EVPN-VXLAN Data Center sFlow with Juniper Apstra

This document serves as a detailed guide for configuring sFlow telemetry on Junos OS devices in an Apstra-managed data center fabric. It explains the objectives of integrating sFlow with the Apstra Flow application, outlines the necessary configuration procedures, and provides CLI command examples to support implementation. This document is intended for network engineers and administrators who are deploying or managing Apstra-based data center fabrics. The users require visibility into traffic flows for performance monitoring, capacity planning, and anomaly detection using Apstra Flow application.

Table of Contents

Solution Benefits

This document describes the benefits of using sFlow for monitoring networks and demonstrates how to apply sFlow technology to existing Juniper Validated Designs (JVDs), including the **3-Stage Data Center Design with Juniper Apstra** (JVD). While there are many applications that can collect and visualize data from sFlow capable devices, this document highlights the use of Juniper Apstra sFlow to monitor traffic on a 3-stage fabric that was deployed with Juniper Apstra.

The solution discussed in this document can also be extended to other Juniper Data Center designs such as **5-Stage EVPN-VXLAN Data Center** and other AI/ML Juniper validated designs.

With network flow monitoring, network engineers and administrators can troubleshoot application issues across a DC fabric that supports distributed, cloud-native, virtualized, and containerized workloads.

sFlow technology

sFlow is a packet-sampling–based telemetry technology supported on most Juniper devices. It provides real-time visibility into network traffic by exporting sampled packets and interface statistics to a centralized collector using UDP. Juniper's implementation of sFlow complies with RFC 3176. Hardware application-specific integrated circuits (ASICs) perform the sampling, which simplifies the monitoring process and increases accuracy.

Using sFlow technology offers several key benefits for network operators, especially in large-scale, high-performance environments. Here are some of the main advantages:

1. **Network Visibility:** sFlow provides real-time, packet-level visibility across the entire network without overwhelming the device CPU or memory.
2. **Sampling Flexibility:** The sampling rate on sFlow can be configured as needed.
3. **Traffic Analysis:** sFlow enables continuous monitoring of traffic flows, interface statistics, and application usage.
4. **Proactive Capacity planning:** sFlow helps network operators to forecast bandwidth needs by analyzing the traffic trends.
5. **Client and Server Flow visibility**: sFlow provides detailed insights into client server interaction, offering critical information about ports, protocols, and IP addresses. This visibility helps detect unauthorized access and identifies unexpected traffic flows.

Juniper QFX Series Switches support sFlow version 5, the most widely adopted and standardized version of the protocol as defined in RFC 3176. sFlow v5 is compatible with most open-source and commercial collectors such as ElastiFlow, Grafana (via exporters), and Juniper Apstra.

Apstra Flow Benefits

Apstra Flow delivers deep, real-time visibility into data center traffic by leveraging sFlow telemetry across the fabric. It enables proactive monitoring by analyzing flow paths, application usages, and hotspots in the network. Apstra Flow visualizes traffic flows, identifies anomalies, and correlates network behavior with intent-based policies. Apstra Flow empowers network operators to maintain optimal performance, reduce mean time to resolution (MTTR), and ensure policy compliance across multi-vendor environments—all from a single, unified interface.

Key features of Apstra Flow include:

- **Integrated with Apstra Analytics Dashboard:** Linking Apstra Flow with the Apstra Telemetry dashboard provides users access to flow data alongside real-time telemetry which is useful information when you are troubleshooting.
- **Intent-Based Flow Visualization:** Aligns flow data with Apstra's intent-based policies, allowing users to validate traffic paths and ensure compliance with the design intent.

- **Enhanced Operational Efficiency:** Offers centralized visibility and analytics, streamlining network operations and supporting proactive decision-making.
- **Support for Multi-vendor and Multi-flow Protocols:** Apstra Flow collector supports sFlow, NetFlow v1, v5, v6, v7, v9, IPFIX, and IFA information elements (IEs). These IEs contain attribute values that are related to the observed network traffic. The Apstra Flow collector supports IEs from many vendors and multiple networking technologies.

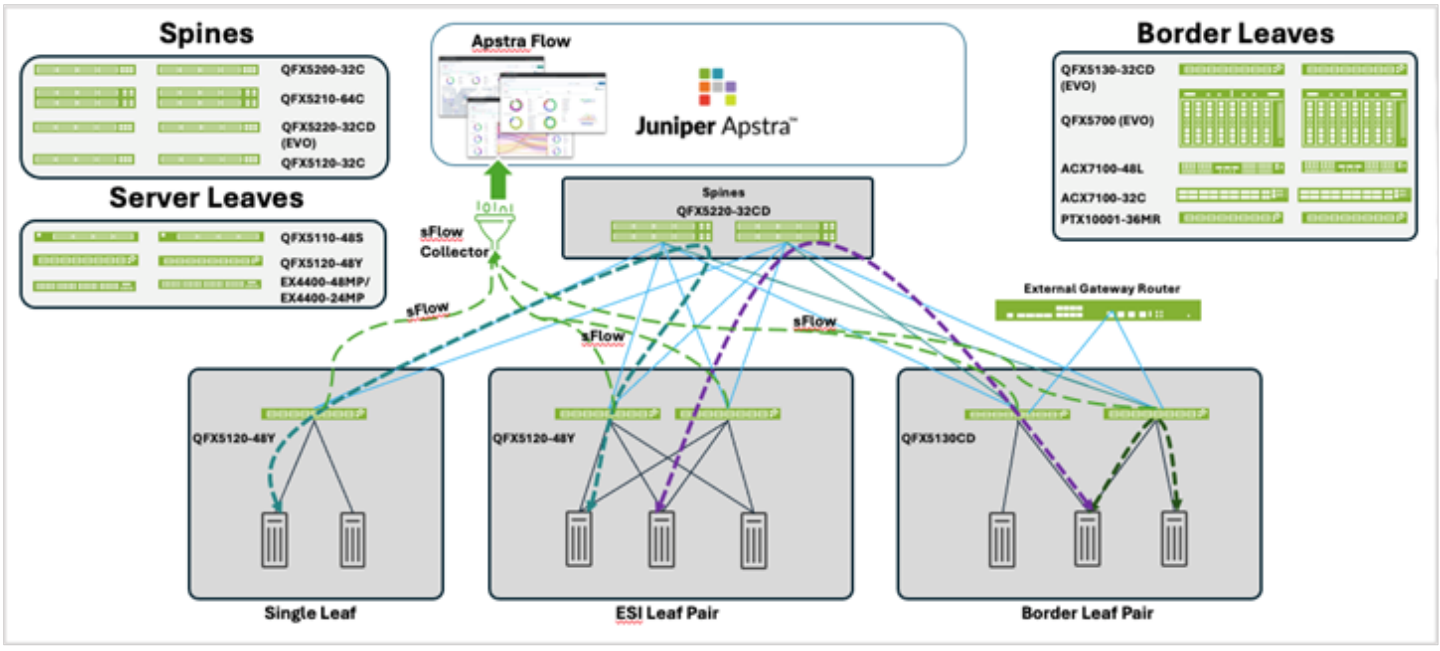
This document outlines the configuration of sFlow on Juniper devices using Juniper Apstra and details the deployment of Juniper Apstra Flow for telemetry and monitoring.

Use Case and Reference Architecture

This document demonstrates the use of sFlow in the **3-Stage Data Center Design with Juniper Apstra** (JVD). The reference architecture shown below in Figure 1: 3-stage Reference design with Juniper Apstra Flow uses Juniper switches to form the ERB architecture managed by Apstra. For purposes of this document, the sFlows are monitored using the Apstra Flow application.

Note: Apstra Flow is a feature in the Apstra Premium tier licensing plan. This feature is available only to customers who are already an Apstra premium customer. For Apstra licensing information, refer to the **Juniper Licensing User Guide**. Contact your Juniper account representative for more information.

Figure 1: 3-stage Reference design with Juniper Apstra Flow



Juniper Hardware and Software Components

For this solution, the Juniper products and software versions are listed below. The listed architecture represents the recommended base representation for the validated solution. As part of a complete solution suite, we routinely swap hardware devices with other models during iterative use case testing. Each platform also goes through the same tests for each specified version of Junos OS.

