Juniper Apstra Version 4.2.1, 4.2.1.1 Release Notes

Known Critical Apstra Issues

Junos Device Deployment Failures After Upgrade to Apstra 4.2.1 Due to Missing mgmt_junos VRF (AOS-44834)

In Apstra 4.2.1, Junos device gRPC telemetry requires the configuration of the device mgmt_junos VRF with system management-instance. If the user is upgrading from an earlier version of Apstra and does not have the device configured for mgmt_junos VRF with system management-instance there will be deployment errors when the incremental configuration is deployed to the device when activating the new Apstra 4.2.1 controller.

Workaround

Before upgrading to Apstra 4.2.1, the user must add the device mgmt_junos VRF with system management instance to the device and the Apstra pristine configuration. Refer to https://kb.juniper.net/KB77094 for more information. Contact Juniper Apstra Support for assistance.

New Features

Support for Dell E3248PXE-ON switch (RFE-2939)

Feature Category: Device Profiles

Support for Dell E3248PXE-ON has been added in Apstra 4.2.1

Block upgrades with Juniper EX4300s in Blueprints (RFE-3017)

Feature Category: Device Profiles

Apstra 4.2.0 deprecated EX4300s and upgrades to Apstra 4.2.1 will be blocked if EX4300s are present in active Blueprints.

Add Device Profile for Dell Z9664F-ON (RFE-2625)

Feature Category: Device Profiles

Apstra now has a Device Profile for Dell Z9664F-ON

Add Device Profile for Dell S5448F-ON (RFE-2624)

Feature Category: Device Profiles

Apstra now has a Device Profile for Dell S5448F-ON

Supported device operating systems for Apstra 4.2.1 (RFE-2913)

Feature Category: Device Operating Systems

The following updates have been made for network operating systems qualified for the Apstra 4.2.1 release.

Juniper Networks:
Junos (All roles including Access Only)
21.2R3-S6, 21.4R3-S5, 22.2R3, 22.4R3.

Junos Evolved for the IP-Forwarder role (Spines in EVPN or any role in an IP-Fabric):
21.2R3-S6-EVO, 21.4R3-S5-EVO, 22.2R3-EVO, 22.4R3-EVO.

Junos Evolved for EVPN leaf roles:
22.2R3-EVO, 22.4R3-EVO

Interconnect Gateway Leaf
22.4R3, 22.4R3-EVO

Cisco Systems:
NXOS 10.2(5), 9.3(11)

Arista Networks:
EOS 4.27.6M, 4.25.3.1M, 4.24.5M

Dell EMC & Edgecore:
Enterprise SONiC 4.1.2, 4.0.5, Edge Standard SONiC 4.1.2

Apstra CLI command to change device root passwords. (RFE-2731)

Feature Category: Device Operating Systems

A new Apstra CLI command has been added to change device root passwords for Juniper, Arista, and SONiC devices. The new command is "scenario change-root-password --system --old-password --new-password " or for all devices "scenario change-root-password --all --old-password --new-password "

Add support for the Dell SONiC Edge Standard image (RFE-3003)

Feature Category: Device Operating Systems

SONiC Edge Standard version 4.1.2 is now supported.

Switch Port Group Validation (JUNOS EVO) (RFE-3086)

Feature Category: Design, Build, Operate

Apstra introduces an advanced capability to validate port assignments, taking into account the specific hardware limitations of your switch. This enhancement allows Apstra to proactively alert you to potential port issues arising from hardware constraints before any configuration is pushed. Please note that this feature is exclusively applicable to JUNOS EVO platforms.

Support for Cisco to Arista interop between two Blueprints when configured with Over-The-Top DCI (RFE-2849)

Feature Category: Design, Build, Operate

You can now support Over-The-Top DCI between a Cisco Blueprint and an Arista Blueprint.

Expose the routing policy in the Routing Zone list view (RFE-2791)

Feature Category: Design, Build, Operate

You can now see the routing policy used by each Routing Zone under the Routing Zone list view.

Expose the rack type description field in the rack type list view (RFE-2159)

Feature Category: Design, Build, Operate

Once you have created a new rack type and added a description, the description field will now be exposed in the rack type list view and help you find your racks!

Enhanced Visibility of Sub-Interface IP Addresses (RFE-2058)

Feature Category: Design, Build, Operate

You can now access sub-interface IP address details directly from the 'Staged > Physical > Interfaces' section. This feature allows you to view both IPv4 and IPv6 addresses assigned to the sub-interface, with a convenient link provided to the routing zone where you can easily edit IP addresses.

Blueprint Dashboard Tooltips (RFE-2822)

Feature Category: Design, Build, Operate

Your blueprint dashboard has 18 distinct anomaly categories which enable you to quickly identify issues within your fabric. We have integrated informative tooltips for each anomaly, providing additional context to enhance your understanding of the displayed information.

Allow to update dual-rack uplink speed one link at a time (RFE-2806)

Feature Category: Design, Build, Operate

Having a mix of link speed between a rack and its spines should never be considered a good permanent design. However, it is sometimes a necessary step to minimize traffic impact when you need to upgrade the overall fabric link speed. Therefore, it is now possible to update the uplink speed of a leaf-pair, one link at a time. A build warning will be raised to alert users until all the uplinks are configured at the same speed again for each leaf-pair.

Added Integrated Data Center Interconnect (DCI) support for Juniper Junos. This is also referred to a VXLAN Stitching. (RFE-2535)

Feature Category: Design, Build, Operate

Apstra 4.2.1 enables support of Integrated Data Center Interconnect (DCI), sometimes referred to as VXLAN Stitching, support for Juniper Junos. Integrated DCI offers improved scalability, resiliency, and flexibility over the Over-the-Top DCI model. You can selectively import and export Layer-2 and/or Layer-3 services between data centers. You select capable designated border leaf devices at each data center that advertise EVPN Route Type 2 and Route Type 5s.

Add/Remove Connectivity Templates from the network topology view (RFE-2396)

Feature Category: Design, Build, Operate

You can directly add/remove connectivity templates when selecting a leaf or access node in the topology view. The new action is called "manage connectivity templates".

Add configurable timeout for external TACACs+ Provider (RFE-2831)

Feature Category: Design, Build, Operate

You can now change the default 30s timeout for external TACACs+ connection under the advanced settings when creating a new external Provider, up to 120s (although longer than 60s should be done in coordination with Apstra support). This allows longer timeouts when a customer is using MFA.

Ability to change warning/error level for specific blueprint validations (RFE-2995)

Feature Category: Design, Build, Operate

Apstra has a lot of built-in network design validations that help you avoid making mistakes like assigning the same IP address or ASN twice. Some validations are blocking, raised as "errors" and preventing you from committing a change. Others are raised as "warnings" to alert you something seems off but is not preventing you from committing a change. You can now decide to change the warning/error level for some built-in validation so that it either becomes blocking or non-blocking based on your preferences.

New Apstra Flow collector and visualizer (RFE-2649)

Feature Category: Telemetry and Analytics

Apstra now provides a comprehensive flow data collector for sFlow, NetFlow, IPFIX, and IFA plus multiple dashboards to visualize and analyze network traffic.

IBA probe to detect devices requiring a switch reboot due to Junos Shared Tunnels configuration (RFE-3072)

Feature Category: Telemetry and Analytics

When you upgrade from 4.1.X to 4.2.1, you have the possibility to opt-in for a Reference-Design enhancement which transitions all Junos VTEP-enabled devices to use VLAN-Aware MAC-VRF instead of the traditional Default Switch instance.
When enabling this configuration mode, the QFX5K and EX4400 VTEP enabled devices will get an incremental configuration to enable VxLAN shared tunnels. This configuration requires a switch reboot to take effect, forwarding issues may be observed if the device is not rebooted.
You now have an IBA probe which is automatically triggered to alert you of any devices requiring this reboot so you can plan for it.

Various improvements on Apstra Server Event/Audit Log system (RFE-2706)

Feature Category: Platform

Your Apstra Server Audit logs are now available and kept for a year (time-based), instead of being limited to a number of events. Sorting and querying were added in the web interface to help you find specific logs (based on timestamp, username, user's IP address, type of changes, and much more!). You can also use the new API to export audit logs more easily to 3rd party systems.

Supported Upgrade Paths to Apstra 4.2.1.1 (RFE-2915)

Feature Category: Platform

This release supports upgrade paths from previous Apstra 4.1.X, 4.2.0, and 4.2.1 releases.

Users must use VM-VM for upgrades from Apstra 4.1.X and 4.2.0. From Apstra 4.2.1, users must use an in-place upgrade. See the user guide for the documented list of supported upgrade paths and upgrade methods.

Support of Junos Evolved on-box agents (RFE-3037)

Feature Category: Platform

You now have the ability to leverage on-box agents with devices running the Junos Evolved on-box agents.

Show Apstra version in menu bar (RFE-2824)

Feature Category: Platform

The Apstra version is now displayed in the top left of the menu bar for easy access to see what version of Apstra is deployed.

FIPS 140-2 support for Apstra VM and cluster (RFE-2401)

Feature Category: Platform

Apstra 4.2.1 is the first release that offers FIPS 140-2 capability for those who require FIPS compliance. The US National Institute of Standards and Technology (NIST) develops the FIPS standards for US government agencies and contractors with specific security requirements for cryptographic modules. For more information about FIPS, go to the NIST FIPS FAQ page. The base Operating System is Ubuntu 22.04 LTS, and OpenSSL 3.0.10 for the cryptographic modules.

The FIPS capability is disabled by default in 4.2.1. A new host CLI command `aos-fips` which needs to be run as sudo is used to enable, disable, and view the status of the FIPS.

There are three main commands available via aos_fips on Apstra VM:
enable: Enables the FIPS mode on the Apstra VM;
disable: Disables the FIPS mode on the Apstra VM;
status: Reports of the FIPS mode on the Apstra VM (Apstra (AOS) config, SSH configuration, NGINX config, Docker containers, acid test for the host, host OpenSSL configuration)

You must enable FIPS mode on all Apstra VMs in the cluster (the order should not matter). Restarting the VM is required FIPS after changing modes.

Apstra Guest VM Support on Windows Server 2019 (RFE-2882)

Feature Category: Platform

Ability to install Apstra as a Guest VM on Windows Server 2019

Apstra-CLI Command for enabling/disabling LEDs on Juniper switches (RFE-2956)

Feature Category: Apstra CLI

New Apstra-CLI commands 'system turn-beacon-on' and 'system turn-beacon-off' to respectively turn on/off LEDs on a managed switch. Valid for Juniper devices on both EVO or non EVO. On Modular devices you can select the fps number.

Changed Features

The Generic Systems nodes are no longer highlighted in yellow when the system IDs are not assigned (RFE-2839)

Feature Category: Design, Build, Operate

In previous versions, if a Generic System is not assigned a System ID they show yellow in the topology view. However, most Apstra customers do not assign System IDs to Generic Systems. In 4.2.1, only fabric devices without assigned System IDs show yellow; Generic Systems are always shown in gray.

Static VXLAN Renaming (RFE-3083)

Feature Category: Design, Build, Operate

In an effort to provide users with clearer deployment options, the template formerly known as "Static VXLAN" has been renamed to "Pure IP Fabric." This change aims to enhance user understanding and streamline the process for those seeking to deploy a fabric without a network virtualization overlay.

Reorganized and clarified blueprint fabric settings (RFE-2919)

Feature Category: Design, Build, Operate

The Blueprint Settings tab has been reorganized to enhance clarity and provide a more intuitive workflow. The fabric settings have been grouped into categories and settings renamed to more precisely and clearly reflect their use.

Re-design ZTP configurator UI to handle large datasets (RFE-2997)

Feature Category: Design, Build, Operate

The Apstra ZTP configurator has been redesigned from an accordion-style UI to a tree-style UI to provide better visualizations of large datasets.

Guided workflow for creating internal versus external Generic System (RFE-2859)

Feature Category: Design, Build, Operate

We have consolidated the two actions "Add Generic System" and â€œAdd External Generic Systemâ€ into one action called "Add internal/external generic system" and added guidance about when to use which type of Generic System. This action is available at the leaf and access nodes level. At the Spine or Super-spine. level, only external generic systems can be added.

"Endpoints" and "Routing Zone Groups" sub-menus moved from "Virtual" to "Policies" tab (RFE-2861)

Feature Category: Design, Build, Operate

To make changes to your blueprint "Network Endpoints" and "Routing Zone Groups", you now have to navigate to the Blueprint>Staged>"Policies" tab, instead of the "Virutal" tab. You can create/edit your "Routing Zone Groups" under the "Policies">"Routing Zone Constraints" sub-tab. This change better organizes policy workflows.

Support float numbers as input to analytics processors using Dynamic Stages (RFE-1165)

Feature Category: Telemetry and Analytics

You now can support float type input to the following processors, we configured in dynamic stages: Min, Max, Sum, Standard-Deviation, Average, Range Check and Periodic Average.

Move 'Enable Root Cause Analytics' from Active tab to Analytics tab (RFE-1433)

Feature Category: Telemetry and Analytics

The 'Enable Root Cause Analytics' action has been moved from the Active tab to the Analytics tab to make it easier to find and align with the product design of not enabling production changes in the Active tab.

Add support for CLI commands absent from the schema when defining a custom collector. (RFE-3066)

Feature Category: Telemetry and Analytics

You now can define a custom collector for a CLI command even if not present in the loaded schemas. As long as the CLI commands is executable on the target devices, it will be usable in the collector's definition. Removing this limitation allow you to expand the scope of the possible use-cases.

