CDR sub-field 12 and the same incorrect value is overwritten in the next sub-field 13. **Steps to Replicate:** 1. Make a basic SIP call with the PAI header in INVITE listed below: P-Asserted-Identity: "Lamoda, Test" <tel: +1234567890;cpc=ordinary> 2. Send a 486 error response from server script. 3. Verify the ATTEMPT CDR field "Displayname of Tel URI PAI header" is properly updated with first 11 characters of display name. COMMA replaced with %2C. %2C is considered as single character.	The code is modified to convert COMMA with %2C. The %2C is considered as 1 character. **Workaround:** SMM rule to delete COMMA from Display name of PAI Header.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128773	SBX-128430 (10.1.6)	2	Call transfer - OA timer expiry on A leg side of the call **Impact:** For some cases where there are multiple offer/answers on ingress and egress leg during call transfer, random calls may fail to transfer due to OA timer expiry. **Root Cause:** Before and during the bridging of an A-B call and its subsequent transfer to C, internal "modify" instructions are sent to the NRMA (Node Resource Manager). The NRMA handles outstanding "modify" requests individually, so numerous requests could cause a race condition with ignored messages. **Steps to Replicate:** 1. Run an A-B call where A and B have multiple offer/answer. 2. Refer B to C - C (180) trigger tone playing a 200OK.	The code is modified to suppress the internal 'modify' offer in this scenario as it is not necessary when playing a tone. **Workaround:** Disable the Tone on.
SBX-128775	N/A	2	Incorrect mapping of PCI slot ids and Pkt interfaces in port redundancy scenario. **Impact:** Inaccurate PCI slot ID mapping **Root Cause:** The SRIOV environment variables of the SC pod does not provide the accurate ordering of the PCI devices. **Steps to Replicate**: 1. Launch a 12.0 SBC CNe deployment using 12.0 release Helm chart with port-redundancy enabled for SC pod. 2. Observing the mapping of PCI slot IDs in /opt/sonus/conf/swe/.port_map.txt file and /etc/podinfo/network-annotation; the mapping will be disorganized. This incorrect mapping of PCI slot ID with the interface name results in unintended network topology of the solution.	Network annotation file(/etc/podinfo/network-annotations) is parsed to get accurate mapping of the PCI slot IDs with the corresponding interface. **Workaround:** None