Juniper Hardware Components

The following switches have been tested and validated to work with the 3-Stage Fabric with Juniper Apstra JVD in the following roles:

Table 1: Validated Devices and Positioning

Validated Devices and Positioning			
Solution	**Server Leaf Switches**	**Border Leaf Switches**	**Spine**
3-stage EVPN-VXLAN (ERB)	QFX5120-48Y-8C*	QFX5130-32CD*	QFX5220-32CD*
	QFX5110-48S	QFX5700	QFX5120-32C
	—	ACX7100-48L	—
	—	ACX7100-32C	—
	—	PTX10001-36MR	—

* marked are baseline devices

Table 2: Juniper Qualified Software

Juniper Software	
Juniper Products	**Software or Image version**
Junos OS Evolved & Junos OS image	**Junos OS and Junos OS Evolved 24.4R2 Junos OS and Junos OS Evolved 24.2R2 Junos OS and Junos OS Evolved 23.4R2-S5**
Juniper Apstra	**6.0.0-189**
Juniper Apstra Flow	**6.0.0**

Configuration Walkthrough

For the purposes of this use case, the baseline Juniper devices are listed in Table 3: 3-Stage Data Center Baseline Devices. This document focuses on the configuration of sFlow on Juniper devices with the Apstra Flow application. Apstra Flow can be extended to other vendor devices that support sFlow technology to visualize network traffic flows.

Table 3: 3-Stage Data Center Baseline Devices

Juniper Devices	Role
QFX5220-32CD	Spine
QFX5120-48Y	Server Leaf
QFX5130-32CD	Border Leaf

Prerequisites

Use Apstra to deploy the 3-stage EVPN-VXLAN data center following the guidelines outlined in the **3-Stage Data Center Design with Juniper Apstra** JVD. For the purposes of this use case, the following devices were configured as follows:

- Three QFX5120-48Y switches (Junos OS) as server leaf
- Two QFX5130-32CD switches (Junos OS Evolved) as border leaf
- Two QFX5220-32CD switches (Junos OS Evolved) as Spine

sFlow technology on Juniper Switches

Juniper QFX Series Switches implement sFlow using a distributed architecture that is designed for scalable and efficient traffic monitoring. The sFlow system comprises two primary components:

1. Embedded sFlow Agent: Located within the switch. This agent manages the sampling process and prepares data for export.
2. External sFlow Collector: A remote system that receives and analyzes the sampled data exported by the switch.

When you enable sFlow, the embedded agent begins sampling packets and collecting interface statistics. Each Packet Forwarding Engine (PFE) on the switch includes dedicated subagents that perform the actual sampling. These subagents forward the sampled packets and statistics to the main sFlow agent.

The sFlow agent aggregates this data and formats it into UDP datagrams, which are then transmitted to the configured external sFlow collectors. These datagrams contain enriched flow information, including packet headers, interface details, and traffic metadata, enabling comprehensive network visibility and analysis. For more information about platform-specific sFlow behavior refer to the notes for each platform.

Note: Up to four collectors can be configured on Juniper switches.

Juniper QFX Series Switches support sFlow version 5, the most widely adopted and standardized version of the protocol as defined in RFC 3176. sFlow v5 is compatible with most open-source and commercial collectors such as ElastiFlow, Grafana (via exporters), and Juniper Apstra.

Configuring sFlow on Juniper Devices

For the purposes of this document, sFlow was configured on Junos OS and Junos OS Evolved devices using Apstra configlets. Juniper Apstra provides a standard sFlow configlet, that can be customized to align with the specific requirements of the devices deployed within the fabric.

Note: Export of sFlow data using management instance is not supported in Junos OS Evolved Release 23.4R2-S5.

A static route must be configured on Junos OS switches since sFlow export uses management instances.

Configuration of sFlow on Juniper Switches

To configure sFlow, the revenue port (or WAN port) on the switches is used to connect to the sFlow collector as shown in Test Topology. The collector is directly connected to the fabric on one of the leaf switches, and the default Apstra underlay policy will advertise that route into the fabric, thus making it reachable from every fabric switch.

The configuration also includes setting the sFlow agent ID (usually the collector's management IP), defining the collector IP and UDP port (for example, 6343), and specifying polling and sampling intervals. Interfaces intended for monitoring must

be explicitly included. A property set can be defined to parameterize the collector IP. The source IP in the configuration below provides the collector with the device's management IP to indicate the source of the sflow record from the device.

SNMP needs to be configured so that Apstra Flow can render the interface names, refer section Flow Enrichment for more details.

Note: The polling interval and sampling rate should be carefully configured based on the specific monitoring requirements and the volume of traffic in the network.

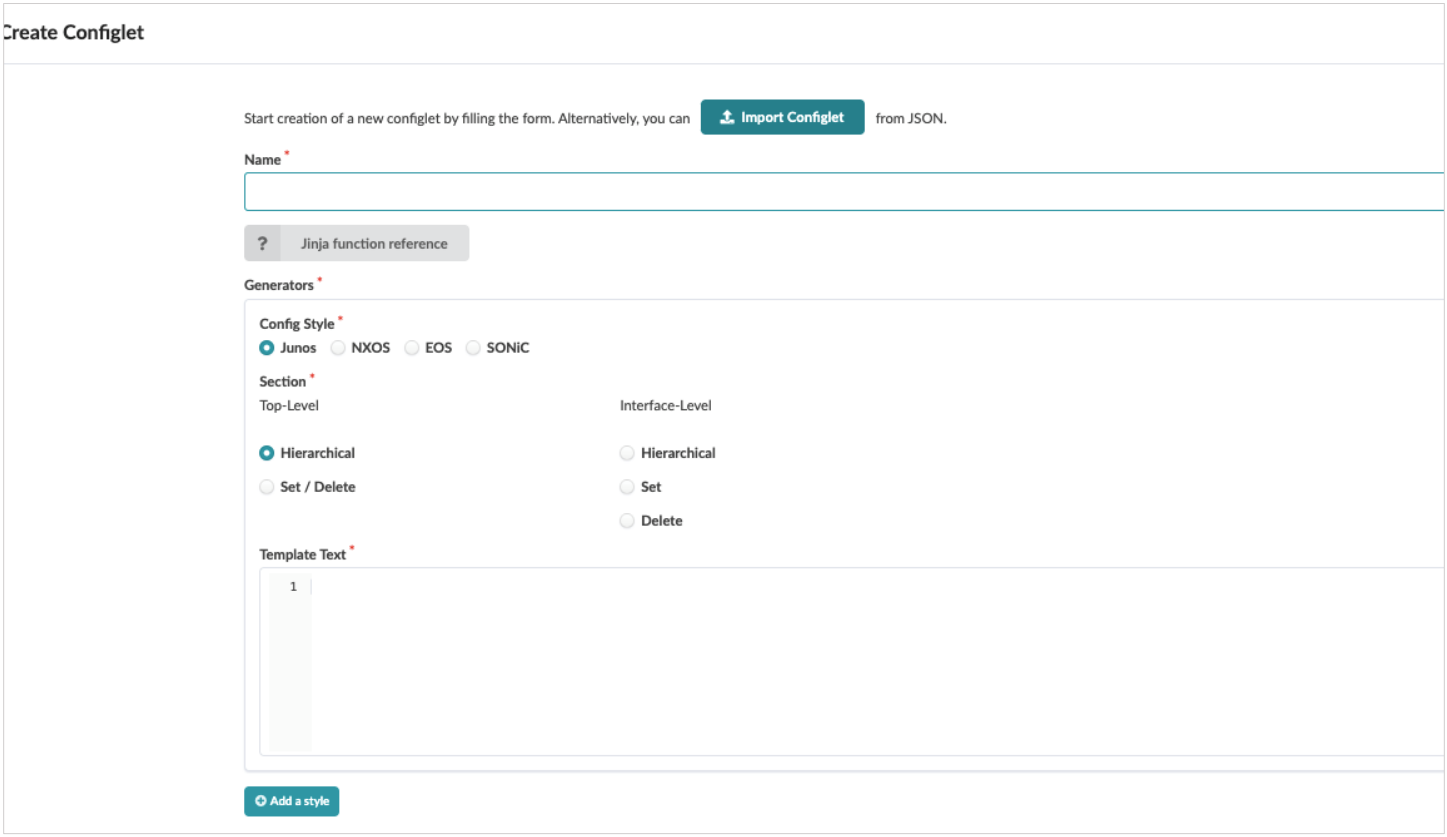
For the purposes of this lab, a separate revenue/WAN port was used to send sFlow traffic toward the collector.

```
groups {
    global {
       snmp {
          routing-instance-access;
          community public {
             routing-instance mgmt_junos;
          }
       }
    }
}
protocols {
    sflow {
        polling-interval 10;
        sample-rate {
            ingress 1024;
            egress 1024;
        }
        source-ip 10.48.9.123;
        collector 10.219.1.2 {
            udp-port 6343;
        }
        interfaces et-0/0/0;
        interfaces et-0/0/1;
        interfaces et-0/2/0:2;
    }
}
```

Configlets can be created using Apstra by logging into Apstra UI. Navigate to **Design > Configlet** and then click create configlet. Configlets can also be imported as shown below in Figure 2: Import Configlet. For more information about creating configlets refer to the **Apstra guide**.