Option to disable original Apstra server after VM-to-VM upgrade (RFE-2854)

Feature Category: Platform

A new option will be presented to users during Apstra VM-to-VM upgrades to ask if the user wants to disable the original server to prevent issues with multiple active Apstra instances after upgrading.

Option to allow users to override worker node credentials on upgrade. (RFE-3002)

Feature Category: Platform

The Apstra upgrade aos_import_state script is extended to support an additional argument --override-cluster-node-credentials. When specified this will initiate an interactive menu where users can provide just the password for the specific cluster IP or an option to provide a password for all worker nodes.

Improve Technical Support page layout (RFE-3076)

Feature Category: Platform

Improve the Technical Support page layout to be a table that provides improved page layout, search, sort, and batch operations.

Removed Features

Remove 3D Topology View (RFE-2976)

Feature Category: Design, Build, Operate

The blueprint 3D topology view has been removed. The default view is now the 2D view.

Tech Preview Features

Tech Previews give you the ability to test functionality and provide feedback during the development process of innovations that are not final production features. The goal of a Tech Preview is for the feature to gain wider exposure and potential full support in a future release. Customers are encouraged to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported.

Tech Previews may not be functionally complete, may have functional alterations in future releases, or may get dropped under changing markets or unexpected conditions, at Juniper'□s sole discretion. Juniper recommends that you use Tech Preview features in non-production environments only.

Juniper considers feedback to add and improve future iterations of the general availability of the innovations. Your feedback does not assert any intellectual property claim, and Juniper may implement your feedback without violating your or any other party's rights.

These features are "as is" and voluntary use. Support Services will attempt to resolve any issues that customers experience when using these features and create bug reports on behalf of support cases. However, Juniper may not provide comprehensive support services to Tech Preview features. Certain features may have reduced or modified security, accessibility, availability, and reliability standards relative to General Availability software. Tech Preview is not supported under existing service agreements, SLAs, or support service.

For additional details, please contact Juniper Support or your local account team.

ZTP support for Juniper Junos OS Evolved 23.X (RFE-3026)

Feature Category: Device Profiles

Tech Preview support in Apstra ZTP for Juniper Junos OS Evolved 23.X versions which no longer support Python 2.

Add Device Profile for Juniper QFX5240-64QD (RFE-3007)

Feature Category: Device Profiles

Apstra now has a Device Profile for Juniper QFX5240-64QD in Tech Preview

---

Add Device Profile for Juniper QFX5240-64OD. This DP is currently Tech Preview (RFE-3048)

Feature Category: Device Profiles

Apstra now has a Device Profile for Juniper QFX5240-64OD

Add Device Profile for Juniper QFX5230-64CD (RFE-2656)

Feature Category: Device Profiles

Apstra now has a Device Profile for QFX5230-64CD

Add Device Profile for Juniper QFX5130-48C/CM (RFE-2884)

Feature Category: Device Profiles

Apstra now has a Device Profile for Juniper QFX5130-48C/CM in Tech Preview

---

Tech Preview support of Juniper QFX5120 for Integrated DCI (VXLAN Stitching) (RFE-2971)

Feature Category: Device Operating Systems

EVPN VXLAN Stitching support for QFX5120 release has support in the apstra reference design & back-end, but is pending general-availability release of Junos release 23.2+ or higher.

Fixed Apstra General Issues

A blueprint commit can produce a functionally empty configuration push against a SONiC device (AOS-43298)

In some cases, the controller may push an unnecessary functionally empty configuration against a SONiC device.

Normally, configuration is pushed only to devices that do really need a configuration change. If a configuration change is not needed during a blueprint commit, the controller is able to determine that very fact and skip pushing configuration to that device. For example, a new virtual network creation is not expected to cause any change to the spines of a network.

For a SONiC device whose previous operation was a full config apply operation, the next blueprint commit may cause a functionally empty config push that is not strictly needed. Also, a full config apply and a subsequent controller restart may cause a spontaneous functionally empty config push against a SONiC device.

Please note that the functionally empty configuration push does not have any adverse effect on the SONiC device, changes nothing and causes no traffic disruption.

Resolution

This defect is present only in Apstra 4.2.0 and is fixed in Apstra 4.2.1.

AOS Upgrade to 4.2.1 Will Fail if MLAG Peer Links Option Is Selected in the Interface Configlet (AOS-43093)

AOS upgrade will fail if, before the upgrade, MLAG peer links were chosen as a role in the interface configlet. Before 4.2.0 release, MLAG peer links in the interface configlet was disregarded for rendering configuration, even when selected. Before upgrading, we advise turning off the MLAG peer links in the interface config of the blueprint because functionality changed. After an upgrade, there won't be any configuration changes in the device where interface configlet is applied.

Application Endpoints "Bulk unassign templates" Button Unassigns All Connectivty Templates (AOS-42540)

In the Application Endpoints table view, if the user uses the "Bulk unassign templates" button to unassign one connectivity template from several application endpoints, all connectivity templates will be unassigned.

Apstra 4.2.1 upgrade while running aos_import_state may never complete with large scale Connectivity Templates (AOS-44627)

During the Apstra upgrade to 4.2.1 while running aos_import_state the upgrade may continue to run for a long time and never complete. This is caused by a bug when querying the blueprint topology for Connectivity Templates which never completes when lots of Connectivity templates have assignments on a blueprint.

Resolution

In Apstra 4.2.1.1, the blueprint query used during the Apstra upgrade has been improved to eliminate the potential timeout.

Apstra Authentication Agent Crashes When More Than One LDAP Servers Timeout (AOS-42566)

If the user adds more than one LDAP server and the server does not respond, Apstra will timeout and crash the Apstra authentication agent (Authagent), causing all new login attempts to fail until the agent recovers.

Apstra Upgrade With Freeform Blueprints Deployment Status Failed (AOS-43809)

If a user is doing an Upgrade to Apstra 4.2.1 with Freeform Blueprints, the `-ignore-config-validation-results aos_import_state` deployment state post upgrade is shown as failed. But this is only cosmetic, no config has been pushed to the device.

Apstra ZTP Faliure During Junos Upgrade with Console Special Characters (AOS-43732)

Apstra ZTP may fail due to device console issues messages (e.g. "Scheduler Oinker") with special characters during a Junos upgrade.

Apstra ZTP UI ztp.json Configurator Invalid System Agent Parameters (AOS-42550)

If the user uses the Apstra ZTP UI ztp.json configurator to assign the system-agent-params in the ztp.json file, empty variables like "id", "platform", or "operation_mode" will be stored with empty strings ("") in ztp.json.

```
"system-agent-params": {
    "id": "",
    "agent_type": "onbox",
    "platform": "",
    "job_on_create": "install",
    "operation_mode": "",
    "profile": "",
    "packages": [],
    "force_package_install": false,
    "install_requirements": false,
    "enable_monitor": false
}
```

This will likely cause the Apstra system agent creation API call from ZTP to fail.

Apstra ZTP UI ztp.json Configurator Invalid System Agent Parameters (AOS-43402)

If the user uses the Apstra ZTP UI ztp.json configurator to assign the system-agent-params in the ztp.json file, empty variables like "id", "platform", or "operation_mode" will be stored with empty strings ("") in ztp.json.

```
"system-agent-params": {
    "id": "",
    "agent_type": "onbox",
    "platform": "",
    "job_on_create": "install",
    "operation_mode": "",
    "profile": "",
    "packages": [],
    "force_package_install": false,
    "install_requirements": false,
    "enable_monitor": false
}
```

This will likely cause the Apstra system agent creation API call from ZTP to fail.

Apstra ZTP UI ztp.json Configurator Invalid System Agent Parameters (AOS-42311)

If the user uses the Apstra ZTP UI ztp.json configurator to assign the system-agent-params in the ztp.json file, empty variables like "id", "platform", or "operation_mode" will be stored with empty strings ("") in ztp.json.

```
"system-agent-params": {
    "id": "",
    "agent_type": "onbox",
    "platform": "",
    "job_on_create": "install",
    "operation_mode": "",
    "profile": "",
    "packages": [],
    "force_package_install": false,
    "install_requirements": false,
    "enable_monitor": false
}
```

This will likely cause the Apstra system agent creation API call from ZTP to fail.

Apstra ZTP UI ztp.json Configurator Invalid System Agent Parameters (AOS-43403)

If the user uses the Apstra ZTP UI ztp.json configurator to assign the system-agent-params in the ztp.json file, empty variables like "id", "platform", or "operation_mode" will be stored with empty strings ("") in ztp.json.

```
"system-agent-params": {
    "id": "",
    "agent_type": "onbox",
    "platform": "",
    "job_on_create": "install",
    "operation_mode": "",
    "profile": "",
    "packages": [],
    "force_package_install": false,
    "install_requirements": false,
    "enable_monitor": false
}
```

This will likely cause the Apstra system agent creation API call from ZTP to fail.

Apstra-CLI "system-agents update" Command Resets System Agent Credentials (AOS-42921)

The Apstra-CLI (a.k.a. AOS-CLI) "system-agents update" command is used to update an existing Apstra system agent. However, if the "username" and "password" options aren't used, any existing system agent credentials will be removed.

Arsita EOS VXlan Floodlist Anomalies When Flood Map for Vteps Programmed Correctly (AOS-43128)

Occasional race conditions may exist for the VXlan collector when cached VNI entries from the device, which will cause false positive IBA VXlan Floodlist probe anomalies even though the VXlan floodmap is programmed correctly in the devices.

Blueprint Commit Task failed with an internal error (AOS-44029)

The Blueprint Commit Task failed with an internal error. Navigate Blueprints-> Blueprint Name -> Staged -> Tasks -> Detailed Status to find the below response

```
"deploy_config_version": 1216,
 "api_response": "",
 "deploy_errors": "Internal error"
```

Check the Platform -> Event Log for the error details:

```
Fail: [Errno 2] No such file or directory:
'/var/lib/aos/db/blueprint_backups/64401e76-2bfa-4378-8f96-
7c05ac969915/1216/graph.json.zip'
```

Root Cause: When user commits the blueprint, Apstra attempts to create a backup of the current state. If it fails, logs the error, sets the status to failure, and aborts the transaction. During a blueprint commit, BuilderAgent was backing up the graph when ScotchAgent's RevisionManager, which was cleaning up stray backups, accidentally deleted the file BuilderAgent was using. This resulted in a FileNotFoundError when BuilderAgent tried to access the file, causing the commit task to fail.

Resolution

Issue fixed in 4.2.1 ensuring stale files are cleaned up reliably.

BuilderAgent Crash by changing label of global anycast vtep interface node via REST API (AOS-40762)

BuilderAgent uses only one automatically generated label for global anycast vtep interface node per blueprint. If the label is changed or modified to different value by API call, it can make more than one entries exist and then cause BuilderAgent to crash from violation of one unique entry.

---

cabling-map Patch API with if_name as empty string causes "Staging is not synced with config" when adding generic systems to leaf switches (AOS-43429)

cabling-map Patch API call with if_name as empty string is accepted and makes if_name value not synced in the graph DB without triggering validation error. The condition in the graph DB makes adding generic systems into the leaf node, which has if_name as empty string, fail with not synced error message.

Cannot Apply a Junos Interface Configlet Under Under Unit 0 Using an L3 Sub-interface (AOS-40825)

Junos interface configlet is not rendered under unit 0 for interfaces.

Cannot Delete or Edit MLAG or ESI Leaf Labels in Rack Designer (AOS-39063)

When using the new graphical rack designer with MLAG or ESI leaf pairs, the user cannot manually delete or edit the leaf label.

Custom telemetry collectors may in some cases erroneously produce multiple entries in query result for the same outer xml tag (AOS-42947)

In some cases where XML structure contains nested tags that are repeating inside the context of the outer tag, like for example in the 'show interfaces queue' output, the generated query result might contain erroneously repeating entries in the context of the outer tag.

Resolution

The issue was fixed in Apstra release 4.2.1

Device Configuration on the Access-Access ae Interfaces Will Be Deleted During the Apstra 4.2 Upgrade When Interface Configlet Is Applied to the Layer-3 Generics Role on Access Switches (AOS-42898)

Before the release of Apstra 4.2, if an interface configlet was applied to layer-3 generics on the access switches, it was also applied to the access_access ae interface. The Apstra 4.2 release fixed this incorrect behavior. A Device configuration diff will be seen after upgrading from an earlier release to an Apstra 4.2 release since the fix no longer renders configuration on the access_access ae interface.

Duplicate BGP Neighbor IP Addresses in CT/Remote GW Not Validated (AOS-36684)

Apsta will not validate BGP neighbors with duplicate remote gateways IP address configured in Connectivity Templates.

Enabling "Max Routes" in a Arista EOS Fabric Settings May Cause False EVPN VXLAN Type-5 Route Validation Anomalies (AOS-40992)

In Apstra, if the user enables "max routes" fabric settings such as max_fabric_routes, max_evpn_routes, and max_mlag_routes, Arista EOS devices will report local routes with valid next-hops. This will cause the Apstra IBA EVPN VXLAN Type-5 Route Validation probe to report false anomalies.

Due to behavior specific to Arista EOS, changing fabric BGP settings on EOS will temporarily advertise local routes with the next-hop. As a result, the IBA probe will see two updates, one with and one without the next hop. This causes the Apstra IBA probe to mark the route as permanently missing.