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128782	SBX-128603 (10.1.5)	3	Access SBC switchovers **Impact:** The SCM cores because the code is in an infinite loop. **Root Cause:** A bug introduced in 10.1.3R2 resulted in overwriting a pointer to a Contact with a pointer to an already attempted Contact. As a result, the SCM ends up in an infinite loop because it repeatedly attempts to point to the same Contact. **Steps to Replicate:** Relay a SUBSCRIBE that includes Contacts, and the first Contact is blacklisted.	The code is modified to the newly added code so that it does not overwrite the existing Contact pointer. **Workaround:** None.
SBX-128783	SBX-128712 (11.1.2)	2	[TLS/SRTP] Standby SBC cores while triggered switchover during TLS/SRTP call. **Impact:** The TLS calls getting cleared after switchover, triggering a core. **Root Cause:** Some TLS calls are cleared after switchover due to a timing issue seen on the Standby when going active. **Steps to Replicate:** 1. Load the build V10.01.05-R000-1048 in the cloud HA-SBC. 2. Configure TLS-SRTP and integrate the SBC with PSX. 3. Trigger an A to B call, once the call is stable trigger a switchover using the command 'sbxrestart'. 4. Validate the call is properly working after the failover.	The code is modified to resolve the timing issue during switchover. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128866	N/A	2	The From header is not getting anonymized **Impact:** The From header is not getting anonymized in the following call flow: UAC — SBC1 — UAS | Redirector 1-->STI (Signing) When the SBC sends the INVITE to the SBC, it is not anonymizing the From header. **Root Cause:** In the test call flow, after the SBC gets the 3xx response from the redirector, it dips the routes' local policy engine (ERE). Use the ERE to send all the AVPs even if there is no modification of the AVP during the route processing, and the SBC uses the received AVP to form the from header. **Steps to Replicate:** Test Setup: UAC — SBC1 — UAS | Redirector 1-->STI (Signing) Configuration: 1. At the PSX, a. Deploy the PSX in SIP Redirector mode, which accepts the Initial INVITE sign based on the received SIP PDU by contacting the STI server and responding with a 3xx response with an embedded identity header in the Contact header. 2. At the SBC, a. Configure Ingress PP with passThruPrivacyInfo enabled and attach it to ingress TG.	The code is modified not to send the URI AVPs if it is not modified during the D+ request processing. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
			b. Configure the Egress PP with only supportPrivacyUser set to ifRcvdUserorIdorBoth and attach it to egress TG towards UAS (TG_OUT1_SBX106615). c. Include Privacy in Egress IPSP. 3. Enable the Include Privacy in IPSP in Redirector TG. Enable EnhancedRequeryRedirection	
SBX-128898	N/A	2	Unable to perform LSWU to latest 12.1 build via Platform Manager. **Impact:** The SBC is unable to perform LSWU from the 12.1 build. **Root Cause:** In the new version of php, there was a change in the way php function on an object was invoked. This change causes an error, which results in the upgrade failing. **Steps to Replicate:** 1. Log into the platform manager. 2. Try to perform a LSWU from one 12.1 A build to another. Upgrade should successfully complete.	The code is modified to correct the function invocation on an object **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-128907	N/A	2	Observing SYS ERR in Message.cpp while executing a testcase to check whether the SBC is generating traps 'sonusSbxPathCheckFqdnPeerIpV6EndpointDownNotification2' and 'sonusSbxPathCheckFqdnPeerIpV6EndpointUpNotification2' **Impact:** The SBC generates a SYS error when the DBM routine is invoked at the time of session update. **Root Cause:** The DBM routine was invoked for the VNF setup. **Steps to Replicate:** Run the procedure described in the test case.	The code is modified to add the necessary checks to prohibit the non-CNe setup from using the DB functions. **Workaround:** Run the test case in a CNe setup.
SBX-129038	SBX-127001 (12.0.0)	2	MRFP106 stays OOS and gets removed from RG group on Aug-9 **Impact:** MRFP106 becomes out of service permanently, and gets removed from the rg group. **Root Cause:** MRFP103 was restarted along with all nodes and OAM. During the restart, it hits a gluster issue since OAM was not up. As a result, the SMA RGM tables were not initialized due to an unsuccessful restart which made the CHM also crash causing it to send an RGM down event. Since the SMA was not updated with the RG info, the assigned role returned UNKNOWN and the SBC sets it to STANDBY to cause the role change in serf and RGM. **Steps to Replicate:** On reboot, the MRFP state should not have any issues	The code is modified to skip the RGM down event generation in this scenario **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129056	SBX-127677 (10.1.6)	2	Dialog-ID Transparency functionality: The SBC is not inserting Record-Route header in the 486 Busy Error Response **Impact:** There is a requirement from the customer that we have to add Record-Route in 4XX-7XX responses. **Root Cause:** The SBC not adding Record-Route in failure responses when dialog-Id transparency is enabled. **Steps to Replicate:** 1. Enable dialog Id transparency feature. 2. Make a call from A to B. 3. Reject the call (4XX) from B.	The code is modified to add Record-Route in failure responses when dialog-Id transparency is enabled **Workaround:** None.
SBX-129124	N/A	2	The TCP connection for the MSRP packet exchange between the client and server during hold was not connecting consistently **Impact:** Reconnection of TCP for MSRP was not getting established before and after hold. **Root Cause:** Even on socket deletion, the socket was not removed from the resId table which caused a clash when a new socket was opened and tried to enter that socket into the resId table. **Steps to Replicate:** Try a TCP connection with retries in the scripts and see the connections getting established once negotiation is complete.	The code is modified to remove the socket in the resId Table against a particular resID when the shutdown of socket is in progress. Also decreased the time for the LAST_ACK wait from 5secs to 3 ms (repeats 10 times) so that if received early the microflow and socket can get deleted without holding. **Workaround:** None.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129167	SBX-128919 (13.0.0)	2	Failed to Verify SBC sends OOD NOTIFY for 100 Trying for Monitoring CUCM User and PSTN User **Impact:** After receiving the Refer message, the SBC sends an INVITE with the same number in the To header and From header. **Root Cause:** New feature support was added to allow the SBC to send the Refer transfer number to the policy server when a new flag is enabled. As part of this change, the transfer number is sent in the policy request even when the control is disabled, causing the issue. **Steps to Replicate:** Make a call from A to B, then B transfers A to C by sending a REFER.	The code is modified to pass the Refer transfer number to the policy server only when the control is set. **Workaround:** None.
SBX-129281	SBX-128981 (10.1.6)	2	For second 18x with preconditions "none", SBC does not send UPDATE **Impact:** The SBC is not able to send the UPDATE to the forking and precondition call flow. **Root Cause:** SIPS treats the internal late offer queued as the same previous SDP. Therefore, it does not send out an Update. **Steps to Replicate:** 1. A (non precondition) call B(precondition required). B prime loopback to C. 2. C - forking, precondition transparency. 3. A-B interworking precondition.	The code is modified to ensure SIPS will send the UPDATE regardless of if the previous SDP is for precondition case. **Workaround:** Disable forking.

