Juniper Apstra Version 4.2.0 Release Notes

Known Critical Apstra Issues

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.

Feature Configuration Rendering Changes

Add option to enable "graceful-restart" on Juniper devices (RFE-2764)

Feature Category: Design, Build, Operate

- On Juniper devices "graceful-restart" is, by default, only rendered under the "protocols bgp" configuration hierarchy. This is a necessary but insufficient condition to benefit from the Graceful Restart functionality in the context of Dual-RE Systems switchover. It is also required to render the same "graceful-restart" command under the "routing-options" configuration hierarchy for the default Routing-Zone and under the "routing-instances" configuration hierarchy for the non-default Routing-Zones.
- This is now possible by enabling the option under "Staged" > "Fabric Settings" > "Virtual Network Policy". This option is enabled by default on any new blueprint and disabled by default on any existing blueprint, deployed prior to 4.2.0. You can manually enable it after upgrading to 4.2.0. Be aware that enabling this option on a running blueprint makes BGP and BFD sessions flap.

Duplicate MAC detection timer for Juniper devices (RFE-2425)

Feature Category: Telemetry and Analytics

- Implementing "duplicate-mac-detection auto-recovery-time" under "protocols evpn" configuration hierarchy, with a timer of 5 mins. This allows not to keep the anomaly forever in the "EVPN Host flapping" probe when a duplicate MAC is detected.

New Features

Add Device Profiles for Cisco 93108TC-FX and Cisco 93108TC-FX3P (RFE-2846)

Feature Category: Device Profiles

Apstra has now Device Profiles for Cisco 93108TC-FX and Cisco 93108TC-FX3P fixed switches.

Add Device Profile for Juniper vJunosEvolved (RFE-2834)

Feature Category: Device Profiles

Apstra has now a Device Profile for the vJunosEvolved image which can be used in virtualized environments for training and testing use cases.

Add Device Profile for Juniper vJunos-switch (RFE-2666)

Feature Category: Device Profiles

Apstra has now a Device Profile for the vJunos-switch image which can be used in virtualized environments for training and testing use cases.

Add Device Profile for Juniper ACX7024 (RFE-2553)

Feature Category: Device Profiles

Apstra has now a Device Profile for Juniper ACX7024.

Add Device Profile for Cisco C93360YC-FX2 (RFE-2758)

Feature Category: Device Profiles

Apstra has now a Device Profile for Cisco C93360YC-FX2 fixed switch.

Add Device Profile for Arista 7280CR3MK-32 (RFE-2930)

Feature Category: Device Profiles

Apstra has now a Device Profile for Arista 7280CR3MK-32.

Add Device Line Card for Arista DCS-7500R3-24P-LC (RFE-2699)

Feature Category: Device Profiles

Apstra has now a Device Line Card for Arista DCS-7500R3-24P-LC.

Supported device operating systems for Apstra 4.2.0 (RFE-2773)

Feature Category: Device Operating Systems

The following updates have been made for network operating systems qualified for the Apstra 4.2 release.

Juniper Networks:
Junos (All roles)
21.4R3-S4, 22.2R3, 22.4R2. Deprecated qualification for the 20-train, 20.4R3-S5.

Junos Evolved for the IP-Forwarder role (Spines in EVPN or any role in an IP-Fabric):
21.2R3-EVO, 21.4R3-EVO, 22.2R3-EVO, 22.4R2-EVO. Deprecated qualification for the 20-train, 20.4R3-S3-EVO.

Junos Evolved for EVPN leaf roles:
Added qualification for 22.2R3-EVO, 22.4R2-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
4.0.5. Deprecated qualification for 4.0(2) and the 3.x train

Junos Commit-Check (RFE-2521)

Feature Category: Device Operating Systems

- You can now run Commit-Check on Juniper Junos devices to help verify your candidate configuration before committing.
- This check applies to all the staged changes, including configlets in DataCenter blueprints and configuration templates in Freeform blueprints.
- The result includes commit-check status, the configuration diff, and any error message if the commit-check is unsuccessful.

Adjusting the default settings for VXLAN routing net-hop and interfaces for QFX5110, QFX5120, and EX4400 devices (RFE-1932)

Feature Category: Device Operating Systems

The feature ensures the next-hops table size is proportional to the QFX5110, QFX5120, and EX4400 device capacity in high-scale environments. You can enable this feature in the blueprint settings tab for existing deployed blueprints. Be aware this is service-impacting. This is enabled by default for all new blueprints you deploy.

Virtual Networks Statistics (RFE-2749)

Feature Category: Design, Build, Operate

You can now obtain an easy-to-read summary of the blueprint's logical scale. A new sub-tab "Statistics" is available under "Virtual" for both the "Staged" and "Active" view of the blueprint. You'll find several charts capturing the summary of the logical scale from multiple dimensions. This is an important factor contributing to the scaling capabilities of both managed devices and the Apstra Server.
You will find the following metrics:
1) Virtual Network distribution per Routing Zone.
2) Virtual Network Instances distribution per Virtual Network, i.e. how many individual leafs or access switches a virtual network spans across.
3) Virtual Network Instances distribution per Leaf, i.e. how many virtual networks are hosted on individual leafs.
4) Virtual Network Instances distribution per Access Switch, i.e. how many virtual networks are hosted on individual access switches.
5) Virtual Network Endpoints distribution per Virtual Network, i.e. how many individual Generic System interfaces a virtual network spans across.

6) Virtual Network Endpoints distribution per Generic System Interface, i.e. how many virtual networks are configured on individual Generic System interfaces.
You also can export the information as an image file (.png), for easy sharing and collaboration with Apstra's support and product management.

User Interface for Apstra ZTP (RFE-1131)

Feature Category: Design, Build, Operate

New user interface for Apstra ZTP to manage the dhcp.conf and ztp.json files in an intuitive UI and improve the device onboarding experience.

System tag availability in device model context for configlet usage (RFE-2988)

Feature Category: Design, Build, Operate

System-specific configlets are now available within the device model context for configlet usage in the datacenter reference design. These are exposed underneath the device model key 'system_tags' as a list of tags applied to leafs, spines, superspines, and access switches. These tags will preserve the capitalization of the created tag. A system tag "tag_Foo" will be included in this list as "tag_Foo".

Support for symmetric Integrated Routing and Bridging (RFE-2550)

Feature Category: Design, Build, Operate

For Routing Zones in EVPN blueprints, you can now enable symmetric Integrated Routing and Bridging (IRB) instead of asymmetric. This feature improves scaling for networks with a large number of VLANs and also expands multi-vendor interoperability options. The mac-vrf is already the default for Junos-Evolved. For more information:
https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/topic-map/evpn-sym-t2-routing-ov.html#concept_sym-t2-evpn-vxlan-ov__section_whg_1cf_zrb

---

Option to to transition Junos configuration to MAC-VRF mode (RFE-2634)

Feature Category: Design, Build, Operate

In releases before 4.2, Apstra used a single default switch instance as the configuration mode for Junos. In Apstra 4.2, Apstra transitioned to using MAC-VRF for all new blueprints and

normalized the configuration of Junos to Junos Evolved. This option allows you to transition Junos devices to the MAC-VRF configuration model for any blueprints deployed before the 4.2 release. All models use the VLAN-Aware service type.

Option to select a subset of Virtual Networks or Routing Zones when exporting them to a CSV file (RFE-2631)

Feature Category: Design, Build, Operate

You can now select a specific set of Virtual Networks or Routing Zones before clicking on the export button, which will only export your selection in the CSV file.

Option to only show rows with errors when importing/exporting VNs and RZs (RFE-2702)

Feature Category: Design, Build, Operate

When you import Virtual Networks or Routing Zones using a CSV file, Apstra will parse the file for any errors and return the entries as a table highlighting the errors found.
You now have the option to only show the table entries that contain errors and hide the rest.