Error Not Indicated in the ztp.json Configuration in the UI Editor (AOS-44598)

When the ztp.json configuration with an error is saved, a red dot appears for a second next to the error configuration, then suddenly disappears. The red dot eventually returns.

EVPN Interconnect page raises error for import/export route targets "Value is required" (AOS-39565)

If there are any configured virtual networks that have one of Import or Export route-targets defined, but not both, users visiting the EVPN interconnect tab will see an error in the UI.

EVPN-DCI -- IGW Border leaf advertises locally-attached /32 and /128 regardless of Type5 host routing policy (AOS-42544)

When EVPN-DCI Interconnect is configured, the local gateway will advertise connected server /128 and /32 hosts, without consideration of the Apstra "Type5 host policy" in fabric addressing policy. This is a limitation of the Juniper routing policy framework, where a DCI->DC ADV route cannot be uniquely identified and compared to a direct route advertisement from those connected arp/ND learned hosts. This only applies to the local border gateways that have VNs attached to them.

EX4400 models in Apstra-unsupported VCP mode have different interface naming for PIC 1 (AOS-43264)

It is noted that if an EX4400 device is set to VCP mode, the interface numbering of PIC 1 will be different from what a any existing builtin Apstra Device Profile for an EX4400 device has. Specifically, et-0/1/1 does not exist in VCP mode, but instead becomes et-0/1/2.

Please note that Apstra version 4.2.1 does not support any Juniper EX4400 model in VCP mode.

Incorrect Inteface Naming for Juniper EX4400-24MP EX4400-48MP Device Profiles (AOS-41912)

Apstra device profiles for Juniper EX4400-24MP EX4400-48MP device will incorrectly name device "mge" interfaces (e.g. mge-0/0/0) as "ge" interfaces (e.g. ge-0/0/0).

Inter-VRF Routing With Single Spine Path Requires Manual BGP Reset After Upgrade (AOS-41295)

The Apstra reference design configures "allowas-in 1" spines to optimize routing redundancy with inter-VRF routing with a single spine path. If the EVPN sessions are already up before an upgrade, the change doesnâ€™t take effect until BGP sessions are manually cleared.

Junos Device Deployment Failures After Upgrade to Apstra 4.2.1 Due to Missing mgmt_junos VRF (AOS-44834)

In Apstra 4.2.1, Junos device gRPC telemetry requires the configuration of the device mgmt_junos VRF with system management-instance. If the user is upgrading from an earlier

version of Apstra and does not have the device configured for mgmt_junos VRF with system management-instance there will be deployment errors when the incremental configuration is deployed to the device when activating the new Apstra 4.2.1 controller.

Resolution

In Apstra 4.2.1.1, the Apstra upgrade script will verify all Junos devices have been configured with mgmt_junos VRF with system management-instance and will fail the upgrade otherwise. Please refer to https://kb.juniper.net/KB7709 for the process of updating the Junos devices in Apstra 4.1 before the upgrade to Apstra 4.2.1.1.

Link Tags Not Properly Associated With ESI/MLAG Interfaces (AOS-42414)

Link tags applied to physical interface members are not associated with ESI/MLAG interfaces, but they are associated with non-ESI/MLAG LAG interfaces.

Missing Upgrade Plugin for node_to_node_if_counter Processor (AOS-40850)

If the user has an Apstra blueprint created before Apstra 3.3.0 configured with the Headroom probe, upgrades to Apstra 4.1.1 and later may fail with error `AttributeError: 'NoneType' object has no attribute 'validate_config'` because the `node_to_node_if_counter` processor has been removed.

No Validation Error While Creating Virtual Infra Manager (AOS-35959)

When the user creates a Virtual Infra manager by either providing an incorrect IP address or an incorrect username/password for vCenter or NSX-T, Apstra will not raise any validation error. Just the state shows disconnected.

Node ID for Virtual Infra Manager Device Is Empty in Liveness Anomalies (AOS-36792)

Node ID for virtual infra manager device is empty in liveness anomalies. The system ID and IP or hostname will be listed in the virtual infra section.

Overlapping VNI Values Causing Error Messages to Not Show (AOS-42824)

After a VNI is manually assigned to security zone, if the VNI value belongs to the dynamic VNI

pool for Virtual network, Virtual network may be assigned with the same VNI value. When this duplicate VNI error condition occurs, UI doesn't show error messages correctly.

Overlay Sessions. Not Rendered in a Junos Blueprint With v6-Only Underlay (AOS-41551)

When the user has a blueprint consisting of Junos devices with a v6-only underlay, Apstra will render groups lsclos-l-evpn or lsclos-s-evpn for the overlay sessions.

Possible Memory Leak in BuilderAgent When Creating/Destroying Multiple Blueprints (AOS-39290)

If the user repeatedly creates and deletes Apstra blueprints, a small incremental memory leak in the Apstra BuilderAgent may result in memory exhaustion on the Apstra VM.

Resolution

This memory leak issue with the Apstra BuilderAgent process has been resolved in Apstra 4.2.1.

Route-targets with leading zeroes cause upgrade failures to Apstra 4.2.1.x due to schema validation changes (AOS-42738)

Leading zeroes in route-targets, such as 0555:0555, were accepted in device configurations. However, the route-maps rendered from these configurations failed to react to the generated routes because the leading zeroes were stripped during route generation (e.g., 0555:0555 became 555:555). This mismatch caused the rendered route-maps to be misaligned with the generated routes, resulting in forwarding failures, telemetry collection errors, route installation issues, and routing policy mismatches.

To address this inconsistency, Apstra 4.2.1 introduces stricter schema validation that disallows EVPN RD type:value fields containing leading zeroes. While this change ensures consistent route handling, it may cause upgrade failures if existing configurations include route-targets with leading zeroes.

Resolution

The root cause of the issue is the mismatch between rendered route-maps (containing leading zeroes) and generated routes (stripping leading zeroes). Apstra 4.2 resolves this by disallowing EVPN RD type:value fields with leading zeroes through stricter schema validation. This change ensures consistent behavior and prevents routing policy mismatches, but it requires pre-upgrade configuration changes to avoid upgrade failures.

SONIC Device ARP and Neighbor Suppression Enabled for L2 only VxLAN (AOS-42546)

For SONIC devices, even if layer2-only VxLAN is configured, ARP and neighbor suppression functions will be enabled, making ARP packets sent to the CPU, potentially causing traffic to be dropped.

SONiC SSH_SERVER_VRF Section Not Applied in Service Configuration (AOS-42779)

Even if the Pristine Configuration of a SONiC device includes an `SSH_SERVER_VRF` section, the necessary configuration to allow ssh access only to connections coming from the `mgmt` VRF is not applied to Apstra service configurations. So SSH connections are accepted from all VRFs.

When connectivity template with custom routing policy is applied with BGP session, rendered config may create BGP session with VRF's routing policy instead of custom routing policy (AOS-43501)

When connectivity template with custom routing policy with BGP session is unassigned, Apstra doesn't clean up old BGP protocol endpoint information correctly, used to determine the effective routing policy for each BGP session. These stalled information makes the following assigning CT operation to use VRF's policy instead of custom routing policy.

When Moving a Device to a New Blueprint, It Is Not Available for Commit-check (AOS-42052)

When moving a device to a new Apstra blueprint (and no blueprint commit has been done yet in the new blueprint), it is not available for commit-check even though the system ID is assigned and deploy mode is set to deploy.

Worker node encounters continuous NodeFileMonitorAgent crash (AOS-46491)

The NodeFileMonitorAgent of the worker node encounters a SIGTERM signal, leading to continuous restarts approximately every 1-2 minutes. NodeFileMonitorAgent on startup scans /var/lib/aos/metricdb directory to create a file registry in SysDB. In Apstra 4.1.2, the implementation uses Python to scan the file system and instantiate file registry entities. It takes too long to process a large number of files, resulting in missing Keepalive heartbeat messages.

Resolution

In Apstra 4.2.1, the enhancement was incorporated. Therefore, it is recommended to upgrade to version 4.2.1.1.

ZTP UI Should Not Send Non Configured Params in API Payload (AOS-44596)

The UI should not configure the keys in the ztp.json configuration for system-agent-params if the user has not configured the values. The ZTP UI reports the payload with empty strings, which trips the schema validation. For the attached screenshot, I added Junos as the platform in the GUI for the configurator, and the UI generated a payload with the platform, agent_type, job_on_create, and profile. This is unexpected.

Fixed Apstra Security Issues

Apstra VM SSHd Terrapin Vulnerability (AOS-44494)

Default sshd ciphers and mac exchanges included as part of Apstra base OS are vulnerable to terrapin attack for chacha20-poly1305@openssh.com and etm mac exchange hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com

Resolution

Apstra 4.2.1.1 includes both client and server side fixes.

SSH Terrapin Vulnerability Workaround Using SSH aes128-gcm or aes256-gcm Ciphers Is Not Supported by Apstra Paramiko SSH Client (AOS-44336)

Apstra uses the Paramiko SSH client library to access Junos devices. The Apstra version of Paramiko does not yet support the SSH ciphers aes128-gcm@openssh.com and aes256-gcm@openssh.com. Access from Apstra to the Junos device will not function properly if it is set up to use just these SSH ciphers.

Resolution

Apstra 4.2.1.1 includes an upgraded Paramiko SSH client library, which supports strict key exchange to mitigate the SSH Terrapin Vulnerability (CVE-2023-48795). The Apstra Paramiko SSH client library still does not support SSH GCM ciphers, and users are recommended to use the SSH CTR cipher and HMAC-SHA2 MAC exchange.

Fixed Third-Party Issues

DHCP Relay Is Not Supported for Juniper ACX Platforms (AOS-41771)

Due to an outstanding bug in all available versions of Junos EVO, DHCP relay is not supported by Apstra for Juniper ACX platforms.

DHCPv4 Offer Dropped Client Between Junos and Junos-EVO (AOS-33701)

Due to an existing issue in Junos 22.2R2-EVO, DHCPv4 offer packets are dropped when a virtual network is extended by Junos and Junos-EVO rack devices.

Juniper ACX7100 Kernel Crashes in a Scaled Environment (AOS-41219)

Due to an unresolved bug with Junos 22.4R2-EVO on the ACX7100 hardware platform, the Junos-EVO kernel may crash in a scaled environment.

Junos EVO Commit Check Failure May Cause Apstra Device Management Failure (AOS-41206)

Due to an outstanding bug in all available versions of Junos EVO, various Apstra device management functions may fail due to intermittent, unexpected device configuration commit check failures. This may cause failures with Apstra device system agent uninstallation, OS upgrades, and device configuration deployments after an Apstra blueprint commit.

Junos EVO Devices May Encounter 'Config unlock failed' Deployment Failure (AOS-40787)

Due to an unresolved bug on Junos EVO, deployment may fail with the following error `Config unlock failed: UnlockError(severity: error, bad_element: None, message: Configuration is allowed only from the Routing Engine with GlobalIPOwner attribute assigned')`.

Old Layer-2 State on Juniper ACX7100 Removed From Blueprint (AOS-41230)

Due to an unresolved Junos EVO issue, if the user removes a Juniper ACX7100 from an Apstra blueprint, the device may retain portions of the previous layer-2 state, preventing it from being deployed in a new blueprint.

QFX10002-60C Breakout Intefaces May Not Come Up (AOS-40237)

Due to a Junos 21.2R3-S4 issue on the QFX10002-60C platform, 10G breakout interfaces may not come up.

---

vEX Device Junos mclag-cfgchkd Crash (AOS-41794)

If the uses includes the Junos "multi-chassis mc-lag consistency-check" configuration on Juniper vEX devices running Junos 22.2R3.15, the mclag-cfgchkd process may crash.

Apstra Config Rendering Changes

NXOS, EOS, SONiC EVPN Route-Target and Route-Distinguisher Config Change on Apstra Upgrade (AOS-42144)

In certain circumstances, EVPN Routing Zones can be assigned to a system without VXLAN-enabled virtual networks, static routes, subinterfaces, or BGP connectivity points associated with them.
For those "unused" routing zones a configuration upgrade will ensure the EVPN Route-target and EVPN route-distinguisher are added to the BGP configuration. This only applies to blueprints that have routing zone optimization disabled, have EVPN Routing zones without any VTEPs on them, and were built before Apstra 4.2.0. This upgrade plugin is only applicable to NXOS, EOS, and SONiC.

Known Apstra General Issues

"On Device Configlet Preview" Might Emit Error if the Device Is Unassigned (AOS-43233)

Attempting to pull the configlet preview for specific blueprint device ("On Device Configlet Preview"), by clicking on the device label under the general configlet preview page might fail with a slightly misleading error, if the device is unassigned. Certainly trying to get a preview for a

device which is not assigned is bound to cause an error, as a real preview for a device that doesn't exist isn't possible. However, the error emitted is slightly confusing.

[SONiC] Golden Config Validation Error When Modifying FRR Log Level from "Informational" to "Notifications" (AOS-49660)

Apstra sets the FRR log level to "log syslog informational" by default in the SONiC device. When a customer attempts to change the log level to "log syslog notifications" using a configlet, the golden configuration validation fails due to a mismatch between the expected and running configurations. Apstra has made "log syslog informational" a prerequisite for golden config validation, using it as a verification key.