Issue Id	Original Issue	Sev	Problem Description	Resolution
SBX-129426	SBX-128937 (10.1.6)	2	Unable to login to EMA for SBC 5400 getting service unavailable **Impact:** The user is not able to log into the EMA after disabling the diffie-Helmlman-group14-sha1 algorithm. **Root Cause:** The Java library used by the EMA to log in supports only diffie-Helmlman-group14-sha1 algorithm, causing the log in to fail. **Steps to Replicate:** 1. Disable the diffie-Helmlman-group14-sha1 algorithm. 2. Log into the EMA. Log in should succeed.	The code is modified to update the library to the latest version which supports the newer diffie-Helmlman algorithms. **Workaround:** None.
SBX-129429	N/A	2	LSWU - failed when Upgrading the SBC from 10.1.4 R to 12.1.0 R via the Platform Manager **Impact:** SWe NP fails to come up occasionally in a Qcow2-based SBC SWe installation and upgrade. **Root Cause:** The udev rules file - /etc/udev/rules.d/70-persistent-net.rules) was not cleaned up (deleted) as part of the Qcow2 image creation, resulting in interface renaming issues when the PCI slot ID clashes with the target VM. (as in, when the udev rules conflict for the same PCI slot IDs). This issue is only encountered if the PCI slot IDs of interfaces during Qcow2 image creation matches with the PCI slot IDs of the interfaces in the target VM. **Steps to Replicate:** Instantiate/ Upgrade the SBC VM using qcow2 with the same PCI slot IDs as the one used in the qcow2 image.	The code is modified to clean up the interface renaming rules file (udev rules file) as part of qcow2 image creation. **Workaround:** If the issue is encountered with a fresh SBC VM instantiation, the VM will auto-recover by going for an additional reboot. Since an additional reboot results in upgrade failure in LSWU, there are no workaround for LSWU.

Known Issues

The following known issues exist in these releases.

Issue ID	Sev	Problem Description	Impact/Workaround
SBX-136333	2	Key not found for address context in sipRegCountDomainIntStats	**Impact Statement:** Stats are generated, but only the address context will be missing for each stats. **Workaround:** No workaround
SBX-136422	1	CNe-FR: Observing call failures post upgrade from 12.1.4-R001 to 12.1.5-142	**Impact Statement:** When ERE is used in CNF-FR, during upgrade, the Postgres schema in standby is getting replaced with the previous version during startup sync. The calls are getting dropped after upgrade **Workaround:** No workaround
SBX-136485	2	Audio+video Call not survived after SC Pod Switch Over	**Impact Statement:** Audio+video call not reconstructed after SC Pod Switchover. This happens only when RTCP is enabled on both the call legs. **Workaround:** No workaround
SBX-136701	1	CNF:[12.1.5R]: Calls are failing during active SLB pod rollback	**Impact Statement:** The new calls will be accepted after an exteneded time after a rollback The issue is intermittent and depends on the order on which the POD goes for restart. **Workaround:** No workaround
SBX-136708	2	SBC got stuck while downloading the configuration from Geo located RAMP	**Impact Statement:** Issue is specific to Geo located RAMP and SBC as the OAM is getting the fragmented packets from RAMP. **Workaround:** OAM docker restart will be required to download the configuration.

Known Limitations

The following limitations exist in this release.

Category	Limitations
SBC Core	RESTCONF 'limit' or 'offset' parameters are not supported in SBC 12.1.3R3 due to ConfD downgrade to 7.3.2. **parameters: offset and limit** The query parameters "limit" and "offset" which also exist in the REST API could also be used in RESTCONF. But these are deprecated and removed in ConfD-7.3. Later, tailf has reinstated the "offset" and "limit" query parameters with RESTCONF in confD 7.4.1. The SBC with confD 7.3.2 version will not support "offset" and "limit" parameters whereas SBC with confD versions above 7.4.1 will support this.
SBC SWe	The RAMP identifies the nodes based on the VNFC-ID. While instantiating SBC/PSX cloud nodes, ensure that you use a unique VNFC-ID only. If you reuse an existing VNFC-ID, RAMP treats this as a re-registration request and overwrites the existing data on the cloud node.
	The physical NIC connectivity must be in active state at the hypervisor level before starting the SWe instance on the SBC SWe platforms. In case of SWe instance with SR-IOV interfaces, manual restart of the SWe instance is required if physical NIC connectivity goes down while the instance is in progress.
	While configuring the SBC SWe Cloud instances, the CLIs commits successfully even if any metaVariable provided is incorrect. The SBC SWe Cloud instance cannot validate the CLIs, as the CDB configuration file is stored in the OAM Node and is shared among all the other SBC SWe Cloud instances in the cluster.
	When upgrading SBC SWe cloud instances from any release prior to 9.1 to release 10.0, you must update your Heat template userdata section to include mandatory SSH key information. An issue in OpenStack requires that you use the stack-update process rather than re-launch after updating the template, which leads to a new UUID for the instance. As a result, you must regenerate and apply new license bundles to the upgraded instances during the upgrade. Refer to Upgrading SBC SWe N:1 HA Nodes on OpenStack using Heat Templates for the relevant procedure.