Note: Configlets should be thoroughly tested and validated in a non-production environment before being applied to a live data center network. Since Apstra does not verify the syntax or correctness of configlets, no warnings or errors will be generated during commit—even if issues exist.

Figure 2: Import Configlet



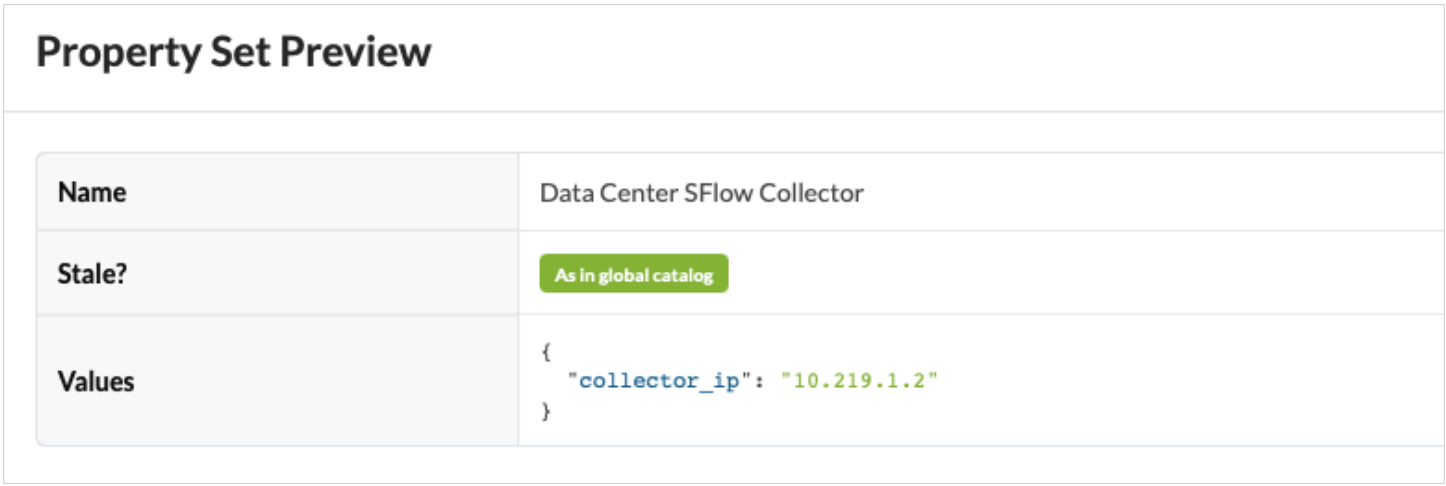
Below is configlet snippet for Junos OS switches. Note that the collector_ip can be configured as a parameter with **Property Set**.

```
groups {
    global {
       snmp {
          routing-instance-access;
          community public {
             routing-instance mgmt_junos;
          }
       }
    }
}
protocols {
    sflow {
        polling-interval 10;
        sample-rate {
            ingress 1024;
            egress 1024;
        }
    {% if management_ip is defined and management_ip %}
        source-ip {{management_ip}};
    {% endif %}
        collector {{collector_ip}} {
            udp-port 6343;
        }
    {% for interface, settings in portSetting.items() %}
        {% if settings['state'] == 'active' %}
        interfaces {{ interface }};
```

```
          {% endif %}
      {% endfor %}
      }
  }
```

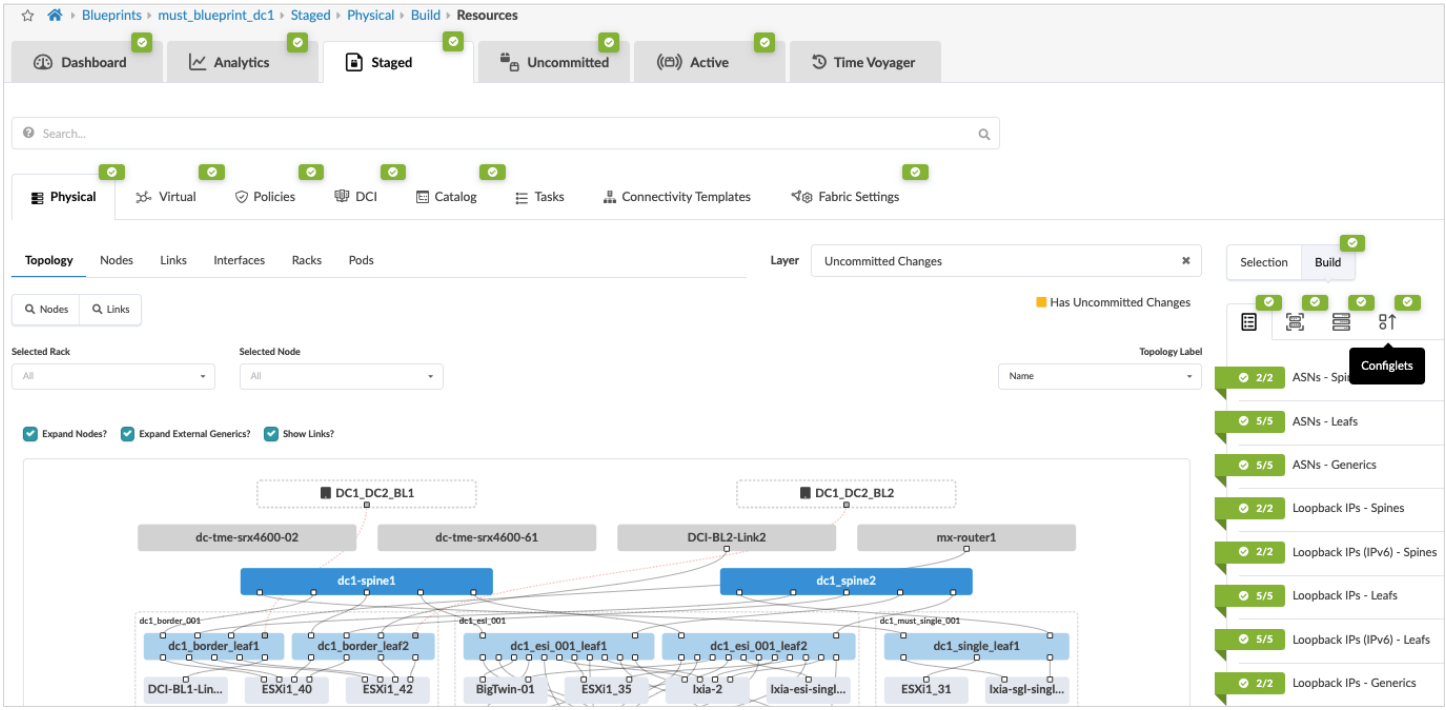
To add Property Sets in Apstra, navigate to **Design > Property Set**. Create a property set for the collector IP address as below. Ensure the property set is imported into the Blueprint by navigating to **Blueprints** > ***<blueprint-name>*** > **Staged** > **Catalog** then click **Import Property Set**.

Figure 3: Property set for collector IP

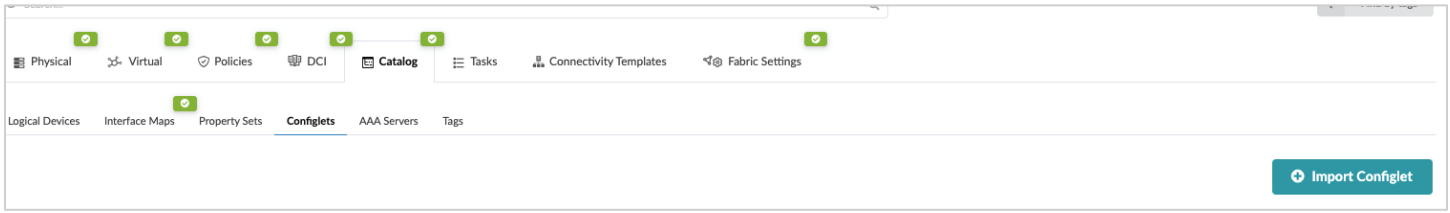


To configure the configlet in the 3-stage Data Center Blueprint, log in to Apstra. Navigate to **Blueprints** > ***<blueprint-name>*** > **Staged** > **Physical** then click configlet as shown below.