Workaround

It is recommended that users avoid changing "log syslog informational" to "log syslog notifications"

Alternate name of interface has the same name as the real interface name (AOS-46121)

In Apstra-configured SONiC devices, the Alternate Name of an interface is always the same as the real interface name (native mode) used in the SONiC OS's Linux kernel. Some customers prefer the standard interface name as an Alternate Name over the native interface name. Since version 5.0.0, AOS does not explicitly define the Alternate Name as the native interface name, so it is automatically filled in by SONiC, which follows the standard interface name for Alternate Name.

```
Example) Alternate Name as native interface name for "show interface status"
command in the sonic-cli

sonic# show interface status
------------------------------------------------------------------------------
------------------------------------------------------
Name                Description                   Oper           Reason
AutoNeg   Speed          MTU            Alternate Name
------------------------------------------------------------------------------
------------------------------------------------------
Ethernet0           -                             down           admin-down
off       25000          9100           Ethernet0

Example) Alternate Name as standard interface name for "show interface status"
command in the sonic-cli

sonic# show interface status
------------------------------------------------------------------------------
------------------------------------------------------
```

```
Name                Description                    Oper           Reason
AutoNeg   Speed          MTU            Alternate Name
-------------------------------------------------------------------------------
-------------------------------------------------
Ethernet0           -                              down           admin-down
off       25000          9100           Eth1/1
```

Apply Config failed when 1G interface in the Juniper EX4400-24MP-EM is configured (AOS-45648)

When 1G interface is configured in the Juniper EX4400-24MP-EM, applying configuration fails because device profile for EX4400-24MP-EM has invalid setting for speed.

Workaround

Please clone device profile for EX4400-24MP-EM and then replace configuration of transformation for 1G over 0-23 ports

```
from
{"global": {"breakout": false, "fpc": 0, "pic": 0, "port": 0, "speed": "1G"},
"interface": {"speed": ""}}
to
{"global": {"breakout": false, "fpc": 0, "pic": 0, "port": 0, "speed": ""},
"interface": {"speed": "1G"}}
```

Please contact Apstra Support Team for more information

Apstra 4.1.1 upgrade to 4.2.1.1 or 4.2.2 disables Generate EVPN host route from ARP/IPv6 ND ARP feature in the fabric policy (AOS-53556)

When using `Generate EVPN host route from ARP/IPv6 ND ARP` feature in the virtual network policy, caution should be used when upgrading from Apstra 4.1.1 or 4.1.0 to Apstra 4.2.1.1 or 4.2.2.

Configuration for this feature is lost during upgrade.
4.1.1 -> 4.1.2 : OK (no issue observed)
4.1.1 -> 4.2.1.1 or 4.2.2 : Reset to default value as disable (losing configuration)

Workaround

Upgrade to Apstra 4.1.2 at first before moving to Apstra 4.2.1.1 or 4.2.2 for non-service impact. The other option with brief service impact is to enable this feature again in the fabric policy before

making the operational mode in the upgraded Apstra controller go from maintenance mode to ready mode, commit the new change, and then change the operational mode to ready status, which will push two commits, one from upgraded changes and the other from enabling the feature for generating EVPN hosts. For further assistance, please contact the Juniper Apstra Support Team.

Apstra 4.2 Post Upgrade May Not Show Interface Generic Checkbox Selections (AOS-42481)

After upgrading to Apstra 4.2, with configlets for layer-2 and layer-3 generic interfaces selected before the upgrade, the section_condition query string does not reflect all the selected checkboxes. Still, the query is equivalent to selecting all the checkboxes. The Apstra UI may incorrectly display that configlets aren't applied to layer-2 generic interfaces.

Apstra 4.2.1 upgrade while running aos_import_state may never complete with large scale Connectivity Templates (AOS-44627)

During the Apstra upgrade to 4.2.1 while running aos_import_state the upgrade may continue to run for a long time and never complete. This is caused by a bug when querying the blueprint topology for Connectivity Templates which never completes when lots of Connectivity templates have assignments on a blueprint.

Apstra may incorrectly render Juniper ACX7100-32C Channelized Port Config (AOS-44243)

When configuring 10G/25G channelized port transformations on Juniper ACX7100-32C, Apstra may incorrectly omit the "unused" configuration parameter on the odd interfaces within the port group if no generic systems are connected to channelized ports on the even interface.

Workaround

The user can add an external generic system to the other even port in the port group for the ACX7100-32C so Apstra will correctly add the "unused" configuration parameter on the odd interface. Please refer to https://apps.juniper.net/port-checker/acx7100-32c/ for more information.

Apstra SysDB crash when Virtual Infra Manager is removed and then added (AOS-45546)

When using AOS <= 4.2.1.x and removing & adding a Virtual Infra Manager (vcenter / nsxt), the Apstra backend database SysDB will have an agentId mismatch within entities related to Virtual Infra (Vcenter/ nsxt). When these entities are present in the Sysdb database, Apstra SysDB will

crash repeatedly, rendering the Apstra GUI inaccessible.

Workaround

Please contact JTAC for support to clean sysdb with provided patch esc_339_generic_all_versions.run

---

Apstra UI prevents setting "IP Links to Generic Systems MTU" to 9216 under fabric settings (AOS-53627)

Apstra customers 4.2.x and greater may encounter an issue where the MTU value for IP Links to Generic Systems cannot be set to 9216 via the UI. Although the UI states that only even values in the range 1280-9216 are accepted, the input of 9216 is incorrectly rejected, while 9214 is accepted.

```
Important Note:
1. This issue is applicable only to customers upgrading from Apstra 4.1.x to
4.2.x or later, where Fabric MTU remains disabled post-upgrade and customers
who wish to continue without enabling the Granular MTU feature.
2. This issue is not applicable to customers with fresh 4.2.x deployments,
where Fabric MTU is enabled by default, activating the Granular MTU feature.
```

Workaround

Although the UI blocks 9216, the backend API does accept this value. As a workaround, users can update the MTU value via the REST API:

```
1. Navigate to Platform â†’ Developers â†’ REST API Explorer.
2. Use the PATCH /api/blueprints/{blueprint_id}/fabric-settings endpoint with
the following payload:
    {
         "external_router_mtu": 9216
    }
3. Verify the update by performing a GET on the same endpoint: GET
/api/blueprints/{blueprint_id}/fabric-settings
4. Navigate to Blueprints â†’ Blueprint Name â†’ Uncommited and check the diff
5. Commit the Blueprint
```

If further assistance is needed, please contact Apstra Support.

Apstra Upgrade Connectivity Validation Uses SSH to Check Connectivity to vCenter (AOS-

44413)

Normally, Apstra uses the VMware vCenter API for communication. If the user configures any vCenter servers in Apstra, the `aos_import_state` upgrade will check connectivity to vCenter using SSH, not API. If the SSH is blocked or the SSH credentials are different than the API credentials, this pre-upgrade check may fail, causing the upgrade process to fail.

Workaround

Before upgrading, please check if SSH from the controller to vCenter can be successfully established using vCenter credentials entered in Apstra. If necessary, the user can skip Apstra upgrade connectivity validation with the `--skip-connectivity-validation` option when running `aos_import_state`.

Apstra-CLI system turn-beacon-on Command with Juniper EX4400 (AOS-43034)

The Juniper EX4400 platform does not have a dedicated Locator/ID LED. The Junos `"show chassis beacon"` command will always return ON. All ports or connected ports will be lit in `"GREEN"` depending on the explicit beacon command. Also, it uses a 5-minute default timer, and CLI supports between 1 and 120 minutes. After a predefined time, the beacon status changes back to the default state in CLI. The switch port status is not changing based on Junos `"request chassis beacon"` command.

Banner not updated by ZTP's custom config in the SONiC device (AOS-45991)

After the SONiC device's banner is updated by a script file configured in the ZTP's custom config, the final stage of ZTP processing replaces the customized banner with another piece of information based on the success or failure of ZTP processing. As a result, unlike in the custom config of ZTP , the banner may not be updated properly.

Workaround

After ZTP processing, manually update banner in the device like the following example or contact Juniper Apstra Support team for further assistance.

```
sed -i s/"#*Banner.\*$"/"Banner \/etc\/ssh\/my_banner"/ /etc/ssh/sshd_config
cat >& /etc/ssh/my_banner << EOF
###########################################################################
#########################
# This device is for the exclusive use of XXXXX.
# All unauthorized access or configuration changes to this device are subject
to prosecution.
```

```
##########################################################################
##########################
EOF

service ssh restart
```

BGP maximum-paths configuration not rendered in the user-defined VRF's BGP configuration for Cisco NXOS device (AOS-46667)

For Cisco NXOS devices, the BGP maximum-paths configuration is currently rendered in only default VRF's BGP configuration; the user-defined VRF's BGP configuration lacks this configuration.

Workaround

Use configlet to explicitly to add maximum-paths into user-defined VRF's BGP configuration

```
Example Configlet:
router bgp {{ bgpService.asn }}
  {% for vrf in security_zones | list | reject('in', ['default']) %}
   vrf {{ vrf }}
   address-family ipv4 unicast
   maximum-paths 64
  {% endfor %}
```

Configlet may not be applied in the SONiC device during the commit when system time moves back (AOS-46890)

When the SONiC device time is set back using the NTP configuration from configlet during the commit process, the device agent may reboot. When the agent reconnects, the device agent tries to reapply configuration changes that were interrupted by the previous commit. However, because the shell script file from configlet exists and matches the controller's information, it may be skipped rather than applied.

Workaround

Apply full push configuration into the SONiC device

Dashboard shows 'Pending' Service Config for All Devices During Commits on Specific

Device, with Delays in Larger Blueprints (AOS-51083)

Users experience confusion when committing changes for specific devices because the Dashboard shows 'Pending Service Config' for all devices, which can mislead them into thinking other devices are being updated as well. This is a known behavior in Apstra's current design. When a commit is made, all devices temporarily enter a 'Pending' state while the system determines which devices require changes. Even devices that don't need updates briefly show as pending, which can create the false impression that changes are being made. Additionally, as the number of devices in a blueprint increases, the delay becomes more noticeable because Apstra processes each device sequentially. This raises concerns about performance and efficiency when managing larger blueprints.

Workaround

There is no immediate workaround. The behavior is aligned with the current system design.

Deleting Link returns error with '<' not supported between instane of 'str' and 'NoneType' (AOS-47479)

When Deleting Link is executed by UI or by delete-switch-system-links API call for the port channel port, the backend recalculates port channel pool to reuse the port channel IDs. The recalculation uses sorting key comprising of generic system's hostname for comparison. If the hostname is null, comparison can fail with the exception because of incompatible type comparison.

Workaround

Please assign the proper hostname into the generic system, connected to leaf node via port channel port.

Deleting Routing zone fails with "Protocol endpoint for protocol session is orphaned" error message (AOS-43808)

After a CT (connectivity template) with dynamic BGP peering and BGP Prefix Dynamic Neighbor information is assigned to the SVI interface for a system, if the system is removed from the virtual network later, the CT becomes unassigned status, which allows the user to delete the CT. After the CT is removed later, protocol_session becomes orphaned from the associated CT. it can lead to failure in deleting the routing zone.

Workaround

Deleting protocol_session via Blueprint Node Delete API or before modifying the virtual network for pruning system, update CT's assignment at first.

Deleting Virtual Networks in CTs with Multiple VLANs - All Active Endpoints Unassigned (AOS-44623)

In version 4.2.0, Apstra introduces the capability for users to forcibly delete a Virtual Network, even if it has active endpoints. Apstra will initially display the interfaces to which the Virtual Network (VN) is currently allocated and prompt the user to confirm the deletion. It's important to note a limitation in the current design: if a user deletes a VN assigned in a CT where Multiple VLANs are present, all active endpoints will be unassigned.

Workaround

User should manually remove the specific VLAN from the CT before proceeding to delete it from the Staged > Virtual Networks section.

Dell SONiC devices after Apstra ZTP loses mgmt IPs if the ZTP server is not available (AOS-44712)

For Dell SONiC devices after Aptra ZTP, they would lose mgmt IPs if the ZTP server is not available because Apstra ZTP processing doesn't configure static IP address to mgmt interface.

Workaround

After Apstra Device Agent is created via ZTP process, update the pristine configuration with the changes, which assign the mgmt interface with static IP address and default GW address or use custom script file that assigns static IP address and default GW address during ZTP process in case SONiC 4.1.2 and Apstra 4.2.1 or 4.2.2 is used. Please contact Juniper Apstra Support for more details.

Device Profile is not assigned when Cisco 93108TC-FX3P device is onboarded (AOS-45123)

When Cisco 93108TC-FX3P device is onboarded, it reports the hardware model differently depending on the version. The current built-in Device Profile for Cisco 93108TC-FX3P has the selector's model as 93108TC-FX3P. If the device reports the hardware model as C93108TC-FX3P (with prefix C), it can't be matched on the built-in device profile. Therefore, the device profile can't be associated with the onboarding device.

Workaround

Clone builtin Cisco 93108TC-FX3P device profile, modify model field value of Selector from 93108TC-FX3P to C?93108TC-FX3P, and the assign the new device profile into the device.

For the further support, please contact Apstra Support Team.

DeviceTelemeryAgent crash in the MAC Telemetry service for the JUNOS/EVO device (AOS-50058)

The JUNOS/EVO device uses GRPC for the MAC Telemetry service. During the GRPC processing, Apstra Controller uses device's credential information (username and password) to populate GRPC meta data. If the password includes non-printable ASCII characters, a validation error for invalid characters can lead DeviceTelemetryAgent to fail with a crash.