<table>
<tr><th>Category</th><th>Limitations</th></tr>
<tr><td>SBC CNe</td><td>The following limitations exist in this release:
You can set the termination message only when the container knows the reason.
When Kubernetes restarts a container or a pod, the SBC does not control it, and the termination message can become inaccurate.
The new setting can fall back to the container log to catch the cases that are not in the control of the container.
The total message length across all containers is limited to 12 KiB, divided equally among each container. For example, if there are 12 containers (initContainers or containers), each holds 1024 bytes of available termination message space.
When the Kubernetes kills the pod or container, the reason is not identified. To learn more about the Kubernetes pod disruption conditions, refer to https://kubernetes.io/docs/concepts/workloads/pods/disruptions/#pod-disruption-conditions.
The following limitations exists for the Termination Message Policy value:<table><tr><th>Termination Message Policy Value</th><th>Limitations</th></tr><tr><td><code>FallbackToLogsOnError</code></td><td>If the termination message file is empty and the container exited with an error, it uses the last chunk of the container log output.
Log output is limited to 2048 bytes or 80 lines, whichever is smaller.</td></tr></table></td></tr>
<tr><td>D-SBC</td><td>The Antitrombone feature is not supported on the D-SBC.</td></tr>
<tr><td>S-SBC</td><td>Editing IP Interface is not reflected in the if configuration (ifConfig). This behavior is observed only on the S-SBC when action is set to "dryup" mode on the IP Interface. The IP address changes are not updated in the kernel and will not be displayed when ifconfig linux command is executed. In case of S-SBC, if the ipInterface configuration needs to be modified and if the action is set to "dryup" in ipInterface configuration, it must be set to "force" before disabling the ipInterface and making any changes.</td></tr>
<tr><td>EMA GUI</td><td>Due to a known EMA GUI issue, it can take up to 10 minutes to process and commit an SMM profile. This may be seen when the profile contains the max of 256 rules within it and provisioning of the SMM profile is being done using the EMA GUI. This will be fixed in a future release.</td></tr>
<tr><td>SNMP traps</td><td>The ACL is not installed to configure SNMP traps for accepting traffic. A dynamic ACL is added to configure SNMP traps. An ACL must be installed for SNMP traps for accepting traffic.</td></tr>
<tr><td>VNFM</td><td>GlusterFS was upgraded from 5.5 to 9.2 in SBC 11.1 due to OS upgrade from Buster to Bullseye. GlusterFS does not support an upgrade from release 5 to 9 and as a result, the automated upgrade of OAM is not possible in 11.1.</td></tr>
</table>

New in SBC 12.01.05R000

Declarative Provisioning

With the new Declarative Provisioning model, Ribbon leverages the power of the CI/CD pipeline for provisioning configuration data to Ribbon devices (SBC and PSX). This allows configuration management in a version-controlled manner. Administators using a GitOps environment with Ansible can update and validate configuration changes. This approach uses a centralized manager to track configuration data, configuration changes, and an auditable record of network updates. You can review details here.

For more information, contact your Ribbon Account representative.

In this section:

New Features in Release 12.01.05R000

The following table lists the new SBC Core features in release 12.01.05.R000.

	Feature ID	Overview
1	SBX-118961	**SBC CNe Support of ATCF-EATF-SRVCC Functionality** The SBC CNe provides support for ATCF, EATF, and SRVCC.
2	SBX-125325	**MCT Support on SBC CNe** The Media Capturing Tool (MCT) is a Ribbon solution for capturing media packets terminated on the SBC. The tool is utilized for various purposes, including complying with regulations, monitoring the quality of service of representatives, and storing call media for quality analysis. Previously, the MCT was only available on VNF deployments. To support the feature on the CNe, support is provided to the following requirements: • GCID is the unique identifier for the call. In VNF, the GCID was the unique identifier for the SBC and MCT tool. On the CNF, the GCID is no longer unique, and a call with the same GCID is hosted on more than 1 SC POD. The GUID is used as a unique identifier for the call instead. • With SLB front-ending the cluster, the INVITE received from the MCT server routes to the correct SC POD instance, which hosts the call that must be recorded. • CLI Triggered MCT recording is not supported on the CNe platform. For more information, refer to: • Monitor Target using MCT - CLI