New logical devices (LDs) and interface maps (IMs) for Juniper devices (RFE-2651)

Feature Category: Design, Build, Operate

We have added over 80 new out-of-the-box logical devices and over 170 interface maps for Juniper devices. These additions reduce the time and steps required to start designing your data center templates while providing more built-in selections to clone and edit for those requiring customized designs.

Interface tagging (RFE-2581)

Feature Category: Design, Build, Operate

In Datacenter reference design you now can apply tags on interfaces, similarly to the tags applicable to Systems and Links.
Both physical and logical interfaces (port-channel) can be tagged.

Intelligently add routing zones configuration only when required by endpoints (RFE-1575)

Feature Category: Design, Build, Operate

Prior to 4.2, the default behavior rendered routing zone (VRF) configuration on all leafs devices in an EVPN blueprint, irrespective if a leaf hosted an endpoint in the routing zone or not. Enabling this selection changes the behavior by intelligently adding routing zones to leaf devices only when required by endpoints, resulting in fewer resources needed and utilization improvements on the devices. This is enabled by default for new blueprints in 4.2 and greater. This can be changed in Policies > Routing Zone Policies.

Import / Export of Freeform Blueprints (RFE-2621)

Feature Category: Design, Build, Operate

You now can easily export and import Freeform Blueprints.
Upon export, some elements of the Blueprint can be selected to be exported or not. As an example, the System to Serial Number association is disabled by default. Check the documentation for more details.

Fine-grained control over MTU settings (RFE-2150)

Feature Category: Design, Build, Operate

You now have the ability to configure blueprint-wide MTU defaults for the fabric interfaces, virtual networks Layer-3 interface, and IP Links to generic systems. Additionally, you can override the default settings individually during service creation for each element.

Execution of "Show" CLI commands for Juniper devices (RFE-1002)

Feature Category: Design, Build, Operate

- You can run any "Show" CLI command on any Juniper-based device. This capability is available for devices acknowledged in Apstra, whether associated with a Blueprint or not. Junos and Junos-EVO CLI schemas for the supported versions are pre-loaded to facilitate the identification of a CLI command and to offer auto-completion whenever possible.
- The command can be executed in text, XML, or JSON, and the output can be copied to the clipboard.

Create new Rack Types using the new Designer Interface (RFE-2680)

Feature Category: Design, Build, Operate

When creating a new Rack Type, you can now choose to do it the traditional way by completing UI Forms "Create in Builder" or by dragging and dropping the elements composing your Rack using the new "Create in Designer" workflow (which is also used for building network topologies in Freeform blueprints).

Create link in existing LAG in one step (RFE-2352)

Feature Category: Design, Build, Operate

Adding a new server-facing link into an existing LAG can now be done in one step: select a leaf in the topology view, click on an unused interface, then click on the existing LAG, and the new option "Create link in LAG" will appear.

Bulk delete Generic Systems (RFE-2355)

Feature Category: Design, Build, Operate

You can now search for and delete multiple Generic Systems at a time under the "Nodes" Table in the Topology view.

Blueprint wide search (RFE-2715)

Feature Category: Design, Build, Operate

A new intelligent search capability that provides you with a user-friendly interface and advanced search filters to locate network elements inside of your blueprints. This enhancement makes it easy for you to quickly find IP addresses, endpoints, virtual networks, and other network data you're looking for.

Allowing a change of Device Profile in a Freeform blueprint (RFE-2687)

Feature Category: Design, Build, Operate

You now can edit the Device Profile selection of a managed system. This is useful in the following situations:

- RMA to replace a faulty device with a new one.
- Change of Device Profile from one model to another one. This use-case is possible if the newly selected Device Profile does not disrupt the existing cabling. Typical valid scenarios include: moving from one device profile to a larger one, or using a modular Device Profile with additional line cards for expansion.
- Replacement of the device profile definition with a new one to address any bugs with the original Device Profile definition.

Allow users to delete Routing Zones or Virtual Networks with active endpoints (RFE-1997)

Feature Category: Design, Build, Operate

In previous releases, in order to delete a Virtual Network, you first had to remove all the associated Connectivity Templates from existing allocated interfaces. This is now done automatically and you can force delete a Virtual Network even with active endpoints. Apstra will first show you which interfaces the Virtual Network is currently allocated to and ask you to confirm before proceeding.

Allow Specifying a Port-Channel ID range when creating LAGs between Spine/Super-Spine and External Generic Systems (RFE-2366)

Feature Category: Design, Build, Operate

You can now optionally specify which port-channel ID or ID range (min, max) you want to use when creating a new LAG interface between a Spine/Super-Spine and an External Generic System.

Administratively enable and disable interfaces (RFE-661)

Feature Category: Design, Build, Operate

You can now administratively enable and disable interfaces using the device context in the UI or via the API. The telemetry expectations are kept in sync with the chosen selection.

Adjusting the default settings for `overlay-ecmp` for the Juniper EX4400 device (RFE-2763)

Feature Category: Design, Build, Operate

In some high-scale environments, the default 8K settings for VXLAN Overlay next-hop are insufficient. You can enable this feature in the blueprint settings tab for existing deployed blueprints. Be aware this is service-impacting. This is enabled by default for all new blueprints you deploy.

Add Showtech Collector for Apstra ZTP (RFE-1836)

Feature Category: Design, Build, Operate

New script located at /usr/bin/ztp_show_tech on the Apstra ZTP to collect necessary logs.

Introducing gRPC based telemetry collection (RFE-1600)

Feature Category: Telemetry and Analytics

First phase of introducing gRPC based telemetry collection. In this release the following changes are delivered:

```
- MAC telemetry service is expanded with a gRPC based telemetry collection in
On-Change mode. Apstra uses gRPC only when the JUNOS version on the switch is
greater than or equal to 22.2R2, otherwise it uses SSH polling.
- The "Collection Type" for any telemetry service is visible through the
Devices > Services view. The "Device Telemetry Health" probe has also been
augmented to collect gRPC related statistics and raise anomalies in case of
sustained failures.
- MAC service requires an extra rendered config, under protocols, to support
remotely learned MACs. Use the built-in junos_protocols.jinja configuration
template to include the necessary configuration.
- In the case of offbox agents, gRPC port (32767) should be open between
agents and devices to allow streaming.
```

Graph Query builder and catalog of predefined queries (RFE-2669)

Feature Category: Telemetry and Analytics

- To define graph queries you can now use a Graph Builder as an alternative to Graph editor. Leverage the drop-down menus for guided and simplified query authoring. You can also switch back and forth between "Editor" and "Builder" views.
- Leverage the built-in catalog of predefined graph queries available to use in every UI location requiring a graph query, including IBA Processors and Freeform's resources generators and resource groups generators. Several examples are shipped by default, prefixed with "DC-" or "FF-" depending on what reference design they are intended for. Select the one closest to your needs and tweak it as you see fit.
- You can also save user-defined queries and reference them in the same way. Be aware that your query must execute correctly before it can be saved.

Exposing the aggregation Methods for IBA historical data (RFE-1624)

Feature Category: Telemetry and Analytics

You now can select the aggregation method to use when displaying the Time-Series data IBA:

- None: Do not aggregate the data
- Average: Average value for the metric in the aggregation period
- Last: Last value for the metric in the aggregation period
- Min: Minimum value for metric in the aggregation period
- Max: Maximum value for metric in the aggregation period

Custom Telemetry Collection (RFE-2491)

Feature Category: Telemetry and Analytics

- You can now ingest new telemetry data using UI-driven workflow for defining custom telemetry services. The functionality leverages Junos and Junos-Evolved CLI schema (RPCs), pre-loaded on the Apstra server, and lets you choose any CLI command and select the data to extract from its output.
- A given telemetry service must have one service schema and one or more collectors definition(s). Collector parameters expose different options to let you customize the collection definition based on several criteria: hardware family, hardware model, and NOS Version.
- The service can then be referenced in an IBA probe and automatically collected according to the definition of the IBA processor. Use the "Extensible Service Data Collector" Processor.