Workaround

Please use only printable ASCII characters for device's password to avoid validation error or use polling mechanism by disabling GRPC in the telemetry service

To disable GRPC service in the telemetry service, change grpc_enabled = 0 in the /etc/aos/aos.conf file and then restart AOS service in the Apstra Controller.

[telemetry_global_config]

Python multithreading enable/disable knob for telemetry collection

multithreading_config = 1

Execution timeout for extensible telemetry collectors

command_timeout = 120

Knob to enable/disable gRPC based service collectors

grpc_enabled = 0

Space separate list of device models where gRPC based service collectors are

disabled. The configuration is case insensitive. The device model can be

retrieved from Managed Devices page. Multiple models can be specified as:

ModelA ModelB ModelC

grpc_disabled_models = QFX5100-48T-6Q QFX5100-24Q-2P QFX5100-48S-6Q

DeviceTelemetryAgent.{pid}.log by gRPC trace logs filling up disk (AOS-51846)

DeviceTelemetryAgent.{pid}.log files in /var/log/aos/ in the offbox agents become large and can fill up the disk

Workaround

The following Python script can be added to run via crontab on an hourly basis, which will clean up older log files. This workaround needs to be applied to controller VM and worker VMs where offbox agents are running (nodes with offbox tags in the Platform/Apstra Cluster/Nodes).

```
# Copyright 2024-present, Apstra, Inc. All rights reserved.
#
# This source code is licensed under End User License Agreement found in the
# LICENSE file at http://apstra.com/eula

import configparser
import json
import os
import re
import shutil
import subprocess
import traceback


SystemIdPattern = re.compile(r'AOS_SYSTEM_ID=offbox,(.+),(.+)')


def update_aos_conf(task_id):
    aos_config = os.path.join(
        '/var/lib/aos/conf.d/task/offbox/',
        task_id,
        'aos.conf',
    )

    parser = configparser.ConfigParser()
    if os.path.isfile(aos_config):
        parser.read(aos_config)

    if not parser.has_section('logrotate'):
        parser.add_section('logrotate')

    if 'max_kept_backups' not in parser.options('logrotate'):
        parser.set('logrotate', 'max_kept_backups', '1')

        staging_file = aos_config + '.staging'
        with open(staging_file, 'w') as f:
            parser.write(f)
```

```
            shutil.move(staging_file, aos_config)
            return True

    return False


def refresh_logging_infra(container_id):
    subprocess.check_output([
        'docker', 'exec', container_id, 'pkill', '-HUP', 'DeviceKeeperAge'
    ])


def get_offbox_containers():
    containers = subprocess.check_output([
        'docker', 'ps', '-q', '--filter',
'label=AOS_CLUSTER_APPLICATION=offbox',
    ]).decode()
    return containers.splitlines()


def get_task_ids():
    def extract_info(container_env):
        try:
            envs = json.loads(container_env)
        except ValueError:
            return None, None

        for env in envs:
            matched = SystemIdPattern.match(env)
            if matched:
                return matched.group(1), matched.group(2)

        return None, None


    containers = get_offbox_containers()
    if not containers:
        return

    containers_env = subprocess.check_output([
        'docker', 'inspect', '--format', '{{json .Config.Env}}', *containers,
    ]).decode()
    for line in containers_env.splitlines():
        task_id, container_id = extract_info(line)
        if not task_id:
            print('Failed to extract task id from container env:
{}'.format(line))
            continue

        yield task_id, container_id


def main():
    for task_id, container_id in get_task_ids():
        try:
            if update_aos_conf(task_id):
```

```
                refresh_logging_infra(container_id)
        except:
            print('Failed to update aos.conf for container:
{}'.format(container_id))
            traceback.print_exc()


main()
```

Even if the above workaround is applied, there is a chance of filling up partition. The below command can be executd with root permission to clean up logs quickly in the controller VM and worker VMs.

```
find /var/log/aos/task -name "*.log" -size +10M -print | grep
"DeviceTelemetry" | xargs -I {} sudo cp /dev/null {}
```

Disallow hyphens (-) in key and value names for telemetry service registry entries (AOS-50120)

Apstra introduced custom telemetry services in the 4.2.0 release. Users define a service schema to structure and store data, based on key and value from the CLI output. The UI doesn't allow hyphens in telemetry key and value names. However, the API allows them. If a telemetry service registry entry with a hyphen is created via the API, the upgrade to Apstra 5.x may fail with validation error.

```
File "/usr/local/lib/python3.10/dist-packages/lollipop/errors.py", line 182,
in raise_errors
  raise ValidationError(self.errors)
lollipop.errors.ValidationError: Invalid data: {'key': 'Unable to identify
"key" from schema'}
```

In Apstra 5.1.0, telemetry key/value names with hyphens are now disallowed.

Workaround

To resolve the issue, follow below steps:

```
1. Navigate to Analytics > Service Registry
```

```
2. Identify the service name that contains hyphens (-) in telemetry keys and
telemetry values within the application_schema payload.
3. Edit the service entry:
   - Click the Edit action for the affected service
   - Replace all hyphens (-) with underscores (_)
   - Click the Update button to save changes
4. Retry the Apstra upgrade process by running aos_import_state again
```

Please contact Apstra Support for further assistance.

Disk Space Exhaustion Due to Unrotated Logs in Apstra ZTP VM Containers (AOS-44969)

Users may encounter disk space exhaustion in the ZTP VM because log rotation is not enabled for the '/var/log/messages' and 'syslog' files in the dhcpd, tftp, and status containers, as well as for the '/logs/rsyslog.log' file in the status container. Although the logrotate utility and a crontab file are available, log rotation is not activated by default. As a result, these logs can accumulate, quickly consuming disk space and potentially causing degraded system performance or service interruptions.

Workaround

To enable log rotation, follow these steps:

```
1. Create logrotate configuration file for each container (dhcpd, tftp,
status) in the /containers_data/logrotate/<container_name> directory.
2. Create logrotate configuration file for rsyslog.log for status container in
the ZTP VM (/containers_data/logrotate/status directory).
3. Add a script to the ZTP VM's cron.hourly directory that executes the
logrotate command inside each container via docker exec, ensuring the logs are
rotated according to the specified configuration.
4. Modify Docker Compose file (/etc/apstra_ztp/docker-compose.yml) to map
logrotate configuration file in the ZTP VM into file inside container.
5. Restart the containers to apply the changes
```

Please contact Juniper Apstra Support team for the further support.

Duplicate Entries shown in the virtual infra inventory (AOS-47478)

The transport VLAN node would remain uncleared in the Graph Database while the Virtual Infra Manager for NSX-T manager with unreachable vCenter or without vCenter is created and added to the blueprint, and then removed from the blueprint and deleted. The same transport VLAN node would be re-created, and duplicate entries would exist if the identical virtual Infra manager for NSX-T was created and added back to Blueprint again.

Workaround

restart AOS service via `sudo service aos restart` and then stalled duplicate entries will be automatically cleared

---

Error Not Indicated in the ztp.json Configuration in the UI Editor (AOS-44598)

When the ztp.json configuration with an error is saved, a red dot appears for a second next to the error configuration, then suddenly disappears. The red dot eventually returns.

Errors With IBA Custom Collectors After Upgrade (AOS-42876)

If the user uses IBA custom collector packages and is upgrading to Apstra 4.2.1, due to migration to Python 3, earlier Python 2 based custom collector packages will not work in Apstra 4.2.1.

Workaround

The user must contact Juniper JTAC Support to request updated Apstra custom collector packages. The user must completely remove existing custom collector packages from system agents and install the new Apstra 4.2.1 custom collector packages.

EVPN IBA Telemetry probe is deprecated and incompatible with the latest NOS versions (AOS-52013)

The EVPN IBA Telemetry probe was originally implemented in older Apstra versions (3.x) but has been deprecated in later versions due to advancements in telemetry collection frameworks. Customers upgrading from older versions (3.x) to Apstra 4.x and then to later might encounter issues with the EVPN IBA Telemetry probe as it may no longer function as expected.

The primary reasons for this are:

```
1. Deprecation of Older Collectors: The EVPN IBA Telemetry probe and
associated collectors were designed for earlier NOS versions. These collectors
relied on commands and logic that are no longer supported by certain vendors
(e.g., with EOS 4.25.3.1M, evpn_type3 collector failed to gather data due to a
plugin error triggered by an unsupported command).
2. Python Dependency Transition: Apstra versions prior to 4.2.x were based on
Python2, whereas 4.2.x and later versions have transitioned to Python3. This
shift in underlying architecture breaks backward compatibility for older
telemetry packages.
```

```
3. Multiple Breakpoints in Compatibility: Over several releases, the
extensible telemetry framework has undergone significant updates, requiring
users to update their custom packages to align with newer standards and
dependencies.
```

Since the EVPN IBA Telemetry probe is deprecated, customers experiencing issues with it are recommended to consider using standard predefined probes, such as EVPN Type-3/Type-5 Route Validation, while being mindful of their limitations.

Limitation: For the predefined Type-3 and Type-5 probes to work, all leaf nodes in the topology must be of the same platform. Mixed-vendor environments are not supported by these probes.

Workaround

If the topology consists of all leaf nodes in the blueprint, users can perform the following actions to mitigate issues with the deprecated EVPN IBA Telemetry probe:

```
1. Perform Apstra upgrade, post upgrade the system enters maintenance mode
2. Delete EVPN IBA Telemetry Probe from all blueprints
3. Remove any related custom telemetry packages added to the agent profile
4. Change Maintenance mode to Normal to resume regular operation
5. If onbox, initiate onbox install for all agents
6. Post upgrade, start  using standard predefined probes such as EVPN Type-
3/Type-5 Route Validation.
```

The EVPN IBA Telemetry Probe has been deprecated. Customers experiencing issues with this probe are recommended to replace it with the standard predefined probes, such as the EVPN Type-3/Type-5 Route Validation probes. For these probes to work properly, all leaf nodes in the topology must be from the same platform, as mixed-vendor environments are not supported. To address the challenges of migrating from the EVPN IBA Telemetry probe to the Type-3/Type-5 probes in mixed-vendor leaf node environments, an enhancement request (: [IBA][Probe] Expand EVPN probes to support mixed-vendor leaf nodes) has been submitted as a long-term solution. To prioritise , please contact sales/PLM.

Export/Import Route Targets Under Routing Zone Introduce Additional Character in Config (AOS-44770)

Junos device config deployment fails for Junos BGP community configurations when the user defines import/export route targets for a routing zone where the second number is greater than 65535 (e.g. 64512:4200000000), as the Apstra rendered config appends an "L" string at the end of the assigned number.

Workaround

The user must use a route target where the second number is less than 65536 (e.g. 64512:65535).

Exporting and importing cabling map triggers validation errors for port-channel interfaces (AOS-45683)

When a cabling map is exported and then imported, UI generates validation errors for port-channel interfaces. The import process doesn't expect port-channel interfaces from the input data. However, the exporting process includes not only individual interfaces but also port-channel interfaces together as output data. Therefore, importing with input data, which has port-channel interfaces, triggers the validation error during the import process.

Workaround

Please use /api/blueprints/{blueprint_id}/experience/web/cabling-map in the REST API explorer for exporting cabling map instead of UI export action.

High interface hold timer value rendered in the Collapsed fabric reference design may affect PXEboot (AOS-42437)

Customers may observe servers on a collapsed fabric failing to PXEboot where interface is rendered with a large hold time for up event as part of the collapsed fabric reference design

Workaround

Use a configlet to reduce the interface hold-timer.

Importing CSV file for virtual network fails with error "Invalid CSV header order" (AOS-47014)

Importing virtual networks from a CSV file fails if the bound_system_ column header, where a virtual network is bound, contains parenthesis or bracket characters. These characters may originate from the system label and are not permitted by CSV header validation.

Workaround

Please remove parenthesis or bracket characters from system's label

---

Inclusion of DNS_SERVER in SONiC configuration, if present in the Pristine Config of a device (AOS-42825)

Starting with Apstra 4.2.1, if the Pristine Configuration of a SONiC device includes the

DNS_SERVER section, the Apstra Device Agent will copy it verbatim into the configuration rendered during any Full Config Apply operation. A Full Config Apply happens when a Device enters the Two-Stage L3 Clos reference design for the first time, when the user explicitly triggers a Full Config Apply and when a Discovery-1 Configuration is pushed to the device.

This Release Note is added to notify customers of a possible appearance of the DNS_SERVER section during or after an upgrade to Apstra 4.2.1. Versions of Apstra prior to 4.2.1 didn't use to copy the DNS_SERVER section from the Pristine to any rendered Configuration.

---

incorrect routing policy applied when assigning/unassigning endpoints in a CT with multiple BGP peerings and distinct routing policies (AOS-51549)

When a Connectivity Template (CT) includes a single Virtual Network (VN) primitive, multiple BGP peering primitives, and distinct routing policies, incremental configuration changes can occur during endpoint assignment and unassignment. These operations may unexpectedly swap or alter import/export routing policies, potentially disrupting routing configurations and causing traffic interruptions on commit.