	Feature ID	Overview
3	SBX-127049	**Support Zero Trust Security Concept and require-ro-rootfs Support** The zero trust standards are a security framework that assures authentication and authorization before access. With the correct configuration profile, the SBC CNe complies with the zero trust standards, and the default configurations on Kubernetes are now updated to comply to zero trust by default. The following configurations were updated so that new installations comply with zero trust, by default: 1. require-ro-rootfs is a read-only root file system policy that writes only to a mounted volume with a persistent state. An immutable root filesystem prevents malicious binaries from writing to the host system. To satisfy zero trust, the readOnlyRootFilesystem configuration is set to "true" by default for all SBC CNE containers. 2. restrict-automount-sa-token is a Kubernetes policy that automatically mounts service account credentials in each pod. These credentials may include roles that allow pods to access API resources. To remain consistent with a zero trust policy, this configuration will default to "true". **Note** To restrict access, set your system to opt out of auto-mounting tokens by configuring automountServiceAccountToken to "false". Only pods that do not communicate with the Kubernetes API can function when the automountServiceAccountToken parameter is set to "false". Because most of the pods need to access the Kubernetes API, it is not possible to set this flag as false, in most cases. For more information, refer to: • Zero Trust Framework in CNF Deployments
4	SBX-127456	**CNF Support for IMSLI Roundrobin Logic Handling and Multi-Country Support** In previous releases, the IMSLI feature worked on the CNe only with a single mediation server. When multiple mediation servers are configured, the interceptions are expected to round-robin between the configured set of mediation servers and the healthiest amongst the mediation servers; that is, a server with both X2 and X3 links up was preferred. Because the X2 and X3 were split into SG and SC POD respectively on the CNF, a solution is required to track both the X2 and X3 health to select the mediation server and is addressed as part of this feature. This feature supports IMS LI server load sharing and Multi-country LI for VoLTE IMS released on the CNe platform

	Feature ID	Overview
5	SBX-127668	**Support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256/ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 with TLS 1.2** The SBC Core 12.1.5 is enhanced to support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256/ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 with TLS 1.2 for TLS calls. For more information, refer to: • CLI Changes in This Release • TLS Profile - CLI • DTLS Profile - CLI • Security - TLS Profile • Security - DTLS Profile
6	SBX-128665	**IMS AKA/IPSec Scaling With NP Offload** IPsec processing was formerly accomplished in the Linux Kernel, which cannot be scaled up to support a higher registration rate and support a large number of subscribers. The Linux kernel only did packet encapsulation and IPSec header formation and performed IPSec policy/ state lookups, whereas NP did the actual packet encryption/decryption/ digest. For scaling the session support and packet crypto operations, NP now performs packet encapsulation and IPSec header formation by having SAD/SPD look-ups, that is, all the IPSec processing is offloaded to the NP. Another reason is that in CNe, Ribbon-specific kernel optimizations are unavailable; hence, the dependency on the Linux kernel for IPSec processing is removed. The IMS-AKA NP offload design will be used on all SBC SWe platforms, and the existing kernel-based design will be used on all hardware platforms. IKE-IPSec will continue to use existing kernel-based design in all variants. For more information, refer to: • SWe Active Profile - CLI • Show Status Address Context • Show Status System

	Feature ID	Overview
7	SBX-128829	**CNF Support of TG Based Registration Rate CAC** Beginning with this release, the SBC CNe supports configuring trunk group Call Admission Control (CAC) to limit the SBC CNe SIP registration count and rates for particular trunk groups. In other words, users can configure: • the total number of concurrent SIP registrations allowed for a trunk group, • the maximum allowed sustained ingress/egress rate (registrations per second) for initial SIP registrations (registerRateMax), and • the maximum allowed ingress/egress burst (above the allowed sustained rate) for initial SIP registrations (registerBurstMax). For more information, refer to: SIP Trunk Group - CAC - CLI
8	SBX-129349	**Application Tracing Enhancements** When call trace filter criteria are provisioned and a call meets the criteria, trace information is written to a tracing file by individual pods. This enhances the user's call debugging when the SBC is deployed as a microservice (CNE deployments). Each call will be identified with a globally unique number (GUID) and every POD that is involved in Call Processing must use this global Identifier to logs its debug information in to its trace file. This helps the debugger to fetch all debug information that belongs to a call from each pod by referring to the GUID. **Notes** • Tracing is not supported in LI. • Global Call Trace Syntax is supported in SLB.