Upgrade Apstra server to Ubuntu 22.04 LTS (RFE-2802)

Feature Category: Platform

The Apstra server has been upgraded to Ubuntu 22.04 LTS to offer you the latest features, security patches, and performance enhancements.

Changed Features

Support for 200G and 400G interfaces for all operating systems (RFE-2357)

Feature Category: Device Operating Systems

This enables 200G and 400G interface support for capable devices across all supported network operating systems.

Enhancements to configlet's scope for interface-based configlets (RFE-2334)

Feature Category: Device Operating Systems

- Enhancements to the configlet's scope, during the import step, when importing an interface-based configlet. You can select the interface role more clearly and distinguish Port-Channel/Aggregated interfaces from physical interfaces, from sub-interfaces. You can also define the configlet's scope based on interface tags.

User-friendly description and resolution for Blueprint Build Errors and Warnings (RFE-2662)

Feature Category: Design, Build, Operate

As you make changes to your Blueprint, Apstra validates the changes and raises any issues as a Build Error or Build Warning under the Uncommitted tab. The description of these issues has

been improved to be easier to understand and act on. Additionally, a "resolution" column was added to help you navigate to the location where to resolve this issue.

Port-channel endpoint groups in Freefrom blueprints (RFE-2713)

Feature Category: Design, Build, Operate

Introducing the notion of port-channel endpoint groups to facilitate the resources allocation to aggregated interfaces.

Performance improvement to the Freeform's cabling-Map editor (RFE-2759)

Feature Category: Design, Build, Operate

- The performance of the cabling-Map editor in Freeform blueprints has been improved to support topologies with up to a 1000 nodes. This UI enhancement allows to edit topologies with high number of nodes.

Option to block users from overriding other users staged changes (RFE-2770)

Feature Category: Design, Build, Operate

Added an option in user roles to toggle users' ability to override other users' staged changes. This option was added as part of the built-in default user role.

Moved MAC-MSB setting to the new blueprint DCI tab (RFE-2918)

Feature Category: Design, Build, Operate

The MAC-MSB setting has been moved to the newly introduced "DCI" tab in deployed blueprints. The DCI tab is a more intuitive and logical location for your workflow, resulting in a smoother and more efficient user experience. There is also a new tooltip describing when you would use this feature.

Increased number of Time Voyager saved revisions (RFE-2137)

Feature Category: Design, Build, Operate

Increased the number of Time Voyager user saved revisions from 5 to up to 100. Additionally, we provided better user feedback on the number of user-saved revisions and the amount left to use.

Improved the blueprint policy tabs and fabric settings interface (RFE-2784)

Feature Category: Design, Build, Operate

The Blueprint "Policies" tab has been reorganized to enhance clarity and provide a more intuitive workflow. The fabric settings have been relocated to their own tab called "Fabric Settings" while the security-related features have remained under "Policies".

Collect Apstra version and VM memory/CPU usage in backups (RFE-2579)

Feature Category: Design, Build, Operate

Collect additional information about the Apstra Server such as the version, and the VM memory and CPU usage in the Apstra backup files to improve the support experience.

Clarify the Accept/Revert config deviation message (RFE-2711)

Feature Category: Design, Build, Operate

Improve the help message when a user selects "Apply Full Config" or "Accept Changes" in the device Telemetry Config page.

Allow overlap of Port Channel ID ranges across different systems (RFE-2780)

Feature Category: Design, Build, Operate

You're now allowed to define overlapping port channel ID ranges as long as they're used on different devices.

Additional options for the topology label in Freeform blueprints (RFE-2682)

Feature Category: Design, Build, Operate

You now can choose the topology label to display in your Freeform's blueprint, including:
1. Hostname
2. Serial number
3. Management IP address

Additional dashboard metrics on the blueprint size (RFE-2714)

Feature Category: Design, Build, Operate

New fields in the blueprint dashboard summary to show physical structure, virtual structure, and total lines of configuration to provide insights on the size of the blueprint deployed by Apstra.

Add an "all" option to the apstra-cli command change-device-password for bulk operation (RFE-2837)

Feature Category: Design, Build, Operate

Add an "all" option to the apstra-cli command "change-device-password" to enable users to change all the device passwords in bulk with one command.

Ability to use policy assurance for IPv4 virtual networks when IPv6 applications are enabled (RFE-2744)

Feature Category: Design, Build, Operate

This change removes the previous constraint that prevented you from using the Apstra Policy Assurance feature when a blueprint had a mix of IPv4 and IPv6 virtual networks in EVPN blueprints. You can now take advantage of the Policy Assurance feature for IPv4 virtual networks in a blueprint with both IPv4 and IPv6 virtual networks deployed.

Update to IBA visualizations (RFE-2655)

Feature Category: Telemetry and Analytics

- Several UI enhancements to the IBA visualizations including: the different line charts, the fuel gauges used in the Match Count processor when "show context" checkbox is enabled,

the Sankey diagram used in the Headroom view of the "Device Traffic" probe and the IBA processors icon when viewing/editing a probe.
- The query fields at the stage level now support Regular expressions.

Support of Grouping Processors for Dynamic Stages (RFE-2573)

Feature Category: Telemetry and Analytics

You can now use grouping processors with dynamic stages input. Grouping is a commonly used technique in analytics to divide large datasets into groups and perform aggregate calculations on them. This helps you make sense of large amounts of data that would otherwise be difficult to understand.
The following grouping processors have been expanded to support input with dynamic stages:

- Match Count
- Match Percentage
- Set Count
- Standard Deviation
- Sum
- Average
- Min
- Max

Support of "Additional Keys" for Dynamic Stage Processors (RFE-2678)

Feature Category: Telemetry and Analytics

You can now use "Additional Keys' capabilities irrespective of the Data type including both Static stages and Dynamic Stages. In 4.2.0 the support of "Additional Keys" has been expanded to processors with Dynamic stages. This allows you to add context to the stage output by augmenting the telemetry data with Graph related data.

Increase polling interval of "Interface_Counters" telemetry service (RFE-2785)

Feature Category: Telemetry and Analytics

- "Interface Counters" telemetry service collection's interval is increased from 5 seconds to 30 seconds on all vendors and models. This increase in the collection interval allows better utilization of the managed device's CPU resources, in particular those with limited resources such as Juniper EX4400.
- This change is transparent to the consumers of this telemetry service including: 1) the "Device Traffic" IBA probe and 2) the "Traffic Heat Layer" visualization.

Enhancement to "BGP Flapping" Probe for better support of Freeform and renaming to "BGP Monitoring" (RFE-2598)

Feature Category: Telemetry and Analytics

"BGP Flapping" probe is now renamed "BGP Monitoring". It now has a better support of the different reference designs whereby an instantiation in Freeform blueprint creates additional stages to raise anomalies when sessions are "Down".

Add support of dynamic stages input for Match_String IBA processor (RFE-2954)

Feature Category: Telemetry and Analytics

You now can use Match_String Processor with dynamic stages input. This lets you expand the set of analytics you can perform on probes with dynamic stages type of data.

Enhancements to "API Explorer" page (RFE-2732)

Feature Category: Platform

Enriching the capabilities of API Explorer to make it the Go-To location for API decimation

- Ability to execute all verbs: POST, PUT, PATCH and GET.
- Granular expansion of the body of the JSON response and selective clipboard capability to copy/paste parts or all of the response.