In CTs with multiple BGP peering primitives, all BGP primitives are managed under a Batch policy. Apstra does not guarantee the execution order within a Batch Policy, especially during unassign and assign operations, where resources are allocated from a pool, and assignment order is unpredictable. This can lead to the unexpected swapping of routing policies.

It's important to note that this issue occurs only when the CT contains multiple BGP peering primitives with distinct routing policies. CTs with a single VN primitive and a single BGP peering primitive (and associated routing policies) do not experience this behavior.

Workaround

To mitigate this issue, the following workaround is recommended:

```
1. Delete the distinct routing policies from the Virtual Network primitive of
the affected Connectivity Template (CT).
2. Create separate Connectivity Templates (CTs) for each routing policy,
ensuring that each CT corresponds to one routing policy.
3. Assign each CT to the appropriate protocol endpoints.
```

This workaround will help avoid the unexpected swapping of routing policies during endpoint assignment and reassignment. Please contact Apstra Support Team for more information

---

Interface Based Configlet May Revert to Advanced Editor Mode (AOS-42549)

If the interface configlets were applied to layer-3 generic systems in the releases prior to Apstra 4.2, then post upgrade to 4.2, the configlet will revert to Advanced editor mode in UI.

Workaround

Customers can disable the advanced editor mode and select all the options under layer-3 edge except "standalone interface" and "member interface" to maintain backward compatibility with releases before Apstra 4.2 if that config was NOT applied to any non-subinterface interfaces. Suppose the configlet was applied to non-subinterfaces as well. In that case, we recommend creating two configlets, one for layer-3 edge subinterfaces and the other for layer-3 edge non-subinterfaces, and using interface predicate and/or interface tags to differentiate between the two configlets.

Interface descriptions are no longer allowed to contain the double quote character (AOS-45883)

Due to issues with configuration rendering across all supported platforms, the use of double quote characters in interface descriptions is no longer permitted on any managed device. In Apstra 5.0.0, user can edit interface descriptions through the UI, but earlier versions allowed editing raw graphs via the Apstra API. If a customer previously used a direct blueprint node API call to add an interface description with double quotes, these characters will be automatically converted to underscores during the 5.0.0 upgrade. Starting from Apstra 5.0.0, any attempt to include a double quote character in an interface description will be rejected by the Apstra API.

Jinja configlet using interface shows no actual changes in the UI even if diff exists (AOS-48906)

When importing a configlet, even if there are uncommitted changes from other Jinja-based configlets based on interface information, the logical diff output for the changes does not match the full node diff output. If the Jinja-based expression using interface uses an empty context, rendering will fail with empty information, resulting in an empty output with changes.

Workaround

For all Jinja-based configlets that use interfaces in the device context, wrap existing jinja statements with jinja if conditional statements to check interfaces are not empty for the configlet in the global catalog, and then remove/add the configlet to the blueprint to reflect the new changes.

```
==== original configlet using interface ====
```

```
{% for intf in interface.values()|selectattr('role', 'eq',
'l2edge')|rejectattr('part_of')|map(attribute='intfName')|list|sort %}
{% if loop.first %}
protocols {
     rstp {
{% endif %}
          replace: interface {{intf}};
{% if loop.last %}
      }
}
{% endif %}
{% endfor %}

==== corrected configlet using interface  ====
{% if interface != '' %}
{% for intf in interface.values()|selectattr('role', 'eq',
'l2edge')|rejectattr('part_of')|map(attribute='intfName')|list|sort %}
{% if loop.first %}
protocols {
     rstp {
{% endif %}
          replace: interface {{intf}};
{% if loop.last %}
      }
}
{% endif %}
{% endfor %}
{% endif %}
```

JUNOS device commit check feature using Apstra UI may incorrectly indicate an error when testing config (AOS-45715)

When using the commit check feature on the Uncommitted tab in Apstra UI, it may incorrectly indicate it experienced a red Error. RpcError(serverity: warning) when the JUNOS device issues a warning over the tested config while retrieving the config diff from the device.

Workaround

Verify that the warnings indicated under Error are benign and expected.

Junos EVPN Routing Instance Mode in the Fabric Policy Is Set to Default in the Upgraded Blueprint Even if Leafs Device Are Juniper EVO Device (AOS-43404)

VLAN-aware EVPN MAC-VRF configuration for the EVPN routing instance on an all-Juniper EVO platform in the fabric has already been generated by Apstra versions before 4.2.1. However, the upgraded blueprint, built earlier than the 4.2.0 version, always uses the default mode setting for the Junos EVPN routing instance mode in the fabric policy, even when every device in the leaf

is on the Juniper EVO platform. Customers cannot switch the routing zone's IRB mode from asymmetric to symmetric using the default mode setting in the Junos EVPN routing instance mode of fabric policy. Users can safely change the Junos EVPN routing instance mode from default to VLAN aware without disrupting service if every leaf device is a Juniper EVO device. On the other hand, the change for the Juniper non-EVO device can be disruptive.

KeyError: 'throughput_health' during Upgrade from 4.1.2 to 4.2.1 (AOS-45070)

In Apstra 4.1.2, the predefined 'throughput_health' dashboard in the two_stage_l3clos reference design was split into 'mlag_throughput_health' and 'esi_throughput_health'. An upgrade plugin to handle this situation was not provided, resulting in a VM to VM upgrade failure from 4.1.2 to 4.2.1. This error message was observed during the upgrade process:

```
File "/usr/lib/python3.10/dist-
packages/aos/upgrade/plugins/dashboard/deviated_predefined_dashboards.py",
line 916, in dashboard_deviates_412_definition
dashboard_matcher = datacenter_dashboards[dashboard_name]
KeyError: 'throughput_health'
```

Workaround

Workaround is to remove the 'throughput_health' dashboard before the upgrade, and then instantiate the 'mlag_throughput_health' and 'esi_throughput_health' dashboards after the upgrade.

LAG telemetry collection may fail in the SONiC device when using static LAG (AOS-46129)

When a device has only one static LAG connection enabled, LAG telemetry collection for a leaf may fail to work properly in the SONiC device. If other non-static LAG connections are configured on the same device, the problem will not occur.

Logical diff section continues to display link changes, even if configlet based on tag is removed (AOS-49983)

Despite the configlet being applied to some nodes based on tags, there were some link changes in the logical diff section. The logical diff tab continued to display the changes even after the configlet was reverted, and there was nothing to commit in the uncommitted tab section.

Workaround

The current diff plugin is not handling the system tag relationship , so it is not able to compute the difference. The workaround to restart the AOS services.

Multiline banner motd or exec is not supported in the Cisco NXOS Device (AOS-40278)

A banner configured in the Cisco NXOS device must be single line. Multiline banner (motd or exec) is not supported.

Workaround

Configure single line banner (motd or exec)

Not Able to See Apstra Flow Dashboards as Tenant Switched to Private (AOS-45813)

When logged into the Apstra Flow UI, occasionally, when the UI times out, the user is switched from the Global to Private tenant, rendering the dashboards inaccessible once they log in again.

Workaround

Manual workaround: Click the user icon at the top right and select Switch tenants to change back to the Global tenant.

Permanent workaround: modify `/etc/opensearch-dashboards/opensearch_dashboards.yml` file to change this:

```
opensearch_security.multitenancy.tenants.preferred: [Private, Global]
```

To this:

```
opensearch_security.multitenancy.tenants.preferred: [Global, Private]
```

Onbox Device Agent Not Supported in Dual Routing Engine Junos-Evolved Devices (AOS-43980)

It is not possible to install and use the Apstra onbox device system agent for Juniper dual routing engine devices running Junos-Evolved version 22.4R2.

Workaround

Please use the Apstra offbox device system agent.

Platform ACL Does Not Allow Loopback and Docker Networks (AOS-44009)

When the Platform ACL feature is enabled, and the default rule (0.0.0.0/0) is set to deny, the Apstra UI and system agents cannot make necessary REST API calls to the Apstra controller.

Workaround

The user must allow access from loopback (127.0.0.0/8) and docker (172.17.0.0/16) networks.

PortChannel description not rendered in the SONiC device (AOS-46316)

The interface description, including the port channel, can be updated via an API. However, Apstra does not render a description of the SONiC device's port channel interface. As a result, the SONiC device contains no description for the port channel interface.

Rack-based template is not shown in the selection during creating blueprint (AOS-47522)

When a rack-based template is created, two fields related to the 5-Staged Clos architecture are Links per Superspine Count and Link to Superspine Speed. The Link to Superspine Speed can be set to a non-null value even if Superspine Count is set to 0. The template is recognized as a component template to create a pod-based template rather than an independent rack-based template if Link to Superspine Speed is set to a non-null value. Therefore, it is not shown in the pop-down field for template as a selectable choice during blueprint creation.

Workaround

Edit the rack template and remove the Link to superspine speed value

---

Rendered Configuration for Interface MTU Value for Layer-2 Servers Is Changed From 9100 to 9216 in the JUNOS and EVO Device (AOS-43495)

Interface MTU values for L2 servers were rendered with a 9100 value in 4.1.2. With the addition of the MTU granularity functionality, it was modified in the Apstra 4.2.0 release to 9216. With these modifications, the leaf switches can receive and locally switch up to 9216-sized frames from L2 servers. However, traffic crossing the fabric may be discarded due to the maximum IP MTU value in the fabric interfaces. Users can set higher fabric MTU to allow intra-virtual traffic with larger MTU from servers. SVI MTU configuration for virtual networks can be tuned more granularly for the inter-virtual network traffic

---

Rotation of frr-reload.log inside the bgp container for SONiC Device (AOS-49921)

Every time a config apply happens in a SONiC device managed by Apstra, the FRR daemon configuration is gracefully reloaded by the frr-reload.py script inside the bgp container. The output of that script is directed to the file /var/log/frr/frr-reload.log inside the same container. The size of that log file is not expected to ever become a concern, unless a customer performs many thousands of config apply operations with a rather large FRR configuration.

Workaround

If the rotation of the /var/log/frr/frr-reload.log inside the bgp container is desirable, Apstra 5.1.0 includes a predefined configlet that can activate an appropriate logrotate cronjob inside the bgp container in regular intervals. The customer can use and/or modify the configlet and use it in their blueprint(s). Please contact Juniper Apstra support if more help is required.

For versions of Apstra earlier than 5.1.0, the same configlet can be manually created and used by the customer. Please contact customer support for further details.

Route anomalies caused by incorrect expected nexthops for leaf loopback address in the 5 Stage Clos topology (AOS-49802)

The expected routes for the loopback address of the leaf node in the spine node are calculated by using pod_label to determine whether the target leaf node and the current spine node are in the same pod. When the pod label is updated by UI, the ExpectationRenderer Agent may not update the new pod label information into all spine and leaf nodes, resulting in including the wrong nexthops into superspine nodes for leaf loopback address, even if the leaf node is directly connected from spine node.

Workaround

Please execute sudo service aos restart to restart ExpectationRenderer Agent

---

SONiC BGP route collector may fail because of stale VRF entries in the FRR routing daemon (AOS-49833)

In some cases where a VRF has been created, used, and then deleted, the FRR bgpd daemon may still indicate the existence of that VRF. Example, the Vrf-PURPLE in this vtysh output:

```
leaf2# show vrf
vrf Vrf-PURPLE inactive
vrf Vrf-blue id 120 table 1001 (configured)
vrf Vrf-red id 122 table 1002 (configured)
vrf mgmt id 47 table 5000
```

The existence of Vrf-PURPLE confuses the Apstra BGP route collector, causing it to crash. In such a case, the BGP route telemetry will stop working.

Workaround

`service bgp restart` in the affected device has been observed to remove the stale entries and thus restores the operation of the Apstra BGP route telemetry. Please do note that doing such a restart will flap all BGP peerings and can momentarily affect traffic.

SONiC device Show Tech collection is failing due to a remote SSH command error (AOS-47972)

SONiC customers may encounter issues generating Device Show Tech due to a remote SSH command failure. When attempting to collect the device show tech data from the Apstra UI, users might see the following error. The error logs indicate that the SSH command to generate the show tech data fails with a return code of 124, which typically indicates a timeout.

```
2024-09-03 11:13:37,467 INFO:TASK: Generate device show tech
2024-09-03 11:13:37,468 INFO:command (timeout-350): service aos show_tech --
output-prefix=/tmp/911b3e70-show-tech
2024-09-03 11:19:27,475 ERROR:Failure reason: , return-code: 124
2024-09-03 11:19:27,475 ERROR:FAILED
2024-09-03 11:19:27,477 ERROR:Failed command: sudo service aos show_tech --
output-prefix=/tmp/911b3e70-show-tech
2024-09-03 11:19:27,477 ERROR:Remote ssh command failed
```

Workaround

To generate the Device Show Tech data, use the following command directly on SONiC devices:

```
sudo python3 /usr/bin/aos_show_tech --platform sonic
```

SONiC device's error log for "Did not log record sleeping for 60s for vrf to be created" during ZTP processing (AOS-46485)

In the current ZTP implementation for SONiC devices, after the VRF is switched to management VRF during the ZTP process, the ZTP script running in the device sends status information to the ZTP server with a sleep time of 60 seconds. The change in VRF disconnects the device for a

certain period and prevents it from sending logs to the ZTP server until reachability is restored. The failures in the delivery of logs would be recorded and displayed on the device as error messages. The error messages don't mean that the ZTP process failed. It can be ignored safely.