	Feature ID	Overview
9	SBX-130195	**TG-Based Subscription/Non-Invite CAC Support in CNF** This feature allows administrators to limit the subscription count and the accepted rate on a particular trunk group by rejecting other subscriptions. The number of subscriptions never exceeds the configured limit and rate values. The SBC limits the acceptance rate of non-INVITE messages on a particular trunk group by rejecting other messages. The number of requests for other non-INVITE OOD messages also never exceeds the configured rate values. The subscription limit, rate, and non-INVITE rate values persist even after a CS pod switchover. Once the active pod comes up, it syncs the trunk group-level counts from all the RS pods and then makes CAC decisions based on the latest consolidated counts. During CS pod switchovers or when the pod is down for any reason, all subscription non-INVITE message requests are accepted while the pod is unavailable, even if the limit or rate values are configured. The parameters needed to limit these rates are already in the SBC but are only fully exposed in some deployments. For this update, these configurable limits are exposed in CNe SBC deployments and are now available for all deployments as a SIP Trunk Group CAC feature on both the egress and ingress arms. CNe SBC users who choose to make use of these features can find them documented under SIP Trunk CAC in the CLI: • subscriptionLimit • subscribeBurstMax • subscribeRateMax • otherReqBurstMax • otherReqRateMax SBC CNe users who make use of the EMA can find the configurations in Configuration > System Provisioning > Category: CAC Provisioning > Zone > CAC > Ingress or All > Address Context > Zone > CAC > Ingress, documented under CAC Provisioning - Zone - CAC, for both the ingress and egress: • Subscription Limit • Call Rate Max • Call Burst Max • Register Rate Max • Register Burst Max For more information, refer to: • SIP Trunk Group - CAC - CLI • SIP Trunk Group - CAC - Egress (EMA) • SIP Trunk Group - CAC - Ingress (EMA)

	Feature ID	Overview
10	SBX-131719	**Retry-after Header Support in 503 CAC Rejection Response in CNF** In instances of a Call Admission Control (CAC) rejection due to a 503-error response code for any reason, a retry-after header is introduced for normal calls to make additional connection attempts. The SBC will account for the configured retry-after values on the Ingress Trunk Group (TG) app while populating the 503-error response retry-after value. The feature is configured through two parameters in the CLI: 'retryAfterMin' and 'retryAfterMax'. After a normal call is rejected, the Retry-After header will generate a random retry-value value between these two configured values. Configuring either of the Retry-After values as zero disables the feature. This feature only applies to normal calls; using INVITE, REGISTER and non-INVITE messages is not supported. For more information, refer to: • SIP Trunk Group - CAC - CLI • SIP Trunk Group - CAC (EMA)
11	SBX-133438	**AWS SBC With 3 Subnets** Due to security policies, network operators may choose to limit the number of interfaces they manage on the subnets. SBC Core cloud deployments require at least four interfaces to function; mgt0, ha0, pkt0, and pkt1. To comply with these security requirements, the SBC SWe on AWS now allows networks to access the four subnets through three interfaces by allowing mgt0 to share an interface with either pkt0 or pkt1, as desired. Because mgt0 needs access to the public network (to send AWS REST API requests for IP movement and peer instance metadata access in HA scenario) the mgt subnet must overlap with a pkt subnet that has public network access. Ensure that the appropriate security group rules are configured for each interface when overlapping subnets. The corresponding flexibility to overlap subnets is available in CFN templates, which allows users to configure the security group rule independently of the subnet used for the interfaces.

	Feature ID	Overview
12	SBX-133604	**SLB CNF Support of Masking IP and Port** This feature ensures that calls route correctly when the SBC CNe SIP-Aware Front-End Load Balancer (SLB) receives a call request with a different IP address or port but the same AOR and zone ID. The SLB is enhanced to use the existing **Mask IP Addressfor Rcb** and **Mask Portfor Rcb** configurations to process calls using different IP addresses and/or ports than those used during the registration process with the SIP TG Registration flag **Require Registration** set to "Required." For more information, refer to: • CNF SLB Processing Calls Using Different IPs and Ports (SBC CNe Features Guide) • Zone - SIP Sig Port - CLI • Signaling Ports - SIP Sig Port (EMA)
13	SBX-134147	**RCB Selection Based on PPI, PAI or From Header** Legitimate calls may still trigger a 403 denial for customers subscribed to privacy services. This feature introduces the CLI flag rcbAorMatchBasedOnHdrs, which allows the INVITE message to connect according to matching header information. The flag can be configured to accept the INVITE according to the FROM header, the PPI header (P-Preferred Identity), the PAI header (P-Asserted Identity), or any combination. Header matches are prioritized in the same order they are added. For more information, refer to: • Zone - CLI • Zone - Rbc Aor Match Based On Hdrs - CLI • System Provisioning - Zone (EMA)
14	SBX-134824	**Support Up to 1500 CPS on VNF** The SBC SWe maximum is updated to up to 1500 CPS on VNF. **Support Notes:** • Only I-SBC is supported. • N:1 HA Mode is not supported. • Not supported on VMware.
15	SBX-89790	**SBC SWe Supports Operation in 64 vCPU VM** The SBC SWe now supports a VM resource profile up to, and including, 64 vCPUs. **Note**: The support of 64 vCPUs is limited to Release 12.1.5R0 and beyond. Refer to SBC SWe Perfomance Information for further details regarding expected CPS and concurrent session capacity increases.

	Feature ID	Overview
16	SBX-127402	**License Expiry Generates Alarm** The SBC will raise the existing alarm sonusCpLicenseBundleExpiredNotification once a day to alert the operator that the Domain Locked License has expired. This alarm continues until a valid license bundle is installed for the expired Domain Locked License feature. For more information, refer to: • sonusCpLicenseBundleExpiredNotification - CRITICAL

Configuration Changes in this Release

The following table summarizes the configuration changes in this release.