Documentation of API endpoints (RFE-2660)

Feature Category: Platform

Enhanced documentation of API endpoints for both Datacenter and Freeform reference designs to help developers during the creation of API workflows.

Apstra-CLI update to content import/export to include new 4.2.0 elements (RFE-2979)

Feature Category: Apstra CLI

Add the capability to export/import the following elements:
-1) Predefined Graph queries: This contains the built-in as well as the user defined queries.
-2) Telemetry Collectors: This contains the user defined telemetry collectors via the Custom Telemetry Collectors functionality.

Apstra-CLI transitioning from "Experimental" to Fully Supported (RFE-2797)

Feature Category: Apstra CLI

Apstra-CLI is now a fully supported utility, the "Experimental" disclaimer is removed.

Removed Features

Remove EX4300 Device Profiles (RFE-2928)

Feature Category: Device Profiles

The EX4300 platforms are no longer supported and therefore the Apstra device profiles have been removed in 4.2.0. Upgrade to 4.2.1 will be blocked if any deployed EX4300's is found. EX4300s must be replaced with a qualified device.

Remove EX3400 Device Profiles (RFE-2923)

Feature Category: Device Profiles

The EX3400 platforms are no longer supported and therefore the corresponding Apstra device profiles have been removed in 4.2.0. Upgrade to 4.2.1 will be blocked if any deployed EX3400's is found. EX3400s must be replaced with a qualified device.

Remove EX2300 Device Profiles (RFE-2695)

Feature Category: Device Profiles

Remove the EX2300 device profiles as devices are no longer supported in data center use cases.

Remove Device Profiles and Interface Maps for Cumulus platforms (RFE-2582)

Feature Category: Device Profiles

The Device Profiles and Interface Maps for Cumulus platforms have been removed.

Cumulus Deprecation (RFE-2308)

Feature Category: Design, Build, Operate

- All Cumulus related elements are removed from the Apstra's UI.

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.

Technical Preview support for Integrated DCI (Data Center Interconnect) technology (RFE-3047)

Feature Category: Design, Build, Operate

This Integrated DCI (Data Center Interconnect) technology to easily enables you to connect multiple DCs and applications together using a standards-based implementation. This model offers an unmatched degree of intelligence to ensure reliability and seamless connectivity over the Over-the-Top model.

Configurable error levels for IP or ASN overlap validations (RFE-2779)

Feature Category: Design, Build, Operate

You can now configure the error level down to warnings only or no errors/warnings at all when an IP or ASN overlap is detected in the staged environment. It is not recommended to lower down the error level unless the IP or ASN overlap is intentional and there's no need for validating it.

Query-Based Analytics (RFE-1671)

Feature Category: Telemetry and Analytics

First phase of introducing a Data Analysis capability under the Analytics umbrella. This is an augmentation to the existing analytics capabilities of Intent-Based Analytics and is categorised under the name of QBA for Query-Based Analytics. It allows to query data coming from multiple sources and join them together for processing. It employs statistical analysis to provide a data-driven approach to analytics. This first phase includes three predefined reports:

- Traffic report.
- Optical Transceiver report.
- Device Health report.

Technical Preview support of Junos Evolved on-box agents (RFE-1948)

Feature Category: Platform

As a Technical Preview, you now have the ability to leverage on-box agents with devices running the Junos Evolved on-box agents.

Fixed Apstra General Issues

"Device Telemetry Health" Probe May Not Raise Anomalies (AOS-35948)

If the "optical_xcvr" service fails on Cisco NXOS devices, the "Device Telemetry Health" probe will not raise anomalies for these sustained telemetry failures.

All AOS Deployments Running a Specific Version Have the Same Set of Secret Keys (AOS-30511)

All AOS deployments running a specific version have the same set of secret keys. This is potentially a security flaw as a user having access to an AOS VM of a version can get access to secret keys installed in a different VM as they are all the same.

Apstra Show Tech Time-out During Arca Dump (AOS-41024)

Customers with a large blueprint and using Arca Automated Root Cause Analysis) may experience a time-out while collecting an Apstra "Show Tech" (aos_show_tech).

Arista 7280CR series deployment failure on maximum-paths command when running EOS prior to 4.25 (AOS-40823)

Configuration deployment Arista 7280CR series of switches will render maximum-paths 512 from the device profile hardware capabilities. When this configuration is rendered on EOS releases prior to 4.25, an error 'maximum-paths 512; invalid input' may be raised.

BGP Graceful Restart Not Enabled by Apstra (AOS-35171)

Apstra only configures graceful-restart under protocols bgp. Apstra does not configure graceful-restart under routing-options for the default routing-instance. Due to a Junos bug, graceful-restart does not work with non-default routing instances.

BlueprintDiffProducerAgent Crash When System Hostame Is Empty and Importing Configlet via Hostname (AOS-37837)

When configlet is imported with hostname based condition, configlet assumes that all systems should have hostname information. When hostname is set to null via clicking clear button in the UI while editing hostname field in the system, BlueprintDiffProducerAgent will crash due to missing hostname.

BuilderAgent crashes are seen after name for link is cleared in the UI (AOS-37065)

Link name for a link between system nodes are automatically created when link is created. However, when link name (link label) is accidentally cleared by clicking clear button in the UI, BuilderAgent
will crash because it uses link label as one of keys for sorting purpose.

Bulk Operation for VXLAN virtual networks without "Reserve across blueprint" configuration makes manually assigned VLAN ID changed (AOS-39517)

For the VXLAN virtual networks which don't have a "Reserve across blueprint" configuration, Bulk operation to add/delete those virtual networks to/from multiple nodes makes manually assigned VLAN ID for each virtual network to be changed to a new VLAN ID from VLAN Pool.

Cannot use exclamation point in NX-OS Configlet for passwords (AOS-14084)

When creating a configlet for custom username or SNMP3 password on an NX-OS device, "!" cannot be part of the password. This will result in an error as "CLI execution error", clierror: "% Ambiguous command".

Changing the Apstra Controller IP Address Will Not Update Uploaded OS Image URLs (AOS-37170)

If the user changes the Apstra Controller IP address either using netplan or aos_config, the URLs for any uploaded OS Images will continue to use the previous IPs, causing NOS upgrades to fail.

Clone Operations on EX4400 Device Profiles Removes Connector Type (AOS-36848)

If an attempt is made to clone the device profile of a device of the Juniper EX4400 family, the Apstra UI will not be able to recognize the connector types in the original device profile and will leave the connector type empty for all the affected ports. The clone cannot be created unless the connector types for every affected port have an acceptable value.

Contiguous Aggregate Routes Specified in Custom Routing Zone Policy Are Aggregated (AOS-38444)

When contiguous routes within a custom policy applied to a RoutingZone are used, the Apstra rendering engine will incorrectly summarize routes when rendering the VRF config for border leafs. Policy for external BGP sessions does not summarize aggregate routes, which may cause a summarized route to not be announced externally. For example, defining two aggregates, '7.7.6.0/24' and '7.7.7.0/24' will result in a BGP aggregate of '7.7.6.0/23', but the RoutesToExt prefix-list will list both ['7.7.6.0/24', '7.7.7.0/24'], preventing the aggregate route from advertising.

Resolution

Upon upgrade to 4.2.0, user-defined BGP aggregations in a contiguous subnet range will be unfolded into the exactly specific user-defined aggregates as optionally defined in a routing policy associated to a routing zone. This also supports a use case of an aggregation for a more specific aggregation within a larger subnet.