SONiC DHCP Relay Towards Helper Goes Over the Default VRF (AOS-44242)

The Apstra reference design implementation for SONiC, communication of the DHCPv4 and DHCPv6 relay always uses the default VRF. This means that the DHCP server must always be reachable over the default VRF, regardless of the VRF to which the DHCP client belongs. The DHCP relay process will not operate correctly if the DHCP server is not reachable over the default VRF.

Workaround

The user must ensure the DHCP server addresses is always reachable over the default VRF.

Alternatively, a full config apply has been observed to put the DHCPv6 and DHCPv4 relay in the correct VRF as well. Do note however, that any subsequent incremental manipulation of the DHCP helper configuration will negate the correct VRF and reset it to default, necessitating another full config apply.

SONiC Displayed MTU for Member of PortChannel May Differ From Real Configured MTU (AOS-44229)

In Apstra 4.1.2, due to an error in the config_db.json rendering, a member Ethernet interface of a PortChannel that has MTU different than 9100 (the default MTU for SONiC interfaces) can display an MTU of 9100, instead of the inherited MTU from the parent PortChannel. The real MTU of the Ethernet member is same as the PortChannel's (as can seen via ifconfig), but displaying the MTU may show 9100 instead.

This bug can happen on an Apstra 4.1.2 controller and can also be carried over to an Apstra 4.2.1 or 4.2.2 controller via upgrade.

Workaround

If the customer wants to display the correct MTU, they can initiate a full config apply in the Apstra 4.2.1 or 4.2.2 controller. Apstra 4.2.1 or 4.2.2 will render the correct MTUs for both PortChannel and its members. To avoid a full config apply, please ask support for a fixer script that can restore the connect MTUs in the SONiC configuration database without doing any real change.

SONiC FRR restart or device reboot may cause configuration anomaly from rearrangement of FRR running configuration sections (AOS-49906)

Rebooting the device or restarting FRR in SONiC may cause the FRR running configuration sections (related with route-map) to be rearranged. The rearranging of sections will typically show a configuration deviation even if the running configuration is exactly the same as before.

Workaround

The anomaly can be eliminated by the user reviewing the deviation and accepting the changes. No further action is necessary.

Stalled poll timers caused by device reset can lead to the agent restart (AOS-49046)

This is a rare case in which a device reboots during a gRPC session, resulting in stale polling timers on the Apstra Agent side. When gRPC restarts, the stale timers are replaced by new timers, which trigger the handling timer for collection, resulting in an agent crash. After the agent restarts from the crash, the system functions normally without any further crashes.

Sustained High Disk Utilization Observed After SONiC NOS Upgrade (AOS-49288)

When upgrading to SONiC 4.1.2 via Apstra, users may notice sustained high disk utilization on their devices. The affected SONiC devices have significant space usage on the /host partition, ranging from 8 to 30 GB. This leaves little free space, potentially affecting system performance and stability. The problem has been identified as FRR logging into the BGP overlay2 storage rather than the correct location at /var/log/frr/frr.log. The disk does not fill up immediately following the NOS upgrade; it takes approximately 2.5 to 3 months for pre-production and 1.5 to 2 weeks for production. The rate of disk space consumption is proportional to the number of connected servers and the frequency of log-triggering events.

```
admin@sonic:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
:
/dev/sda3        32G   30G     0 100% /host  <<<<<<<<<<<<<<<<

root@sonic:~# du -sh /host/image-4.1.2-Enterprise_Standard/docker/*
:
28G  /host/image-4.1.2-Enterprise_Standard/docker/overlay2  <<<<<<<<<<<<<<<<
```

Workaround

As a workaround, the SONiC environment can use the configlet to execute log rotation for containers. The configlet example below utilizes a 10-minute cron job for SONiC devices that are at least 4.1.0. Kindly utilize the below configlet example to create a configlet that utilizes a cron job every 10 minutes, then import it into the blueprint for every SONiC device. Please get in touch with the Juniper Apstra Support team for additional assistance.

Configlet for SONiC Device

```
Section: FILE
Template Text:
  {% if function.min_os_version('4.1.0') %}
  # Rotate FRR logs inside bgp container per 10 minutes
  */10 * * * * root docker exec bgp logrotate --verbose /etc/logrotate.d/frr >
/tmp/bgp-docker-logrotate.log 2>&1
  # if less aggressive rotation, such as hour job, uncomment the below line
for an hourly job and comment the above line for a 10 minute job.
  # 0 * * * * root docker exec bgp logrotate --verbose /etc/logrotate.d/frr >
/tmp/bgp-docker-logrotate.log 2>&1
  {% endif %}
Filename: /etc/cron.d/bgp-docker-logrotate
```

System agent in the dual-re Junos EVO system may not work correctly when routing engine master switchover happens (AOS-43956)

if new system agent (onbox or offbox) for a Junos EVO system, which has dual routing engines, is not created with a master-only address, when routing engine master switchover occurs, the system agent and the device agent may not work correctly or introduce problems.

Example dual routing engine configuration:

```
re0:mgmt-0 {
  unit 0 {
    family inet {
      address 10.49.110.35/19;
      address 10.49.100.226/19 {
        master-only;
      }
    }
  }
}
re1:mgmt-0 {
  unit 0 {
    family inet {
      address 10.49.108.203/19;
```

```
      address 10.49.100.226/19 {
        master-only;
      }
    }
  }
}
```

In the above example, the common address for routing engines is 10.49.100.226. Installing against other management interface addresses will initially work, but will cause serious problems for the system agent if and when a routing engine master switch occurs.

Workaround

Please use the master-only address that is common in both routing engines' management interfaces when creating a system agent. For further support, please contact the Juniper Apstra Support Team.

The Range Check processor stage displays no data when the minimum anomalous value is set to 0.1 (AOS-49137)

Floating-point precision discrepancies can cause problems in the integration between IBA and metricdb when configuring IBA probes. To be more precise, the live data that was obtained from IBA is queried using metricdb using a trie-based matcher. However, minor variations in floating-point values (such as 0.1 being read as 0.10000000149) could cause metricdb to fail to match the desired keys. This can cause probes to miss crucial data when querying specific values.

Workaround

None

UI showed server error: null while displaying racks (AOS-48937)

When displaying racks, Apstra generates statistical information for the rack by sorting through each leaf's position data in ESI or MLAG cases. When a rack is updated by inserting a generic system into one of the leaf nodes that make up ESI/MLAG, Apstra uses sorting criteria based on the label from the leaf nodes. This inconsistent sorting criteria leads to calculation statistics referring to non-existent keys, resulting in errors. This issue only arises when a generic system is connected to one leaf node of an ESI/MLAG pair via a single attachment for a specific speed and the other leaf node lacks an interface for the same speed.

Workaround

To avoid missing key issues, add a generic system at the same speed to the other leaf node in the same ESI/MLAG pair.

Update Link Speed to 10M in the Juniper EX4400 device not allowed in the UI (AOS-50182)

When 10 Mbps speed is selected via Update Link Speed, the user interface (UI) disables the update button so that it cannot be applied, even though the interface supports 10 Mbps.

Upgrade from 4.1.2 to 4.2.1 Failing with TypeError: Type Node Not Found: Aos::Cachaca::CachacaConfig (AOS-45071)

The 'aos/v0/cachaca' directory in MainSysdb was deprecated in version 3.3.0. However, an upgrade plugin is missing for the upgrade path from 3.2.3 to 3.3.0, which would have removed this directory from MainSysdb. It was expected that by reaching version 4.0.1, this directory wouldn't be present in MainSysdb. However, the existence of the 'cachaca' directory is causing the VM to VM upgrade to fail from version 4.1.2 to 4.2.1 with the below traceback.

```
File "/usr/lib/python3/dist-packages/TacJson.py", line 72, in loads
    return e.ptr_.loadJson(jsonStr,flags.ptr_)
TypeError: type node not found: Aos::Cachaca::CachacaConfig (unknownType):
line 1 column 54020286 (char 54020285)
aca::CachacaConfig", "name": "930bd1a7-f2
```

Workaround

Remove 'aos/v0/cachaca' directory from MainSysdb via Acons

```
root@aos-server:/# Acons
:
 39            MainSysdb        tacsysdb                 43      0
:
Choose a connection (1-72) > 39
Selected agent MainSysdb, pid 43 on port 0, socket @001aa in subsystem
Connecting to local unix socket @001aa ...
Connected to process 43

$ cd aos
/aos is &lt;Entity /aos (non-const) of type Tac::DirImpl&gt;
default collection entityRef has:

$ cd v0
/aos/v0 is &lt;Entity /aos/v0 (non-const) of type Tac::DirImpl&gt;
default collection entityRef has:

$ del _['cachaca']
```

Upgrade From Apstra 4.1.X to 4.2.1 May Exhibit Different Interface Configlet Ordering (AOS-43786)

When upgrading an Apstra 4.1.x controller to Apstra 4.2.1, the order by which interfaces are appearing in interface-type configlets may change. There is no known functional impact, but due to the change of the configlet string in its entirety between the two Apstra versions, a difference may be reported during the upgrade procedure. Specifically, the Dump Config menu option (d) during the upgrade may alert of differences which are merely the exact same interfaces appearing in a different order between the old and the new version of the configlet.

---

vCenter Collector's Invalid Mac address Validation error (AOS-45831)

All PNICs in the dummy hypervisor, created by VMware mobility agent, have MAC addresses of none. A validation error is triggered by these invalid PNIC MAC addresses. Because data is not correctly gathered from the vCenter by the Virtual Infra Manager, Apstra's UI is unable to display the correct virtual machine visibility.

Virtual Network configuration changes do not properly reflect as changed after making a change in Apstra (AOS-40852)

After editing a VN (Virtual Network) configuration, if the same Virtual Network is open, none of the changes appear until the VN is opened again in the UI.

Workaround

After Saving the changes to the VN simply close the VN configuration and open it again. The second opening of the VN configuration page should reflect all changes that have taken place.

Virtual Network Validation Error 'Virtual gateway IP allowed only if IPv4 subnet specified' when IPv4 subnet as netmask and Virtual G/W address as static IP address (AOS-43352)

When IPv4 subnet information is configured with netmask information in the Virtual network, Apstra assumes that Virtual G/W address should be dynamically provisioned from dynamic IP pool. If static Virtual Gateway IP address is configured together with netmask in the subnet field, it would trigger validation error not to use static Virtual Gateway IP address

Workaround

Assign static IPv4 block into IPv4 subnet field with static Virtual Gateway IP address or clear Virtual Gateway IP address in the Virtual Network.

VirtualInfraGraphAgent Crash by removing transport zone on multiple transport nodes (AOS-45842)

VirtualInfraGraphAgent creates nodes and relationships based on data provided by Vcenter's collector. When the collector encounters validation errors due to invalid MAC addresses, it may produce incomplete transport vnet information that is separate from the hypervisor. The NSXT configuration change in the problem status, which includes removing the transport zone from multiple transport nodes, causes the dangling transport vnet to be released several times, causing the agent to crash.

VirtualInfraGraphAgent Crash from portgroup not managed by NSXT (AOS-45840)

The current Apstra implementation expects NSXT to exclusively control the ESXi hosts it is managing. When a portgroup is created in the ESXi hosts not by NSXT but by vCenter, restarting VirtualInfraGraphAgent can cause the cleanup process to reference invalid information in the portgroup. If NSXT with vCenters is registered in Apstra, NSXT should create and manage all portgroups.

ZTP devices, which use python3, fails in getting ztp_py3.py file via tftp (AOS-47007)

In Apstra ZTP < 5.0.0, ZTP for Junos EVO devices would fail as the `'ztp_py3.py'` is not available over tftp to provision due to missing the right file permissions.

Workaround

```
chmod +r /containers_data/tftp/ztp_py3.py
```

ZTP UI Should Not Send Non Configured Params in API Payload (AOS-44596)

The UI should not configure the keys in the ztp.json configuration for system-agent-params if the user has not configured the values. The ZTP UI reports the payload with empty strings, which trips the schema validation. For the attached screenshot, I added Junos as the platform in the GUI for the configurator, and the UI generated a payload with the platform, agent_type, job_on_create, and profile. This is unexpected.

Known Apstra Security Issues

Apstra - SONiC 4.1.2 Misconfiguration of CONFIG_DB allows unauthenticated RESTCONF calls (AOS-46786)

SONiC devices configured by Apstra with SONiC release 4.1.0 or higher expose an unauthenticated RESTCONF HTTPS server due to unhandled changes in the configuration database schema between SONiC versions 4.0.0 and 4.1.0. This issue affects all Apstra releases prior to 5.0.0.

When a SONiC device running 4.1.0 or later is configured with "client_auth": "cert" but without a security profile, it will allow any remote HTTPS call to query or modify the device configuration without requiring authentication.

```
root@sonic:/etc/sonic# curl -k https://localhost/restconf/data/openconfig-
system:system/state/hostname
{"openconfig-system:hostname":"sonic"}
```

Workaround

For Apstra versions 4.2.1 and 4.2.2, user can apply given Apstra workaround configlet to all SONiC devices using the text below.

This configlet will migrate the certificate from the Apstra device agent to the new 4.1.0+ trust store and re-enable certificate authentication for the HTTPS RESTCONF server. The configlet should be assigned in the Apstra UI to all SONiC devices across all blueprints, applied under the system section.