Figure 4: Adding sFlow configlet to Apstra

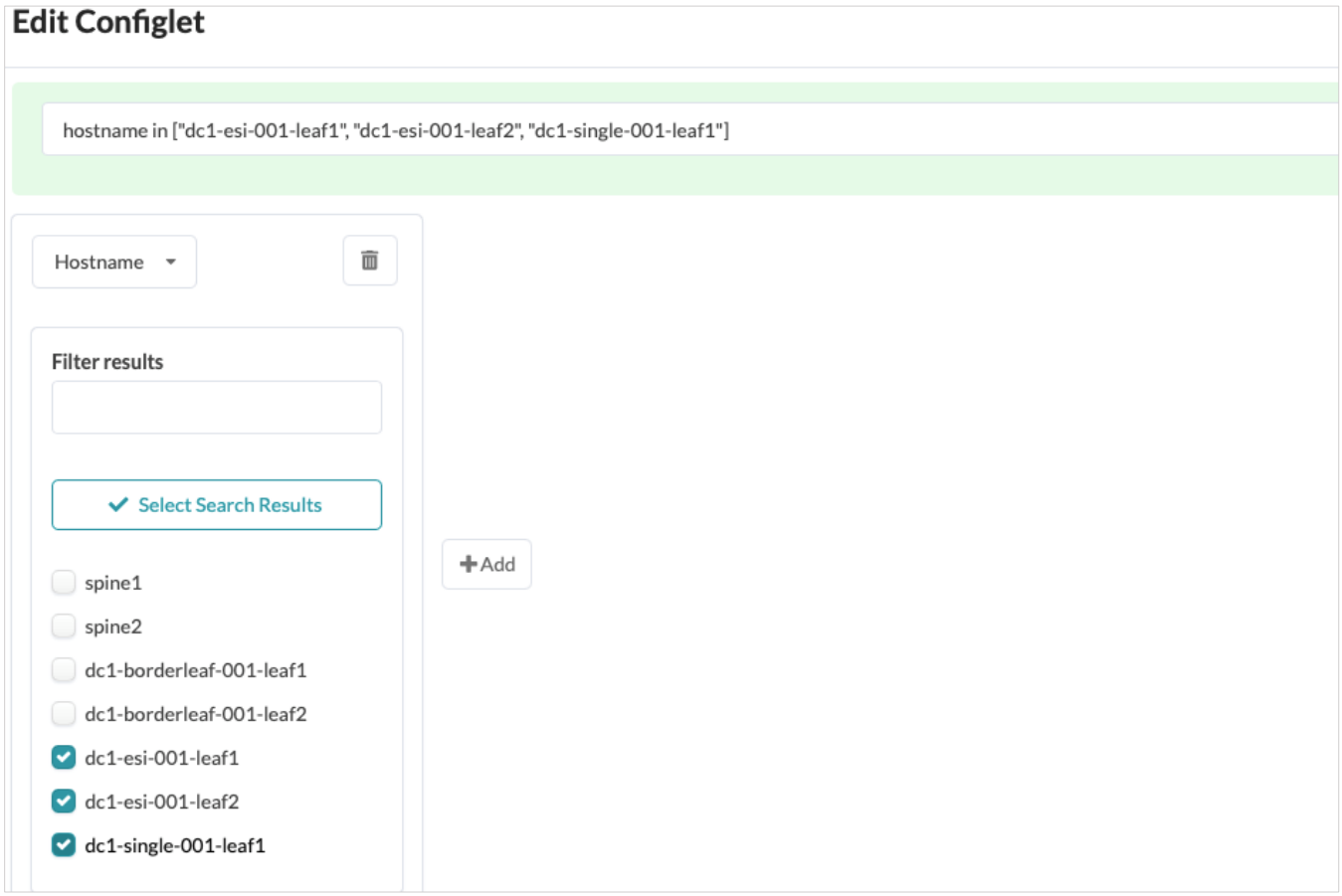


On the next screen, add the configlet as shown below. Alternatively, configlets can also be imported from **Blueprints** > ***<blueprint-name>*** > **Staged** > **Catalog.**



After importing the configlet into Apstra, assign it to the switches by selecting the **Hostname** option to filter devices and then selecting the non-EVO Junos OS switches as shown below in Figure 5: Assigning configlet to non-EVO leaf switches.

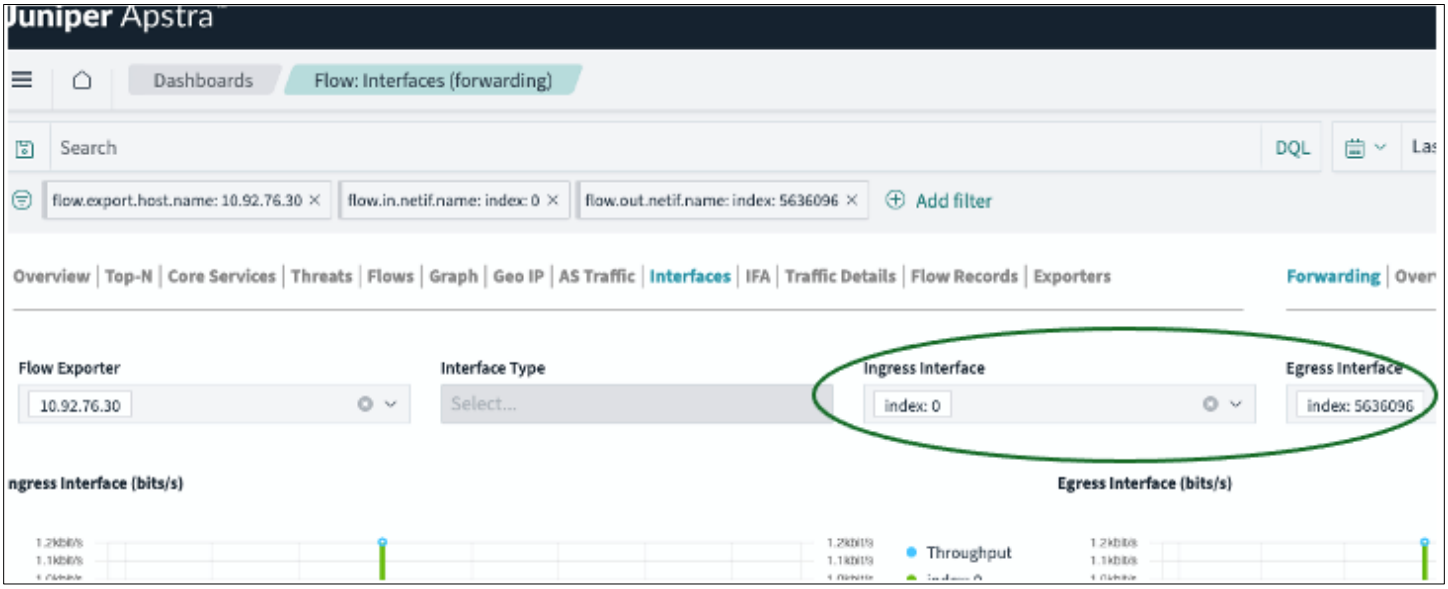
Figure 5: Assigning configlet to non-EVO leaf switches



Flow Enrichment

To display enriched interface information in the Apstra Flow Dashboard, SNMP will also need to be configured to identify the interface name rather than interface index ID as shown in Figure 6: Apstra Flow Dashboard showing Flows with Interface Index ID. An SNMP community string is required to be configured on Juniper switches (for both EVO and non-EVO switches). For more information about configuring the device and the Apstra flow collector, refer to the **Apstra Flow user guide** for steps on configuring SNMP. A standard configlet is also available in Apstra for configuring sFlow on the switches.