Continuous MLAG Anomalies With Cisco NXOS Offbox Agent (AOS-38836)

When servers, connected to VPC switches via MLAG interfaces, are deployed, Apstra raised MLAG anomalies continuously for MLAG interface state as unknown even if it's up state. The issue is related with parsing error of Cisco VPC command output. it can happen only if Cisco device agent is used with offbox agent and servers connected to MLAG interfaces are deployed mode to track link status.

Device Environmental Checks IBA Probe Not Working With Juniper EX3400-48T (AOS-38598)

Apstra users will see sustained execution failure anomalies from telemetry health for Juniper EX3400-48T devices after instantiating the Environmental Checks IBA Probe.

DeviceTelemetryAgent Process' continuous crash in the offbox agent (AOS-37597)

It is presumed that the aos_cache file contains data if it is there when the DeviceTelemetryAgent process starts. There is a situation where the file is left empty due to an unexpected agent process crash. It makes the agent process crash repeatedly with an exception when it restarts and attempts to read data from the empty file.

Resolution

To store data, a temporary file will be used. Rename the file to the aos_cache file if the temporary file is closed to ensure that it always contains the correct data.

IBA Hypervisor MTU Threshold Check Anomaly Telemetry Error (AOS-37312)

The Apstra user may get IBA Hypervisor MTU Threshold Check related anomalies, withe pnic related traceback "KeyError" messages in DeviceTelemetryAgent.

In the VM Query, VM Doesn't Show the Connected Leaf Node and Interface (AOS-37913)

When Leaf node, connected by VMware ESXi hosts, is configured with domain name and hostname, fully qualified hostname is reported to ESXi host via LLDP. When the fully qualified hostname is exactly matched against the leaf node's hostname (non-fully qualified name), it leads to match failure so that the connected leaf node can't be found.

Resolution

In 4.2.0, we introduced protective logic to allow loose match by ignoring the domain name, covering most of scenarios in the customer environment

---

Incorrect Selection of Items When Using Query on "Change Link Speed" (AOS-37589)

Under Staged>Physical>Links>Change Link Speeds, the Query option displayed items according

to the pagination of items. When selecting all for that page, it will select all the items comprised of other pages as well.

Jinja Custom Filters Unavailable for Apstra Configlets (AOS-37781)

Jinja custom filters listed in the Jinja documentation are unavailable for Apstra Configlets. Making use of these will raise blueprint property set validation errors.

Resolution

Jinja custom filters listed in Jinja documentation are now available for Configlet usage beginning with Apstra 4.2.0.

Jinja Extensions jinja2.ext.do and jinja2.ext.loopcontrols Unavailable for Apstra Configlets (AOS-37559)

Jinja extensions jinja2.ext.do and jinja2.ext.loopcontrols are not available for Apstra Configlets, raising template syntax errors when used.

Resolution

Support for these Jinja extensions is available starting with Apstra 4.2.0.

Jinja Functions Unavailable for Apstra Configlets (AOS-34661)

Jinja functions listed in the Jinja documentation are unavailable for Apstra Configlets. Making use of these will raise blueprint property set validation errors.

Resolution

Jinja functions listed in Jinja documentation are now available for Configlet usage beginning with Apstra 4.2.0.

Juniper QFX10008 may fail to report rpm fan telemetry (AOS-40731)

Juniper QFX10008 may fail to report fan telemetry causing telemetry issues within Apstra.

Resolution

Juniper QFX 10008 failing to report fan telemetry is correctly handled and resolved in Apstra 4.2.0

Junos 20.2 QFX 5K & EX series - VXLAN configuration for no-arp-suppression removed and added after agent restart (AOS-23725)

On Junos platforms running 20.2R2 or higher, on QFX 5K & EX series, no-arp-suppression is not required in configuration rendering as underlying bugs have been fixed by Juniper related to this feature.

After the AOS Deployment agent on the AOS controller restarts, two configuration jobs may be unexpectedly pushed in rapid succession without user action:

One configuration containing 'no-arp-suppression' followed by one without 'no-arp-suppression'.

Impact to forwarding/data plane is unknown.

NSX-T 3.2 Integration Does Not Handle LAG Mode (AOS-38557)

The Apstra NSX-T collector may crash because it gets a "none" value when the VDS uplink mode is configured as LAG mode.

NXOS BGP Incorrect local-as Command Negation (AOS-43313)

When reverting a Cisco NXOS BGP configuration which uses the local-as command, Apstra uses just the "no local-as" configuration command which is invalid and will cause a deployment anomaly.

Offbox System Agent and IBA Containers May Restart (AOS-33181)

Certain conditions may cause Apstra offbox system agents and IBA containers to restart when it starts. This will only happen if a new container configuration is created while the agent is down. This should have no impact.

OffboxAgentManager crashes continuously after restoring backup (AOS-37265)

After restoring backup in the new AOS vm, OffboxAgentManager crashes are seen. This issue is

related with system Key difference between old AOS server where backup (taken by show tech) was executed, and new AOS server where restore is executed. This issue can happen for not only OffBoxAgentManager but also OnBoxAgentManager as long as Agent Profile's credential is used.

Predefined External Route Probe Is Not Displaying External Routes From Different BGP Peers (AOS-36501)

Due to an incorrect built-in graph query, the predefined external route IBA probe is not displaying external routes from different BGP peers toward external routers.

Route Anomalies Triggered in Juniper Junos-EVO Device When PIM Is Enabled Into Interface by Configlet (AOS-39289)

Route anomalies are reported in Juniper Junos-EVO device when PIM protocol is enabled via configlet function, even if all route entries correctly exists in the device. This issue is triggered by collector's parsing error during collecting routes in the Juniper Junos-EVO device.

Running `sysctl --system` causes offbox agents to go offline (AOS-36918)

If the user, on the Apstra VM CLI, runs `sysctl --system`, incorrect kernel forwarding parameters in `/etc/sysctl.d/60-aos_sysctl.conf` will be loaded causing off-box system agent Docker containers to go offline.

Running aos_show_tech on SONiC Device in Telemetry Only Mode May Make Device Unresponsive (AOS-36855)

Running the aos_show_tech script on a SONiC device running in Telemetry Only mode generates a very large checkpoint_config.tar and maxes out the available space in /tmp, leading to an unstable system.

Separate CTs Might Swap Assignments in Some Conditions (AOS-41465)

Under specific conditions where the user has multiple, similar connectivity templates (CT), an incorrect graph database structure might occur. This may cause unexpected validation errors when the user makes subsequent CT changes.

Setting VXLAN for the First Time and Enabling DHCP Helper Addresses Simultaneously May Fail in SONiC 4.X Devices (AOS-38701)

If vxlan vtep does not exist and is to be enabled in a blueprint as part of a day-2 operation, and in the same config apply any DHCP helper address is to be set in at least one vxlan-enabled vlan, the config apply operation will fail.

---

sustained error anomaly for Optical Xcvr collector in the Telemetry Health Probe raised for skipped interface (AOS-41017)

If the interface does not support all of the required information for optical transceivers, the Optical Xcvr collector is unable to parse the information, so it attempts to skip the interface and logs the reason in the error. The mechanism increases the collector's error count, which then causes anomalies in the Device Telemetry Health probe. The publishing error mechanism was originally designed to detect real collector issues. Skipping interfaces that may not provide the necessary information should not result in collector errors.

Resolution

Skipping interface would not increase error count for the collector. Therefore, anomaly for collector error would not be triggered.

Updates Made to Pristine Configuration Over UI Not Reflecting in the Backend (AOS-37131)

Pristine configuration edits over the Apstra UI may not be reflected in the backend.

Uploading Packages causes temporary false positives (AOS-12101)

When uploading packages to a device (eg. for using aos_developer_sdk) several Anomalies are seen in the UI (BGP, LAG, Interface and others). The Anomalies are transient, caused by a restart of the Telemetry Agent following the Package upload.