Note: For devices that are not deployed or not assigned to a blueprint, it is strongly recommended to create and run the script manually:

```
#!/bin/sh -

exec > /tmp/fix_cert.out
exec 2>&1

date

grep ^build_version /etc/sonic/sonic_version.yml | grep -q 4.0. && exit 0
```

```
if test -f /etc/aos/aos_ca_cert.pem; then
    cp /etc/aos/aos_ca_cert.pem /home/admin/aos.crt
    sudo -u admin sonic-cli -c 'crypto ca-cert install home://aos.crt' -c
config -c 'crypto trust-store aos ca-cert aos' -c 'crypto security-profile
trust-store aos aos' -c 'ip rest security-profile aos' -c exit
fi
```

true

Apstra VM SSHd Terrapin Vulnerability (AOS-44494)

Default sshd ciphers and mac exchanges included as part of Apstra base OS are vulnerable to terrapin attack for chacha20-poly1305@openssh.com and etm mac exchange hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com

Workaround

To mitigate the Apstra Base OS SSHd Terrapin vulnerability, it is recommended that the most affected cipher and mac exchange be removed from the /etc/ssh/sshd_config file, or upgrade to 4.2.1.1

```
Edit /etc/ssh/sshd_config:
sudo nano /etc/ssh/sshd_config

REPLACE:
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

WITH:
Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-
ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Restart SSHd:
sudo systemctl restart sshd
```

OpenSSH Vulnerability CVE-2024-6387 in Apstra Server Version 4.2.x (AOS-47640)

Apstra server version 4.2.x, which is based on Jammy Ubuntu 22.04 includes OpenSSH version 8.9p1, is exposed to a security vulnerability identified as CVE-2024-6387.

Workaround

We recommend modifying the SSHD configuration according to the Ubuntu Security Team's guidance on CVE-2024-6387 to mitigate the risk. Contact Juniper Apstra Support for assistance.

```
Set LoginGraceTime to 0 in /etc/ssh/sshd_config
sudo systemctl restart sshd
```

SSH Terrapin Vulnerability Workaround Using SSH aes128-gcm or aes256-gcm Ciphers Is Not Supported by Apstra Paramiko SSH Client (AOS-44336)

Apstra uses the Paramiko SSH client library to access Junos devices. The Apstra version of Paramiko does not yet support the SSH ciphers aes128-gcm@openssh.com and aes256-gcm@openssh.com. Access from Apstra to the Junos device will not function properly if it is set up to use just these SSH ciphers.

Workaround

All Apstra versions can work with Junos devices via SSH with aes256-ctr cipher and hmac-sha2-256 or hmac-sha2-512 for hmacs, minimizing the impact of the SSH Terrapin vulnerability

Please use an Apstra system set configlet for Junos devices to configure SSH ciphers and MAC encryption, or upgrade to 4.2.1.1.

```
set system services ssh ciphers aes256-ctr
set system services ssh macs [ hmac-sha2-256 hmac-sha2-512 ]
```

USN-6891-1(Python vulnerabilities) from Tenable scan report (AOS-48042)

Tenable scan reports USN-6891-1 (Python vulnerabilities) for both Apstra 4.2.x Controller and Apstra 4.2.x ZTP.

Workaround

Please contact Juniper Apstra Support Team

Known Third-Party Issues

Any blueprint commit results in the restart all BGP IPv4 and IPv6 peerings in any SONiC device (AOS-45866)

On any configuration push against a SONiC device, Apstra will always utilize the `'frr-reload.py'` script that is accompanying the FRR routing daemon, to gracefully apply any configuration changes made to that daemon, if any. It has been observed that in SONiC versions 4.1.2, this always results in the restarting of all IPv4 and IPv6 peerings. This includes cases where there is no change whatsoever to the FRR routing configuration.

ClusterHealthWriterAgent Error During Initial Deployment (AOS-44106)

On an initial deployment, the customer may see the following traceback error in `/var/log/aos/controller/ClusterHealthWriterAgent.err`:

```
IndexError: Aos::MetricLog::MetricLogWriter.newMetricLogWriter: error in
function call : Tac::RangeException("Error mounting event file:
/var/lib/aos/metricdb/cluster_health_info/container/utilization/meta-
1704279564839064-180-2024-01-03--10-59-24.839098.tel")
```

This issue is identified as an intermittent glitch while interacting with VM FileSystem within the "aos_controller_1" container. The ClusterHealthWriterAgent process will recover on its own after the restart without any action from the user.

Firewall function in the Junos device may not work correctly when Security policy rule with tcp-established used (AOS-45677)

When a rule with the tcp-established option exists in the Security Policy, even if the Apstra correctly renders the device configuration into firewall function, a Junos device running less than 22.2 version may fail to function properly because the entries are incorrectly programmed in the hardware.

Workaround

Upgrade the Junos version to at least qualified NOS version 22.2R3

---

gRPC Sequence Number Overruns Anomaly After Apstra Upgrade (AOS-43731)

Due to a current limitation in Junos, when two gRPC clients are subscribing to the same paths, the user may see Apstra anomalies for "gRPC Sequence Number Overruns" after an upgrade from

Apstra 4.2.0 to Apstra 4.2.1 if the user leaves the old Apstra 4.2.0 controller online.

Workaround

The user should shut down the old Apstra 4.2.0 controller before activating the new Apstra 4.2.1 controller to avoid this issue.

---

gRPC server reset count anomalies in the JUNOS-EVO platform (AOS-53526)

gRPC server reset count anomalies are observed in the JUNOS-EVO platform when `gRPC Max Client connection limit error` occurs in the device due to the problem that gRPC stalled connections are not cleared. gRPC keepalive is not enabled by default on the JUNOS-EVO platform running 22.2R3 or 22.4R3, which is the cause of the problem. gRPC keepalive is enabled for 300 seconds in the `>=23.4R2-EVO release` to avoid a build-up of stalled gRPC connections.

Workaround

In JUNOS-EVO device running 22.2R3 or 22.4R3, apply the below configuration via configlet into the device to enable gRPC keepalive or upgrade the device to `>=23.4R2-EVO`. For further assistance, please contact the Juniper Apstra Support Team.

```
set system services extension-service request-response grpc grpc-keep-alive
300
```

Juniper ACX Incomplete Packet Exported to Sflow Collector (AOS-42800)

When operating Juniper ACX devices, you might encounter a situation where layer-3 packets are inaccurately identified as layer-2 packets. This can result in incomplete packets being exported to the flow collector.

Juniper EVO When Configured With DHCP Relay as Border Leaf Role, DHCP Packets May Be Discarded (AOS-43348)

When Juniper EVO device hosts DHCP servers in a border leaf role with DHCP relay configuration, DHCP may not work as intended due to an unresolved bug in Junos EVO which prevents DHCP packets from being processed correctly.

Workaround

Using Apstra's configlet feature, create configlet to remove the rendered DHCP relay configurations and apply it to the Juniper EVO border leaf device.

Junos EVO Forwards DHCP for Virutal Network With DHCP Forwarding Disabled (AOS-43238)

Due to an outstanding bug in all available versions of Junos EVO, when two virtual networks are hosted on the same set of ESI leafs, one with DHCP enabled and one with DHCP disabled, the virtual network with DHCP disabled will also have DHCP requests forwarded.

Manual Reboot Required for "shared-tunnels" Configuration Following Junos Upgrade (AOS-45139)

In the Apsta 4.2 reference design change for MAC-VRF, the Junos "forwarding-options evpn-vxlan shared-tunnels" configuration is added via the Apstra rendered configuration. However, this command requires a device reboot to take effect with the Junos warning "Config: forwarding-options evpn-vxlan shared-tunnels has changed. A system reboot is mandatory". A user doing a Junos upgrade with Apstra may re-experience this issue after the device is upgraded.

Workaround

To avoid the need to a additional, manual reboot after a device Junos upgrade, the user can add the following configuration to the Apstra device system-agent pristine-configuration.

```
forwarding-options {
  evpn-vxlan {
    shared-tunnels;
  }
}
```

This can be done in the "Decvices / Managed Devices / Pristine Configuration" Apstra UI or using the Apstra-CLI "system pristine_config_append" command.

NXOS BGP Crashes When Removing and Reapplying Dynamic BGP Connectivity Template (AOS-44239)

NX-OS 9.3(11) BGP crashes when removing and reapplying dynamic BGP CT as follows,

- Unassign CT from VLAN interfaces

- Edit CT and specify IPv4 subnet for BGP Prefix Dynamic Neigbors
- Reassign CT to VLAN interfaces
- Edit VN, verify that Secondary IP Allocation mode has changed from 'forced' to 'enabled, and remove IPv4 addresses from leafs
- Commit config

```
BGP-3-ASSERT: bgp- [27133] ../routing-sw/routing/bgp/bgp_peer.c:2004:
Assertion `*prev_peer' failed.
SYSMGR-2-SERVICE_CRASHED: Service "bgp" (PID 27133) hasn't caught signal 11
(core will be saved).
```

Workaround

Manually shutdown the BGP peers before changing the dynamic BGP connectivity template to avoid the BGP crash.

Packet Drops on Untagged Layer-2 Interfaces on EX4400, EX4650, and QFX5120 Platforms (AOS-42959)

Due to an outstanding bug in versions of Junos prior to 22.2R3-S3 on the EX4400, EX4650, and QFX5120 platforms, packets may be dropped on layer-2 interfaces configured with an untagged native VLAN.

Workaround

Upgrade to Junos 22.2R3-S3.

Sonic 4.0.5 drops broadcast traffic on L2VN when the borderleaf also has a L3VN with dhcp-relay enabled (AOS-46321)

When an L2VN and an L3VN with dhcp-relay enabled coexist on the same border leaf device, Sonic 4.0.5 adds an L2 filter rule to drop incoming broadcast traffic at ingress.

```
ebtables rule applied pcnt = 76 -- bcnt = 24928-p 802_1Q -d Broadcast --vlan-
encap 0800 -j DROP
```

Workaround

Upgrade to AOS 4.2.2 and upgrade to Sonic 4.1.2

SONiC 4.1.0/4.1.1 to 4.0.x downgrade fails due to missing SWITCH config_db.json section (AOS-41304)

A device NOS upgrade to SONiC 4.1.1 may fail AFTER SONiC 4.1.1 has been successfully installed, and the downgrade to a previous Sonic version may fail as well.

Workaround

You must ensure (before downgrading) that the upgraded pristine configuration has already been collected. This can be verified by checking that the SWITCH table has been added in the pristine configuration. If the SWITCH table is not there, then by downgrading, the configuration will be completely reset, and any customized configuration will be lost. SONiC 4.1.2 will be fixing this defect and downgrades will work correctly from SONiC 4.1.2 to 4.0.x even if the SWITCH table is missing.

SONiC log rotation may not work, causing /var/log to get filled up (AOS-44012)

Due to `/usr/sbin/` not being in the default PATH and an explicit PATH is not set in cronjob `/etc/cron.d/logrotate`, the regular recurring rotation that is done by `/usr/bin/log-rotate.sh` which is exercised in `/etc/cron.d/logrotate` does not work correctly.

Despite that, if `disk-log-rotate-daemon` is operational, it will also invoke /usr/bin/log-rotate.sh itself, this time with the correct PATH set. However, for this to happen, files `/var/log/rotate/disk/info` and `/var/log/rotate/disk/debug` have to be present in `/var/log`. If these files are removed for any reason by the user, then `/usr/bin/log-rotate.sh` will not be invoked by the `disk-log-rotate-daemon`.

Workaround

Please never manually delete files under `/var/log` in a SONiC device, especially the files mentioned in the description.

Static route for loopback address of external router not installed in the SONiC device (AOS-45557)

If a SONiC device removes and then re-adds an IP address, the device may fail to add a static route involving that address to the kernel routing table, even if the static route configuration exists. The `show ip route` output in `vtysh` in the SONiC device experiencing this issue may

include the following output lines:

```
S>r  198.51.100.2/32 [1/0] via 192.168.0.9, Po1.4, weight 1, 01:59:25
B *  198.51.100.2/32 [20/0] via 10.0.0.3, Vlan201 onlink, weight 1, 01:59:25
```

Above, the "S" static route has been rejected by the kernel and was not installed.

Workaround

A full config apply will restore normal operation, in case such a problem occurs.

Symmetric IRB on Enabled on Junos EVPN-VXLAN Stitching Fails to Forward Traffic (AOS-43921)

Combining Symmetric mode IRB with EVPN VXLAN Stitching is not recommended until an upcoming Junos release supports this feature. If Symmetric IRB is configured, local hosts attached to the EVPN-DCI border gateways will fail to generate the additional Type2 Mac:IP label corresponding to the L3 VNI, they will operate asymmetrically.

Workaround

Avoid attaching hosts to EVPN VXLAN Stitching DCI Border leafs, or disable Symmetric IRB.

Known Apstra Flow Issues

Not Able to See Apstra Flow Dashboards as Tenant Switched to Private (AOSEXT-2, ESD-460)

When logged into the Apstra Flow UI, occasionally, when the UI times out, the user is switched from the Global to Private tenant, rendering the dashboards inaccessible once they log in again.

Affected Product Version

6.4.2

Workaround

Manual workaround:

Click the user icon at the top right and select Switch tenants to change back to the Global tenant.

Permanent workaround:

```
modify /etc/opensearch-dashboards/opensearch_dashboards.yml file to change
following:

    from: opensearch_security.multitenancy.tenants.preferred: [Private,
Global]

    to: opensearch_security.multitenancy.tenants.preferred: [Global, Private]
```