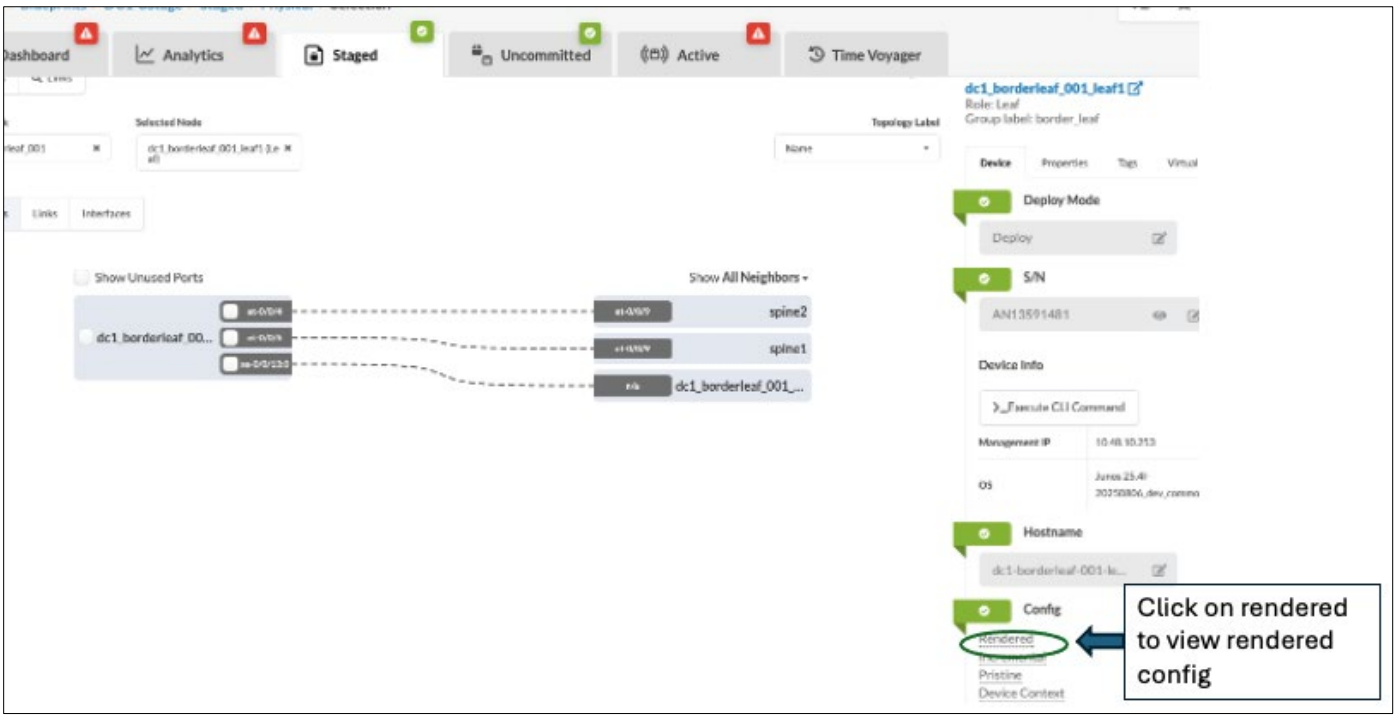
Figure 6: Apstra Flow Dashboard showing Flows with Interface Index ID



On the Apstra Flow collector, the SNMP community should match the SNMP community that's configured on the switches.

Once all the sFlow configlet is applied, check the rendered configuration by navigating in Apstra to **Blueprints** > ***<blueprint-name>*** > **Staged** > **Physical** and selecting the Topology and clicking on switches as shown in Figure 7: Viewing a Rendered Configuration.

Figure 7: Viewing a Rendered Configuration



If the sFlow configuration is rendered correctly for each device in the topology, navigate to **Blueprints** > ***<blueprint-name>*** > **Uncommitted** and commit the configuration in Apstra.

Apstra Flow Deployment

For the purposes of this document, Apstra Flow version 6.0.0 is deployed following the step-by-step instructions in the **Apstra Flow User Guide** for deploying Apstra Flow and adding a collector into Apstra. A single node deployment was set up.

> Note: To determine the appropriate Virtual Machine (VM) size for Apstra Flow, refer to the user guide which outlines scaling recommendations based on the number of devices to be managed. Refer to the **Apstra sizing guide instructions**.

Apstra Flow: Viewing Flow Dashboards

Once the sFlow configuration is committed, the device begins exporting flow data to the Apstra Flow collector, which decodes and visualizes the traffic in the Apstra Flow dashboards.

> Note: While Apstra Flow provides insights into traffic behavior and flow analytics based on sampled sFlow data. It does not deliver precise bandwidth utilization metrics. For accurate interface-level performance data, use Apstra Flow together with the Apstra Telemetry dashboard. This combined approach ensures both deep flow-level visibility with reliable real-time utilization metrics and supports more informed operational decisions and troubleshooting.

Apstra Flow uses the browser date and time to display flows on the UI. The default setting can be viewed by navigating to left-hand pane of Apstra Flow UI. Click the menu (three horizontal lines) and scroll to **Management > Dashboards Management > Advanced Setting**. In case of the Apstra Flow server that was set up using VMware vSphere, NTP was set up to synchronize the time on the server and on Juniper Switches under `[edit system ntp].` Refer to the Junos OS **NTP** documentation for more information.

Integrate Apstra Flow Data with Apstra Telemetry

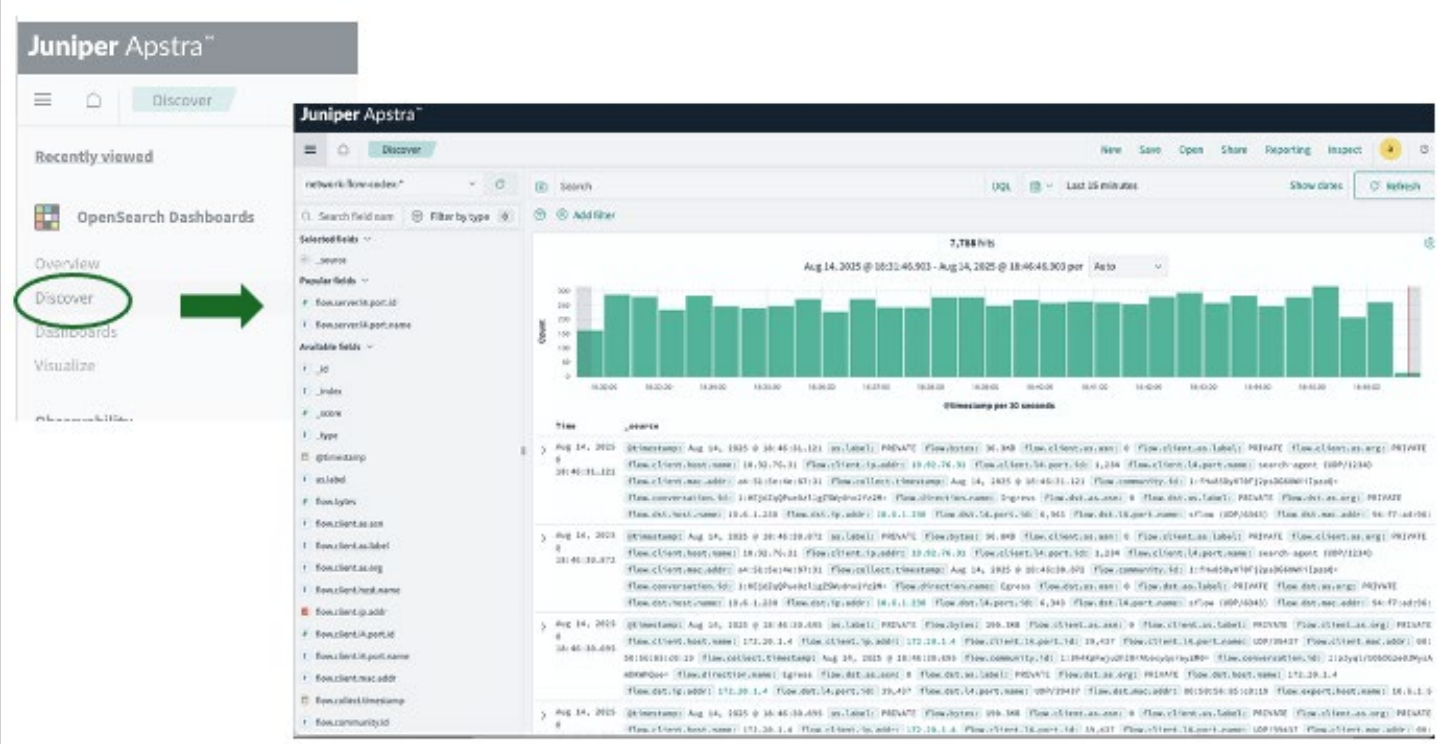
Flow data can be linked with Apstra Analytics. To quickly access the flow data dashboard Apstra telemetry analytics, refer to these **steps**. Quick access to the Flow Dashboard provides access to data during troubleshooting and analysis of flows.