VirtualInfraGraphAgent May Restart When VMware NSX-T Collection and Configuration Coincide (AOS-38903)

If an Apstra user is using VMware NSX-T, a possible race condition may occur, which will cause the Apstra VirtualInfraGraphAgent process to restart, possibly causing temporary system

anomalies. This occurs when a telemetry collection is in progress, and the user makes a configuration change resulting in a possible inconsistent state. The Apstra VirtualInfraGraphAgent process will recover on its own, and virtual-infra functionalities wll not be affected.

ZTP Fails When Apstra ZTP VM Is Located in the Different Subnet From Device and NOS Upgrade Is Performed During ZTP Processing (AOS-40946)

After NOS is upgraded via ZTP processing, during the 2nd phase ZTP processing, JUNOS device may not install default route entry populated into the default routing table even if router option is received by DHCP server. Apstra ZTP assumes that default route is installed in the routing table when DHCP router option is bound into management interface. Because default route entry is missing, Apstra ZTP process in the device can't retrieve ztp.json file from TFTP server which led into failing ZTP processing.

ZTP for EVO Device Succeeds Even if Default Gateway Information Is Missing by DHCP (AOS-40147)

Apstra ZTP process requires devices to learn default gateway information by DHCP. The default gateway information is used to configure the default static route entry in the management routing instance. ZTP processing for Juniper EVO device succeeds without failing, even if default gateway information is missing. After ZTP processing, Juniper EVO device doesn't have a default static route in the management routing instance and becomes isolated from the other networks.

Fixed Third-Party Issues

ACX7100 on Junos 22.2R2-EVO Switches Incorrectly ModifyDestination IPv6 Address for Inner VxLAN Routed Packets After EVPN Trombone Routing (AOS-34809)

If a VTEP sends an EVPN Type5 routed packet to a remote leaf, and that remote leaf then uses an EVPN Type2 route for the destination and has to re-encapsulate to another remote vTEP, the ACX7100 may rewrite the inner IPv6 address of the destination IPv6 address incorrectly within the VXLAN packet. This flow would be seen for something like leaf3 -> leaf1 > leaf2, in which the packet is rewritten from leaf1 >leaf2. For example, route a05:fab:4::/64 is known on leaf3 via two VTEPs on leaf1&leaf2 which are both hosting the destination VN. The destination IPv6 address a05:fab:4::aaaa:aaaa:aaaa:aaaa is known on leaf2. If leaf3->a05:fab:4::aaaa:aaaa:aaaa:aaaa selects leaf1 for ECMP, the packet arrives in on leaf1 which then does a Type2 lookup to the destination a05:fab:4::aaaa:aaaa:aaaa:aaaa. When leaf1 puts the packet on the wire back to leaf2,

it will rewrite the last part of the IPv6 address to a05:fab:4::aaaa:aaaa:aaaa:0 - causing traffic failure. See Junos bug PR1695877 for more information.

All BGP peerings with password get restarted in every config apply on SONiC (AOS-34086)

All BGP peerings with password get restarted in every config apply on SONiC. Any config apply on a SONiC device will cause all BGP peerings that use a BGP password to flap. It is noted that fabric links do not use BGP passwords.

Resolution

AOS renders a n `frr.conf` with bgp passwords as plaintext. In every config push done by AOS, the `frr-reload.py` command is used to gracefully apply the changes by comparing the incoming `frr.conf` to the `show running-config` of FRR. However, the output of FRR `show running-config` command emits a password form that is encrypted.
However, since `frr-reload` cannot understand that the plaintext form is equivalent to the encrypted version of the `neighbor X password Y` command, it proceeds to remove the encrypted form and re-apply the plaintext version. Removing the password and re-applying it causes the session to flap. This happens to every BGP peering using a password every time the `frr-reload.py` command is used.

Changing interface speed and adding same interface to an aggregated ethernet interface in the same commit may fail in Junos Evolved (AOS-40063)

If the member physical interfaces that are going to comprise an ae are initially at different speeds, naturally we have to change the speeds to the desired ae speed and then create the ae from the constituent interfaces.

If the changing of the speed and the creation of the ae is in the same commit, the commit may fail with "Interface aeX with child links of mixed speed but link-speed mixed is not configured". This has been observed in Junos Evolved.

Default Route Nexthop Programmed as Drop in SONiC (AOS-35085)

In SONiC versions up to 3.5.4 and 4.0.2, under rare timing conditions, the deletion and re-addition of a subinterface belonging to a non-default VRF may result in missing hardware routes to next hops behind that interface. This has been observed in a case where the default route towards an external router was missing from the hardware programming. Please refer to vendor bug SONIC-67559.

Unfortunately, it is relatively difficult to detect the occurrence of this bug, as the route is missing

from the hardware, but present in the routing daemon and the kernel of the device.

Resolution

Enterprise SONiC 3.5.5 and 4.0.3 will contain a fix for this bug.

Interface Status gRPC Streaming Telemetry (AOS-40646)

Due to unresolved Junos and Junos EVO 22.4R2.8 issues, interface status gRPC streaming telemetry may fail due to a race condition that happens if the data to report closely aligns with the thresholds. This will cause unexpected Apstra anomalies.

IPv6 Communication Is Not Established Between VM/Host on L2 VXLAN Use Case (AOS-38715)

IPv6 communication between vm/host on L2 vxlan use case is not established. The affected SONiC versions are 4.0.1 and 4.0.2.
SONiC 4.0.3 or 4.0.5 are not affected.

Juniper QFX10000 Devices Unable to Send Packets on Tagged Layer2 Interfaces (AOS-35096)

Juniper QFX10000 devices cannot send packets on tagged layer2 interfaces for external router connections.

Juniper QFX5220-128C Junos EVO Downgrade Failure (AOS-40892)

NOS upgrade through Apstra fails intermittently with "AssertionError: Job has not finished." This is due to an unresolved Junos EVO bug. The Junos EVO kernel may core dump when downgrading Junos EVO version on QFX5220-128C.

Junos BGP Graceful Restart Not Working for Non-default Routing Instances (AOS-35849)

Currently, for dual routing engine Junos devices, Apstra enables BGP graceful restart. Due to a current issue in Junos 22.2R2, graceful restart is not enabled for non-default routing instances.

JUNOS DHCP Relay services continue to function even after disabling the service (AOS-26195)

On Junos devices with the DHCP Relay service enabled, disabling it does not stop the service to function.

Junos Link-local Session Does Not Come Up After the Leaf Reboots (AOS-29127)

Due to a Junos issue, if a user creates a BGP link-local session over SVI and assigns it to a leaf to server port-channel, the session comes up, but if the leaf device is rebooted, the BGP session will not come up.

Loss of IPv6 traffic on the Juniper_EX4400-48T platform (AOS-38006)

Under certain circumstances, IPv6 traffic might not work on certain vxlan-enabled vlans of a Juniper_EX4400-48T device.

Apstra Config Rendering Changes

'vrf-table-label' Removed From Junos EVPN Configuration (AOS-40778)

The Junos EVPN vrf-table-label configuration is not needed for evpn-fabric. This has been removed from the Apstra Datacenter Reference Design.

Inter-VRF Routing Problem w/ Single Spine Path (AOS-38834)

Due to an issue with the Apstra EVPN reference design, problems with inter-vrf routing via an external router can occur if there is a single spine (either by design, failure, undeploy, or drain) and the route is originated on a non-border-leaf. The one spine will drop the route due to as-path loop.

Resolution

Apstra 4.2.0+ increases the number of times the spine/superspine AS can appear in the ASPATH from 1 -> 2 times to support inter-vrf routing between leafs through a single spine path.