Configuration	Description
CLI	**SBX-127668 SBC Support for Transport Layer Security 1.2** The SBC Core 12.1.5 is enhanced to support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256/ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 with TLS 1.2 for TLS calls. **Command Syntax** `% set profiles security tlsProfile defaultTlsProfile cipherSuite1` `  Possible completions:` `  nosuite  rsa-with-3des-ede-cbc-sha  rsa-with-aes-128-cbc-sha  rsa-with-aes-128-cbc-sha-256` `  rsa-with-aes-256-cbc-sha  rsa-with-aes-256-cbc-sha-256  rsa-with-null-sha  tls_aes_128_gcm_sha256` `  tls_aes_256_gcm_sha384  tls_chacha20_poly1305_sha256  tls_dhe_rsa_with_aes_128_gcm_sha256` `tls_ecdh_ecdsa_with_aes_256_gcm_sha384` `  tls_ecdhe_ecdsa_with_aes_128_gcm_sha256` `tls_ecdhe_ecdsa_with_aes_256_cbc_sha384` `tls_ecdhe_ecdsa_with_aes_256_gcm_sha384` `tls_ecdhe_rsa_with_aes_128_cbc_sha` `  tls_ecdhe_rsa_with_aes_128_gcm_sha256` `tls_ecdhe_rsa_with_aes_256_cbc_sha384` `tls_ecdhe_rsa_with_aes_256_gcm_sha384` `tls_rsa_with_aes_128_gcm_sha256` `  tls_rsa_with_aes_256_gcm_sha384` **Command Parameters** N/A **Configuration Examples** `set profiles security tlsProfile defaultTlsProfile cipherSuite1 tls_ecdhe_ecdsa_with_aes_128_gcm_sha256` `set profiles security tlsProfile tlsProfileAS cipherSuite1 tls_dhe_rsa_with_aes_128_gcm_sha256`

Configuration	Description
CLI	**SBX-128665 IMS AKA/IPSec Scaling With NP Offload** • A new option `standard_slb_xlarge_profile` has been added for configuring an extra large profile for >2M microflows need, that is, for up to 10M IMS AKA subscribers in the `sweActiveProfile` CLI command `% set system sweActiveProfile name <standard_slb_xlarge_profile>` • The following new show command will display the number of IPSec SAs configured in NP in an address context: `% show status addressContext <addrCtxtName> ipsec npStatistics saCount` • The output of the existing `show` command to display microflow statistics will be modified to show the destination IP address of the microflow: `% show status system ipPolicing uFlowStats` **Command Syntax** **For <standard_slb_xlarge_profile>** `% set system sweActiveProfile name <standard_slb_xlarge_profile>` **For show status addressContext <addrCtxtName>** `% show status addressContext <name> ipsec npStatistics saCount` **For show status system ipPolicing uFlowStats** `% show status system ipPolicing uFlowStats`

Configuration	Description
CLI	**SBX-130195 TG Based Subscription/Non-Invite CAC support in CNF** This feature allows administrators to limit the subscription count and the accepted rate on a particular trunk group by rejecting other subscriptions. The number of subscriptions never exceeds the configured limit and rate values. The SBC limits the acceptance rate of non-INVITE messages on a particular trunk group by rejecting other messages. The number of requests for other non-INVITE OOD messages also never exceeds the configured rate values. The subscription limit, rate, and non-INVITE rate values persist even after a CS pod switchover. Once the active pod comes up, it syncs the trunk group-level counts from all the RS pods and then makes CAC decisions based on the latest consolidated counts. During CS pod switchovers or when the pod is down for any reason, all subscription non-INVITE message requests are accepted while the pod is unavailable, even if the limit or rate values are configured. The parameters needed to limit these rates are already in the SBC but are only fully exposed in some deployments. For this update, these configurable limits are exposed in CNe SBC deployments and are now available for all deployments as a SIP Trunk Group CAC feature on both the egress and ingress arms. CNe SBC users who choose to make use of these features can find them documented under SIP Trunk CAC in the CLI: **Command Syntax** `% set addressContext <addressContext_name> zone <zone_name> cac egress` `callBurstMax <"unlimited" or for SBC 5400/SWe: 1-900; SBC 7000/SBC CNe: 1-2700>` `callRateMax <"unlimited" or for SBC 5400/SWe: 1-450; SBC 7000/SBC CNe: 1-1350>` `registerBurstMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000>` `registerRateMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000>` `% set addressContext <addressContext_name> zone <zone_name> cac ingress` `callBurstMax <"unlimited" or for SBC 5400/SWe/CNF: 1-900; SBC 7000: 1-2700>` `callRateMax <"unlimited" or for SBC 5400/SWe/CNF: 1-450; SBC 7000: 1-1350>` `registerBurstMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000>` `registerRateMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000>` `% set addressContext <addressContext_name> zone <zone_name> sipTrunkGroup <sipTrunkGroup_name> cac` `subscriptionLimit <0-2147483647>`