> Note: To achieve multi-tenancy in Apstra Flow 5.1.0, we recommend deploying multiple Apstra Flow instances (collectors and UI) and exporting the flows from each data center or Apstra blueprint switches to dedicated Apstra Flow instances. This approach ensures data isolation and tenant-specific visibility. Contact your Juniper account representative for more information.

Apstra Flow: OpenSearch Discover

After sFlow is configured on the devices, log in to Apstra Flow and click the 'Discover' application from the OpenSearch Dashboard. This feature allows users to view and analyze the flow records fields and apply filters to search using certain flow attributes. This can be used to verify that flow data is reaching Apstra Flow and to explore the fields on a flow record for set filters.

Figure 8 : Apstra Flow - OpenSearch Dashboard Discover to view and analyze flow records



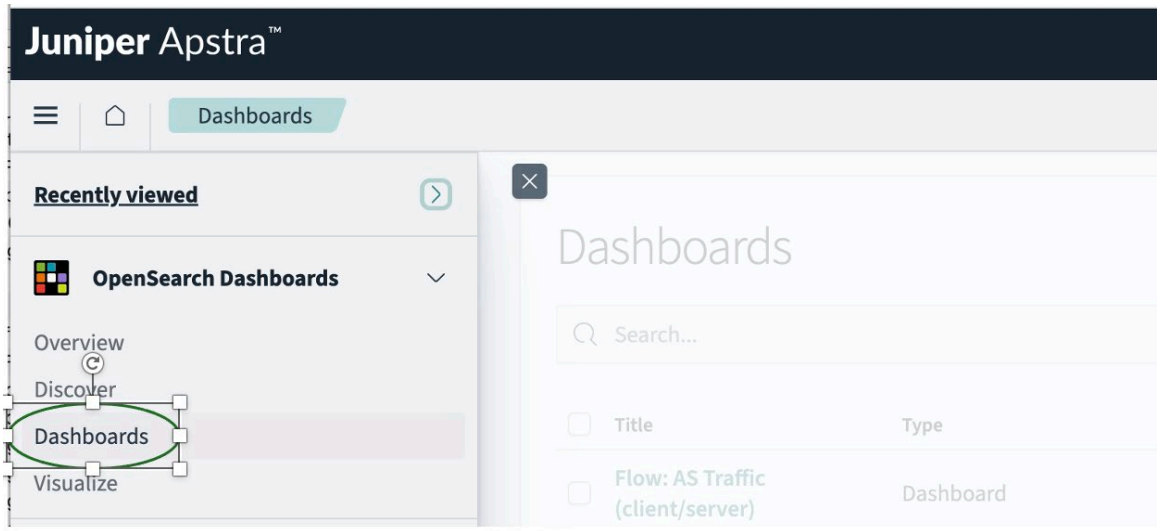
Apstra Flow Dashboards

Once the Apstra sFlow collector receives sFlow data, the information can be visualized on Apstra Flow using a wide variety of standard Dashboards. The **Apstra guide** covers information about various dashboards. This document touches upon some of the key dashboards that users can use to validate the sFlow setup and to visualize flow examples that illustrate the dashboards.

Flow Exporter

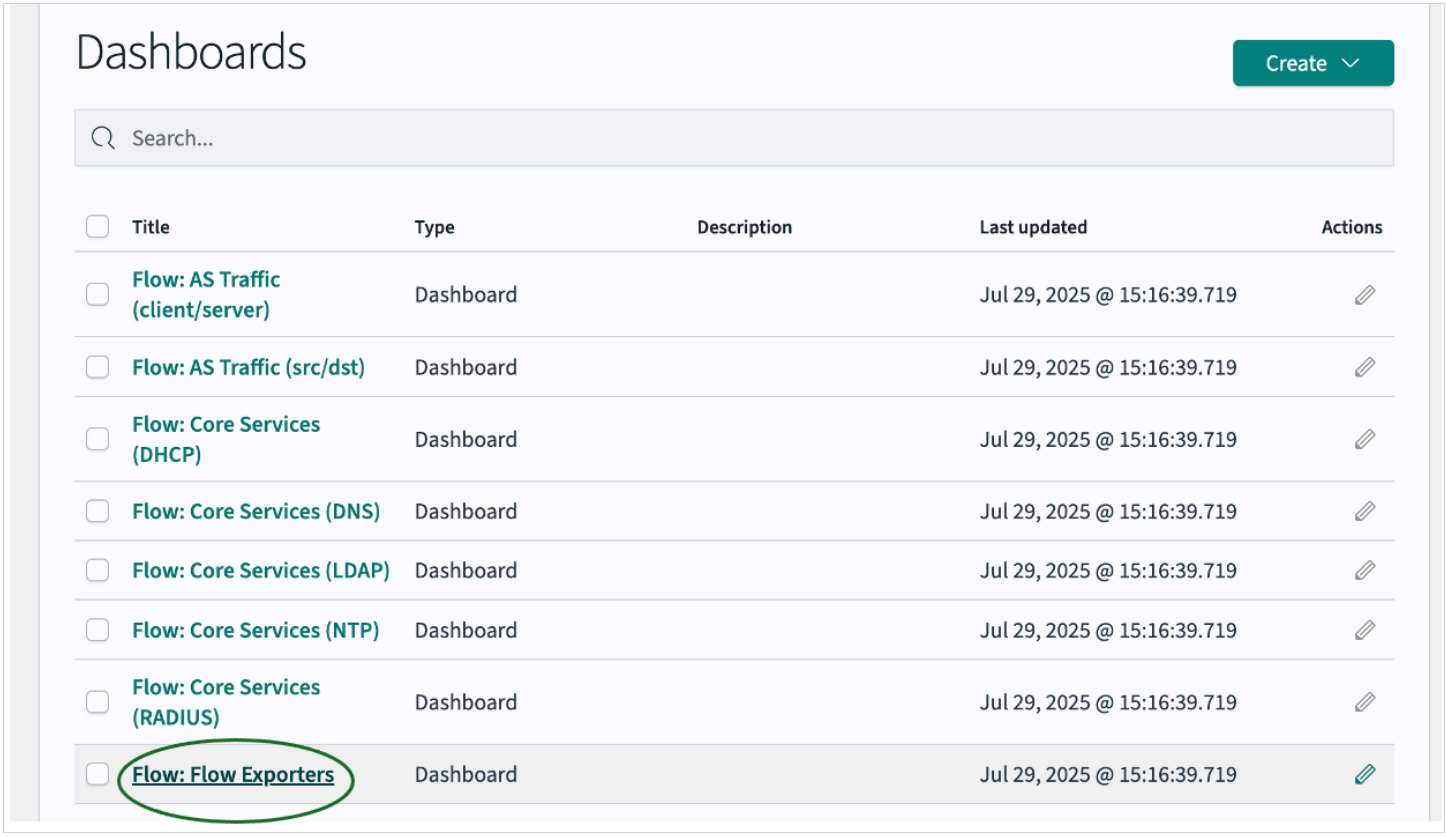
As a first step ensure all devices configured for sFlow are displayed as flow exporter on Apstra Flow Dashboard. On the left panel, select Opensearch **Dashboards >> Dashboard** to access the list of Dashboards.