Note that Arista EOS will not immediately learn these routes upon upgrade, a 'clear ip bgp * soft' may need to be executed manually by the user in order for the spines to retroactively learn the alternative routes.

Junos 'device-count' for lag is incorrectly counting ae interfaces (AOS-40448)

Junos 'device-count' configuration for defining the number of aggregated ethernet ports is incorrectly including layer3 port-channel subinterfaces in the total device count.

Resolution

Apstra 4.2.0 corrects the device interface count during configuration rendering to only include parent aggregated interfaces.

Junos EVO Leafs Flooding DHCP Messages (AOS-33697)

Due to a bug in Junos 22.2-EVO, DHCP discover messages are incorrectly flooded across EVPN fabric.

Resolution

Apstra 4.2.0 adds the 'no-dhcp-flood' configuration to L3 IRBs to avoid incorrect flooding of DHCP messages

---

SONiC FRRouting Configuration Moves allowas-in to Per Address Family Configuration (AOS-41298)

SONiC FRRouting configuration now assigns the allowas-in command underneath the appropriate evpn or IPv6 address family. Before this change, allowas-in was only effectively functional for the ipv4 unicast address-family. This resolves potential inter-vrf route leaking reachability issues through external connectivity points which were preventing re-learned routes between VRFS from being re-advertised into EVPN for other VTEPs.

Unexpected Policy Changes And Potential BGP Flap When Draining One Leaf In Leaf Pair (AOS-37948)

In Apstra, when the user sets one leaf in a leaf pair to drain mode, Apstra fabrics with Juniper Junos devices will deploy unexpected policy changes between the spines and the other leaf in the leaf pair. This may result in the network operating system resetting the BGP session between the

spines and the other leaf. Apstra fabrics with other vendor devices (SONiC, Cisco, Arista) are not affected by this issue.

Resolution

Upon upgrade to 4.2.0, BGP-AOS-Policy is no longer removed from BGP neighbor export configuration when another device is drained. The correction for this issue may also result in a BGP notification flap on existing BGP sessions if any spine-leaf or spine-superspine BGP Session is drained on a device. If spine1 is peering with leaf1, leaf2, leaf3, and leaf1 is drained, BGP policies will be corrected between spine1 & leaf2/leaf3 to re-insert BGP-AOS-Policy during upgrade. Modifying BGP export policy on Junos is an unavoidably disruptive operation, so these sessions may flap.

Known Apstra General Issues

[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"

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.

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
```

AOS device agent installation fails on Junos and Junos EVO device with hostname as IP address (AOS-47453)

If the Junos and Junos EVO devices do not have a name-server configuration, AOS device agent installation fails when a hostname is used instead of an IP address. The missing name-server configuration in the device hostname prevents the management IP address from being resolved.

Workaround

Here are the two workarounds. Either of them can be used to resolve the problem.
Option 1: Configure the name server on the device. This allows the device to resolve the hostname and use the correct management IP address.
Option 2: When configuring system agents in AOS, use IP addresses rather than hostname.

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.

Workaround

The user needs to manually unassign connectivity templates from each intended application endpoint.

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

Applying MTU Configlet Fails on NXOS Due to Rendering Order (AOS-40165)

If an Apstra user uses a configlet to attempt to modify the MTU on Cisco NXOS subinterfaces, due to the rendering order that Apstra applies the configuration, NXOS may return an "ERROR: MTU must be greater than all the sub interface mtus" error for a parent interface or "MTU of sub-interface greater than parent interface detected" error for the subinterface.

Workaround

This configlet workflow is not supported by Apstra. If users use this, they must configure their configlet to make the MTU changes in an order compatible with NXOS.

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.

Workaround

Edit the LDAP provider under Provider-specific Parameters, Advanced Config, set the Timeout(seconds) to 15 seconds or lower to prevent the provider timeout from crashing Authagent.

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 ZTP Duplicate Entries for Junos Devices (AOS-40023)

When monitoring Apstra ZTP device status in the Apstra UI under "ZTP Status" / "Devices", there may be duplicate entries for Junos devices. Apstra ZTP will try to ensure the physical management interface for the Junos device is used instead of any virtual management interface (e.g. "vme" interface). Junos may use the virtual interface when ZTP starts but cannot be added to the required "mgmt_junos" routing-instance. This is done as the first step in ZTP in order to ensure that the management IP address does not change during the rest of the steps involved in ZTP (especially those involving connectivity to Apstra). Enabling a different management interface will cause the DHCP server to give out a new lease. Also, the vendor class identifier for the new management interface is cleared so that the DHCP server does not give out vendor-specific options to this interface, which may re-trigger a new ZTP session while the current session is active. This is expecetd behavior.

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.

Workaround

Manually reboot the device to complete the Junos upgrade, then repeat ZTP.

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.

Workaround

The user can workaround this issue by not editing ztp.json using the Apstra ZTP UI configurator; only use the Apstra ZTP UI code editor or directly edit the /containers_data/tftp/ztp.json file in the Apstra ZTP VM CLI, removing the invalid variables and only assigning the necessary variables.

```
"system-agent-params": {
    "agent_type": "onbox",
    "job_on_create": "install"
}
```

Refer to the Apstra ZTP documentation ...

https://www.juniper.net/documentation/us/en/software/apstra4.2/apstra-user-guide/topics/task/apstra-ztp-configure.html

---

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.

Workaround

The user can workaround this issue by not editing ztp.json using the Apstra ZTP UI configurator; only use the Apstra ZTP UI code editor or directly edit the /containers_data/tftp/ztp.json file in the Apstra ZTP VM CLI, removing the invalid variables and only assigning the necessary variables.

```
"system-agent-params": {
    "agent_type": "onbox",
    "job_on_create": "install"
}
```

Refer to the Apstra ZTP documentation ...

https://www.juniper.net/documentation/us/en/software/apstra4.2/apstra-user-guide/topics/task/apstra-ztp-configure.html

---

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.

Workaround

The user can workaround this issue by not editing ztp.json using the Apstra ZTP UI configurator; only use the Apstra ZTP UI code editor or directly edit the /containers_data/tftp/ztp.json file in the Apstra ZTP VM CLI, removing the invalid variables and only assigning the necessary `"system-agent-params"` variables.

Onbox:

```
"system-agent-params": {
    "agent_type": "onbox",
    "job_on_create": "install"
}
```

Offbox:

```
"system-agent-params": {
    "platform": "junos",
    "agent_type": "offbox",
    "job_on_create": "install"
}
```

Refer to the Apstra ZTP documentation ...

https://www.juniper.net/documentation/us/en/software/apstra4.2/apstra-user-guide/topics/task/apstra-ztp-configure.html

---

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.

Workaround

The user can workaround this issue by not editing ztp.json using the Apstra ZTP UI configurator; only use the Apstra ZTP UI code editor or directly edit the /containers_data/tftp/ztp.json file in the Apstra ZTP VM CLI, removing the invalid variables and only assigning the necessary variables.

```
"system-agent-params": {
    "agent_type": "onbox",
    "job_on_create": "install"
}
```

Refer to the Apstra ZTP documentation ...

https://www.juniper.net/documentation/us/en/software/apstra4.2/apstra-user-guide/topics/task/apstra-ztp-configure.html

---

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.

Workaround

The user must use the "username" and "password" options with proper credentials when updating a system agent with the Apstra-CLI "system-agents update" command.

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.

Workaround

The user needs to either restart the Apstra service on the device or initiate a config change for the device from Apstra.

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
```

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.

Workaround

Perform a Blueprint Revert and attempt the Blueprint commit again.

---

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.

Workaround

Call cabling-map Patch API with the right payload information (if_name must not be empty string) to fix issue.