Configuration	Description
	% set addressContext <addressContext_name> zone <zone_name> sipTrunkGroup <sipTrunkGroup_name> cac egress callBurstMax <"unlimited" or for SBC 5400/SWe: 1-900; SBC 7000/SBC CNF: 1-2700> callRateMax <"unlimited" or for SBC 5400/SWe: 1-450; SBC 7000/SBC CNF: 1-1350> otherReqBurstMax <"unlimited" or SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> otherReqRateMax <"unlimited" or for SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> registerBurstMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> registerRateMax <"unlimited or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> subscribeBurstMax <"unlimited" or for SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> subscribeRateMax <"unlimited" or for SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> % set addressContext <addressContext_name> zone <zone_name> sipTrunkGroup <sipTrunkGroup_name> cac ingress callBurstMax <"unlimited" or for SBC 5400/SWe/CNF: 1-900; SBC 7000: 1-2700> callRateMax <"unlimited" or for SBC 5400/SWe/CNF: 1-450; SBC 7000: 1-1350> otherReqBurstMax <"unlimited" or SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> otherReqRateMax <"unlimited" or SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> registerBurstMax <"unlimited" or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> registerRateMax <"unlimited or for SBC CNF: 1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> subscribeBurstMax <"unlimited" or SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000> subscribeRateMax <"unlimited" or SBC CNF:1-1000; SBC 5400/SWe: 1-1500; SBC 7000: 1-3000>

Configuration	Description
CLI	**SBX-131719 Configuration based retry after header support in 503 CAC rejection Response** In instances of a Call Admission Control (CAC) rejection due to a 503-error response code for any reason, a retry-after header is introduced for normal calls to make additional connection attempts. The SBC will account for the configured retry-after values on the Ingress Trunk Group (TG) app while populating the 503-error response retry-after value. The feature is configured through two parameters in the CLI: 'retryAfterMin' and 'retryAfterMax'. After a normal call is rejected, the Retry-After header will generate a random retry-value value between these two configured values. Configuring either of the Retry-After values as zero disables the feature. This feature only applies to normal calls; using INVITE, REGISTER and non-INVITE messages is not supported. **Command Syntax** `% set addressContext <ac_name> zone <zone_name> sipTrunkGroup <tg_name> cac` `retryAfterMin <0-120s>` `retryAfterMax <0-120s>` You can configure both `retryAfterMin` and `retryAfterMax` to '0'; however, if you assign a value to one parameter, the other must also be assigned a value. If either of these parameters are configured with the value '0' , the SBC will not add a Retry-After header to 503 responses. **Configuration Example** `set addressContext <ac_name> zone <zone_name> sipTrunkGroup <tg_name> cac retryAfterMin 10 retryAfterMax 40`

Configuration	Description
CLI	**SBX-134147 RCB selection based on PPI, PAI or From header** This feature allows users to choose the header order in which the SBC fetches the Registration Control Block (RCB) using the Address of Record (AOR). **Command Syntax** `% set addressContext <addressContext_name> zone <zone_name> rcbAorMatchBasedOnHdrs <from-header | pai-header | ppi-header>` **Command Parameters** • `rbcAorMatchBasedOnHdrs` – For calls from sources behind privacy services, configure to accept INVITE messages according to one, two, or three of the header flags. The system will detect these header flags in the order you add them. ◦ `from-header` – Use the FROM tag in the INVITE message's header ◦ `pai-header` – Use the P-Asserted Identity tag in the INVITE message's header ◦ ppi-header – Use the P-Preferred Identity tag in the INVITE message's header **Configuration Example** All of the following examples are valid, but will prioritize different header matches `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ pai-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ ppi-header ]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ from-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ pai-header, ppi-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ pai-header, from-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ ppi-header, from-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ pai-header, ppi-header, from-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ pai-header, from-header, ppi-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ ppi-header, pai-header, from-header]` `% set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [ ppi-header, from-header, pai-header]`

Configuration	Description
	`` % set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [from-header, pai-header, ppi-header] % set addressContext default zone ZONE_NAME rcbAorMatchBasedOnHdrs [from-header, ppi-header, pai-header] ```
Alarms	**SBX-127402 License Expiry Generates Alarm** The SBC will raise the existing alarm sonusCpLicenseBundleExpiredNotification once a day to alert the operator that the Domain Locked License has expired. This alarm continues until a valid license bundle is installed for the expired Domain Locked License feature. For more information, refer to: • sonusCpLicenseBundleExpiredNotification - CRITICAL