Figure 9: Dashboard option provides a list of Dashboard that can be selected



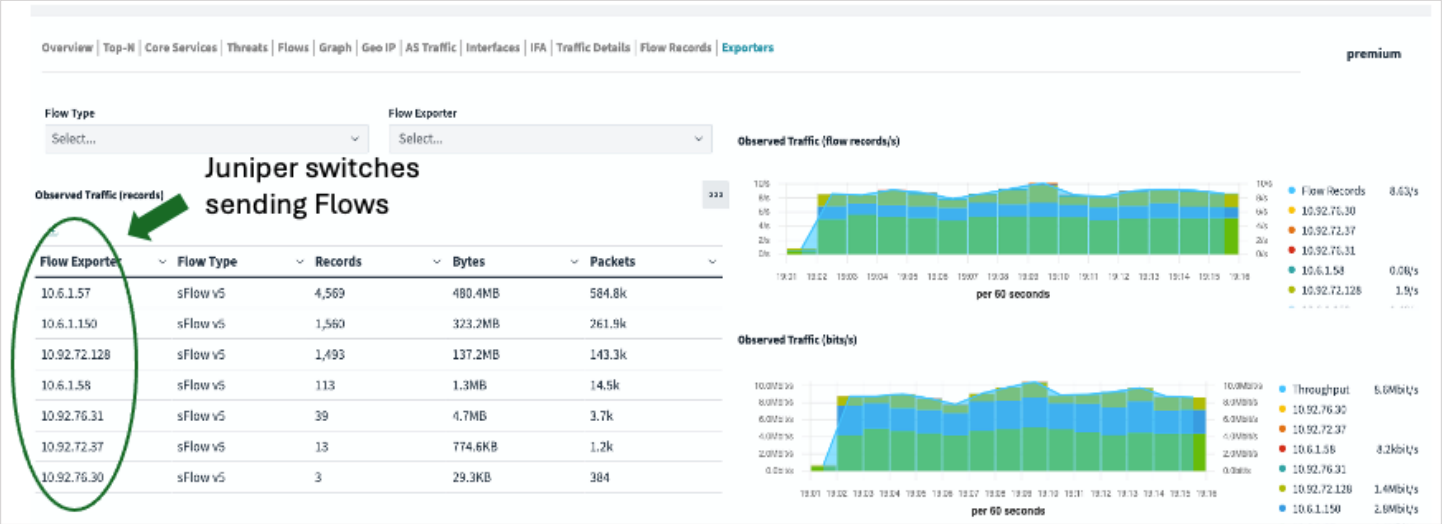
The next screen displays a list of available standard dashboards that are shipped with Apstra Flow. Click **Flow:Flow Exporters** to verify that all devices configured for sFlow are exporting sFlow data.

Figure 10: List of pre-set Dashboards available in Apstra Flow



On the next screen, all the flow exporters or devices configured to send sFlows to Apstra Flow are visible as Flow Exporters.

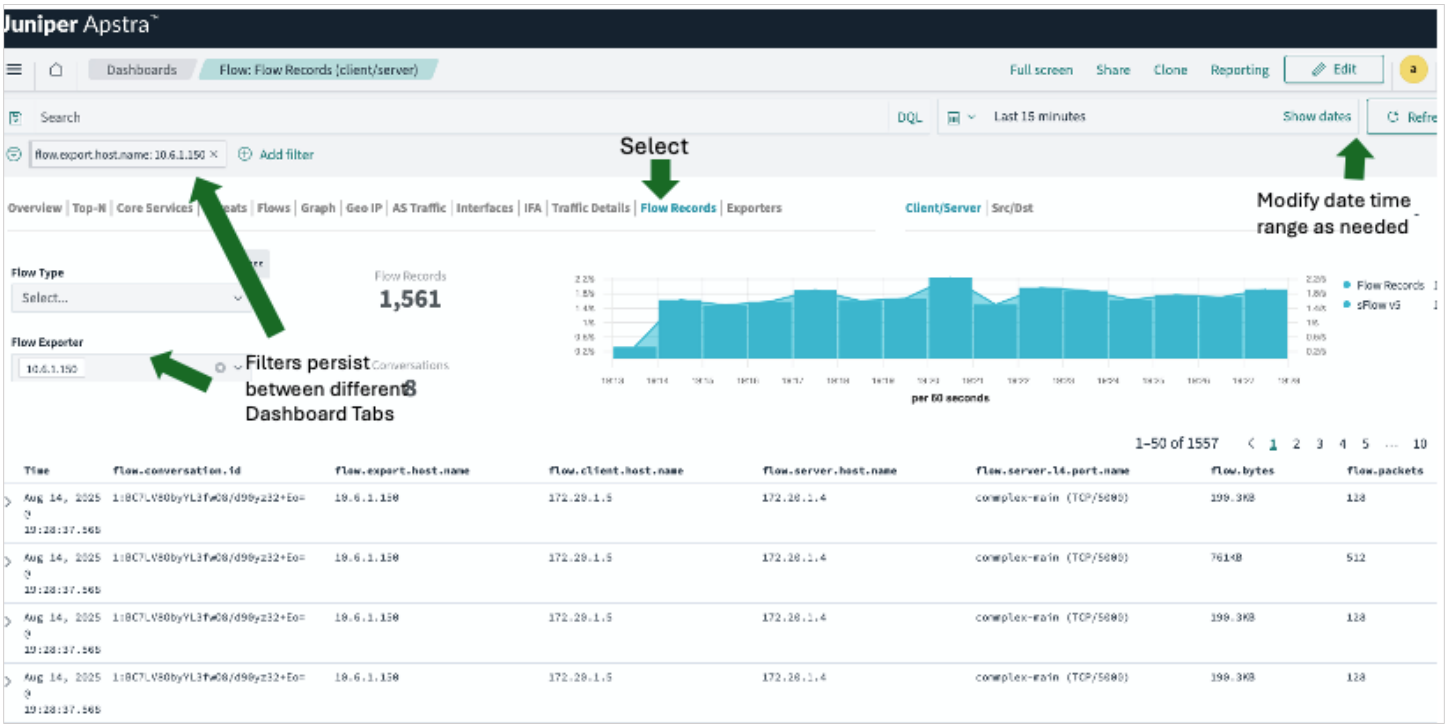
Figure 11: Juniper Switches as Flow Exporter



Flow Records

This dashboard helps to analyze the flow records from each flow exporter.

Figure 12: Flow Records to view sFlow records

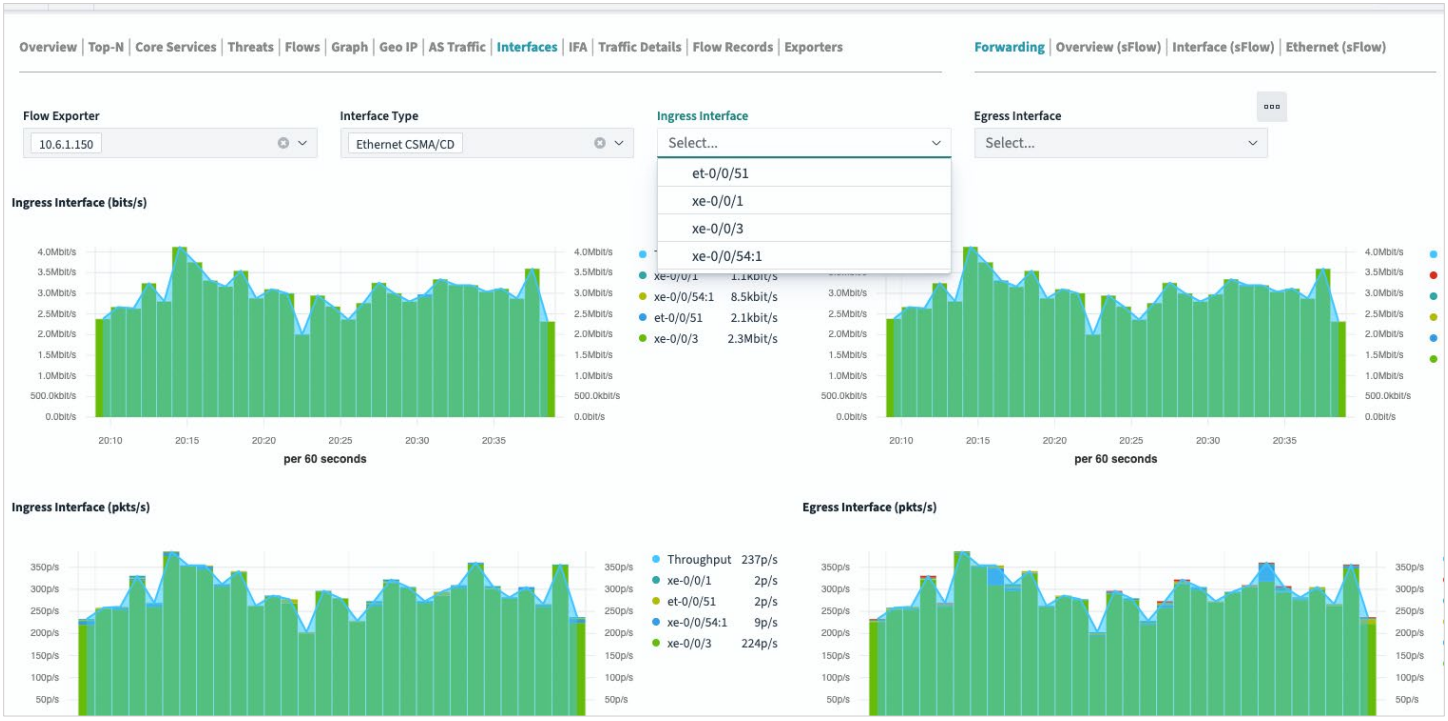


Interfaces

Use the Interfaces dashboard tab to view the interfaces that generate traffic. To ensure Apstra Flow displays the Interface names and not the SNMP indexes, apply the flow enrichment configuration described in Flow Enrichment.