Cannot Access connector-types API (AOS-40292)

Users with Apstra blueprint read permission cannot access connector-types API.

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.

Workaround

User can configure system based configlet and render the config under unit 0 for an specific 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.

Workaround

The user can edit the leaf label using the rack builder.

Commit Check Can Fail While Rendering a Configuration, if Staging Blueprint Is Being Edited Simultaneously (AOS-39456)

If staging blueprint changes are being carried out and a commit check operation is triggered simultaneously while those changes haven't been concluded, the configuration rendering mechanism inside the commit check operation may fail.

Workaround

Simply trigger again the commit check for a device whose commit check failed with an error similar to "Commit check for (serial number) rejected: Failed to render (serial number): Failed to render (serial number): Rendering failed..."

Configlet Configured VRF Removed From Device When Apstra Routing Zone Deleted (AOS-39192)

If the Apstra user is managing a Cisco NXOS device and they remove an Routing Zone (VRF) from Apstra and the user still has the VRF configured via an Apstra Configlet, the VRF will be removed from the device.

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

Configured GRPC Port Not Removed on System Agent Uninstall (AOS-40260)

Apstra does not have a state machine to preserve the state of the device before which Apstra configured GRPC on the device during system agent install. Due to this, Apstra may not remove the GRPC port during system agent uninstall.

Workaround

The user may need to manually remove the GRPC port after the Apstra system agent uninstall.

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 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.

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.

Device System Health IBA Probe Sustained High Disk Utilization for Older Arista Devices (AOS-39788)

Due to the increased size of the Apsta on-box device system agent, users may experience unexpected sustained high disk utilization errors from the Device System Health IBA probe for older Arista devices such as the Arista 7050QX-3.

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
```

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 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.

Workaround

The user will need to remove any duplicates.

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

---

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.

Workaround

The user can restore the proper behavior of the IBA probe by disabling and enabling the probe.

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.

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.

Workaround

Either remove the import/export route target, or ensure at least one import and export target are both configured on the virtual network.

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.

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

---

Incorrect Incremental Device Configuration When Replacing Device Profile With a New Line Card (AOS-42128)

When the user replaces an Interface Map with an updated modular chassis Device Profile with removed line card configuration, Apstra renders the correct, complete configuration. However, the incremental device configuration may be incorrect, leaving the interface configuration for ports on the removed line card.

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).

Workaround

The user can manually clone the device profile and correct the interface names in the new device profile. Contact Juniper Support for assistance.

---

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 counter telemetry service in the EX4400-48T (working as leaf) device fails with timeout after device reboots (AOS-40917)

After device reboots, device would take longer for stabilizing services under highly loaded environment. While it's under stabilizing period, telemetry service for interface counter in the device can fail from timeout (default: 2 minutes). In the steady state, telemetry service for interface counter should not trigger timeouts.

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.

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.

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.

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.

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.

Workaround

Prior to starting the Apstra 4.1.x upgrade, the user must remove all probes with the `node_to_node_if_counter` processor.

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)

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.

Workaround

The user will need to correct the IP or credentials if the Virtual Infra manager is disconnected.

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.

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.

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.

Workaround

Fix duplicate VNI issue by assigning unique static VNI value, which shouldn't come from dynamic VNI pool where virtual network uses, to Security Zone.

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.

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.

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.

Workaround

The user can kill the Apstra BuilderAgent process to release the memory. It will automatically restart.

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

---

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

---

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.

Workaround

Before upgrading to Apstra 4.2:

```
1. Identify route-targets with leading zeroes in all blueprints (Edit Routing
Zone)
2. Update affected Route Target Policies by removing leading zeroes (e.g.,
change 0555:0555 to 555:555).
3. Review and commit the changes in all blueprint.
4. Proceed with the VM-to-VM upgrade.
```

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 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 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 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 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.

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

User-defined extra import or export host routes without CIDR prefixlength not included in configuration (AOS-47151)

User-defined host routes within extra import or export prefix-list entries in a routing policy were not being included in device configuration if they did not have the /32 CIDR prefix length. For example, '3.3.3.3 le_mask=None ge_mask=None' was not rendered, while '3.3.3.3/32 le_mask=None ge_mask=None' was being rendered.

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.

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.

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
```

Known 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

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.

Apstra ZTP Fails for Juniper QFX5700 (AOS-40324)

Due to an outstanding issue with Junos 22.4R2.10-EVO, during the ZTP process, the device will maintain some stale state in the alternative boot partition, which may cause ZTP states in the device to be stale, causing the Apstra ZTP process to fail.

Changing VTEP Address as a Day-2 Operation in SONiC May Fail (AOS-34891)

Changing the IP address of the VTEP of a SONiC device as part of a day-2 operation, may fail and the device may be left in a failed deployment state. The danger is more acute in cases of Blueprints with a large number of VRFs and VNs.

If the IP address of the VTEP is being set for the first time, e.g. when the blueprint is deployed for the first time, this release note does not apply. Only cases where the VTEP has already been set to an initial IP address and VNIs have been created using it.

Workaround

It is suggested to apply full config after attempting to alter the VTEP IP address and getting a failure.

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.

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.

EVPN Tunnel Delay After Reboot Due to Apstra "graceful-restart" Option (AOS-42823)

In Apstra 4.2.0, "graceful-restart" was added as a default fabric setting in the Juniper BGP/EVPN reference design. Due to an outstanding bug in versions of Junos, after the device is rebooted, it may take up to 60-70 seconds for EVPN type-5 tunnels to get programmed in the device PFE blackholing traffic from LACP dual-connected generic systems.

Workaround

The user can workaround this issue by applying a Junos set interface Configlet to configure "lacp aggregate-wait-time" on generic system facing interfaces ...

```
aggregated-ether-options lacp aggregate-wait-time 90
```

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

FRR Does Not Support maximum-prefix on EVPN Sessions (AOS-38611)

In platforms using FRR (at present SONiC), there is no setting available to set the maximum number of prefixes for the l2vpn evpn afi/safi. So, even if the limit exists in the blueprint, it is not possible to enforce it on SONiC devices.

---

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 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.

Workaround

If encountered, please contact ACX platform Juniper Support.

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.

Workaround

Junos EVO users can workaround this issue by changing the device hostname to a hostname containing a dash ("-") character.

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')`.

Workaround

The user can attempt to reboot the device to resolve the error. Please contact platform Juniper Support.

Junos Evolved Device Sees No LLDP Neighbours (AOS-39435)

Under certain circumstances, a Junos Evolved device may not see its LLDP neighbours, even though its neighbours are seeing it normally. There is no other impact, but the AOS telemetry expectations will pick up the missing neighbours and raise cabling anomalies.

Workaround

The command `restart layer2-control` can be used to restart the l2cpd process, which will correct the problem. However, caution is in order when issuing that command, as it restarts other layer2 protocols handled by l2cpd, such as STP.

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.

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.

Workaround

After removing the device from a Apstra blueprint, the user can restart the l2ald daemon with the Junos `restart l2-learning` command.

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.

Workaround

Upgrade QFX10002-60C to Junos 21.2R3-S5. Contact QFX Platform Juniper Support.

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 Hostcfgd may not respond to CONFIG_DB key events (AOS-32963)

The hostcfgd daemon in SONiC Cyrus up to 4.0.2 may not respond to CONFIG_DB key changes. For example, issuing the command "config vrf del mgmt" may not delete the mgmt vrf. This may cause Apstra agent jobs (install, uninstall, NOS upgrade) to fail unexpectedly.

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.

---

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.

Workaround

The user will need to ensure not to include the Junos "multi-chassis mc-lag consistency-check"

configuration in the device configuration before the device system agent installation so it will not be present in the Apstra device pristine configuration.