The Interfaces dashboard provides a glimpse of the traffic generated from the ingress and egress interfaces.

Figure 13 : Ingress and Egress Interfaces for each flow exporter

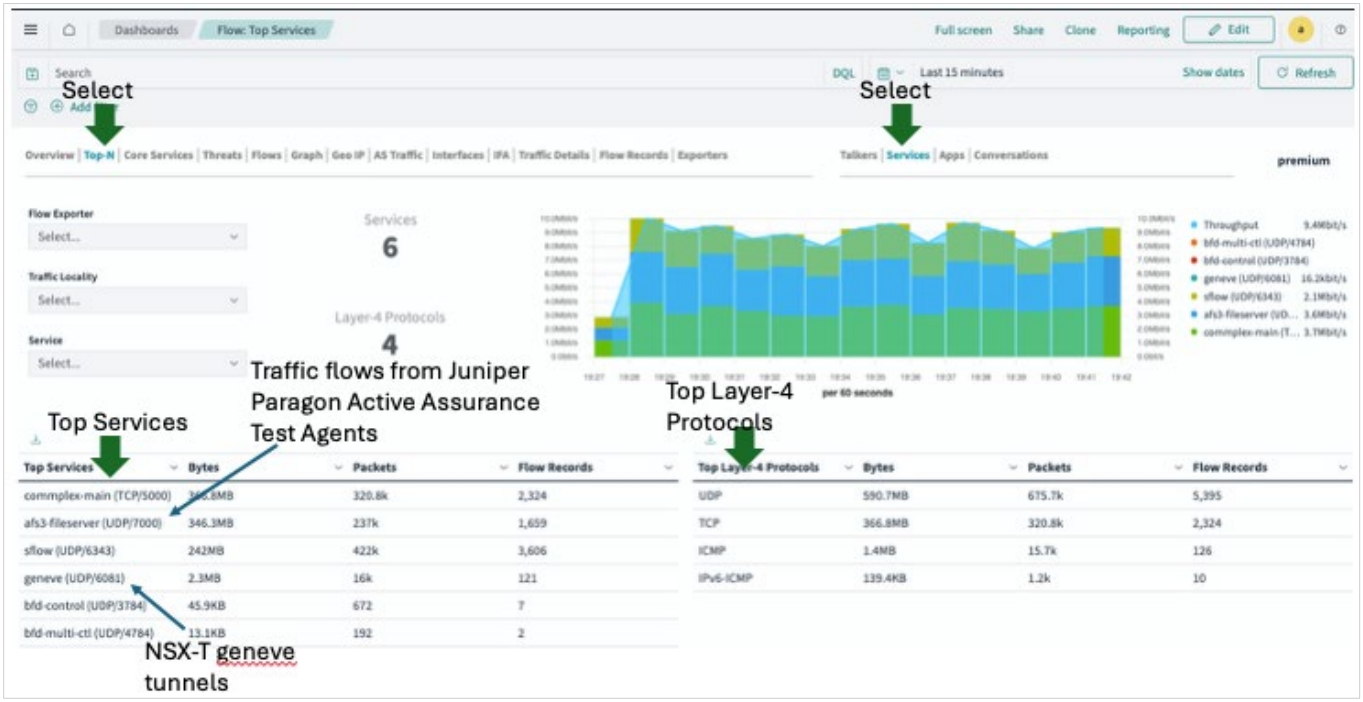


Top-N Dashboard

The Top-N dashboard provides an overview of Top services, Talkers, Apps, Clients and Top Conversations. **Figure 14: Top Services flowing through the Data Center Fabric** displays the Top Services. To create a filter that persists, use the drop down fields within the dashboard to filter or use the “Add filter” to persist a filter while navigating to other tabs.

Note: The “Search” bar at the top does not persist while navigating to other tabs.

Figure 14: Top Services flowing through the Data Center Fabric



In the above dashboards, we point out some services that show different applications generating flows such as VMware NSX-T and Juniper Paragon Active Assurance. These examples will be further discussed in other dashboards to explain Apstra Flow. The test agents used for Paragon Active Assurance reside on host connected to the data center leaf switches. Similarly, the VMs reside on ESXi servers connected to the leaf switches.

Note: VMware NSX-T setup is beyond the scope of this document. There is a dedicated JVDE document that explains the setup and integration of VMware NSX-T inline mode with Juniper Apstra. Refer the **3-stage NSX-T integration JVDE**.

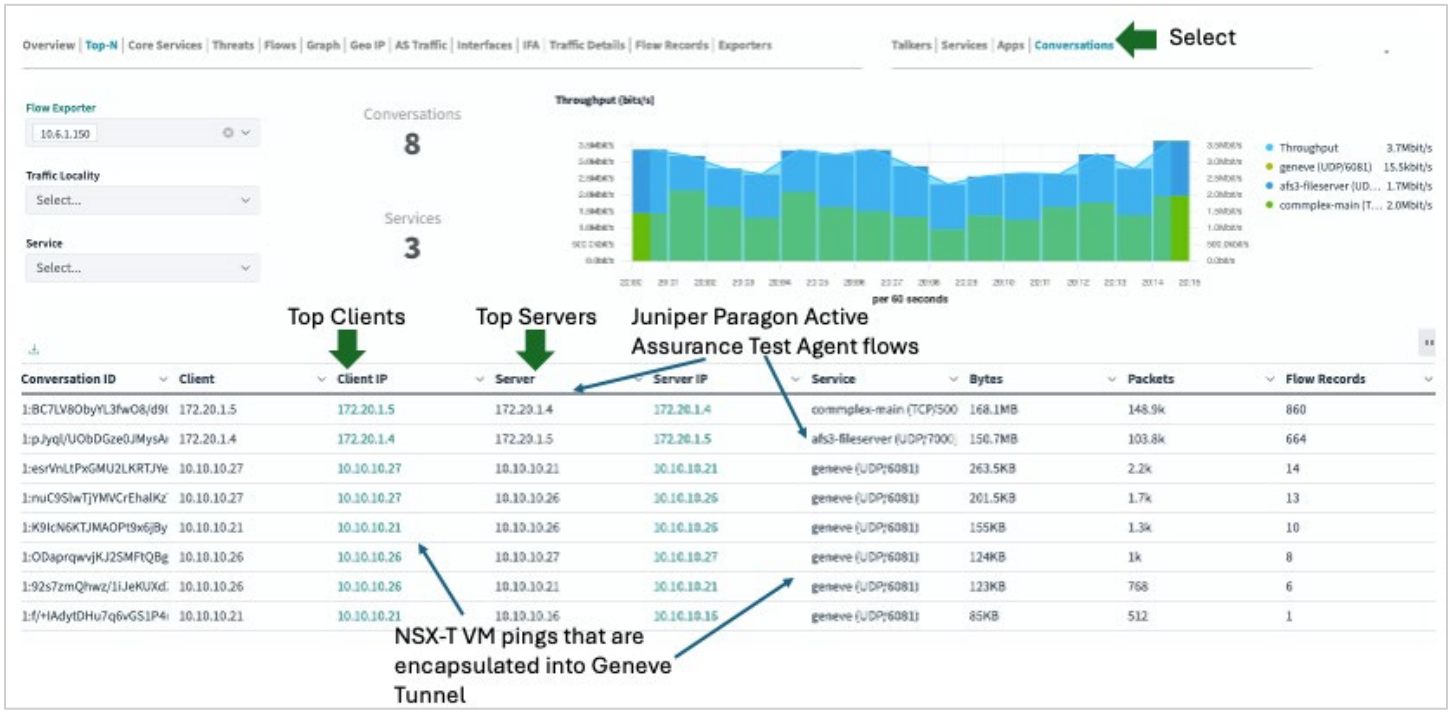
The Juniper Paragon Active Assurance application (PAA) is a programmable test and service assurance solution. PAA uses software-based and traffic-generating Test Agents that are delivered from the cloud as a SaaS solution or deployed on-premises in NFV environments. For this lab, an on-premise deployment of Paragon Active Assurance was used and is outside the scope of this use case. The purpose of this deployment was to create different traffic flows to demonstrate Apstra Flow capabilities. To set up Paragon Active Assurance, refer the Paragon Active Assurance **documentation**. For more information, contact your Juniper account representative for more information.

Client and Server Flows

Navigating to Top Conversations dashboard as shown in Figure 15: Top Conversations showing Clients and servers shows the Clients and Servers that are generating these flows.

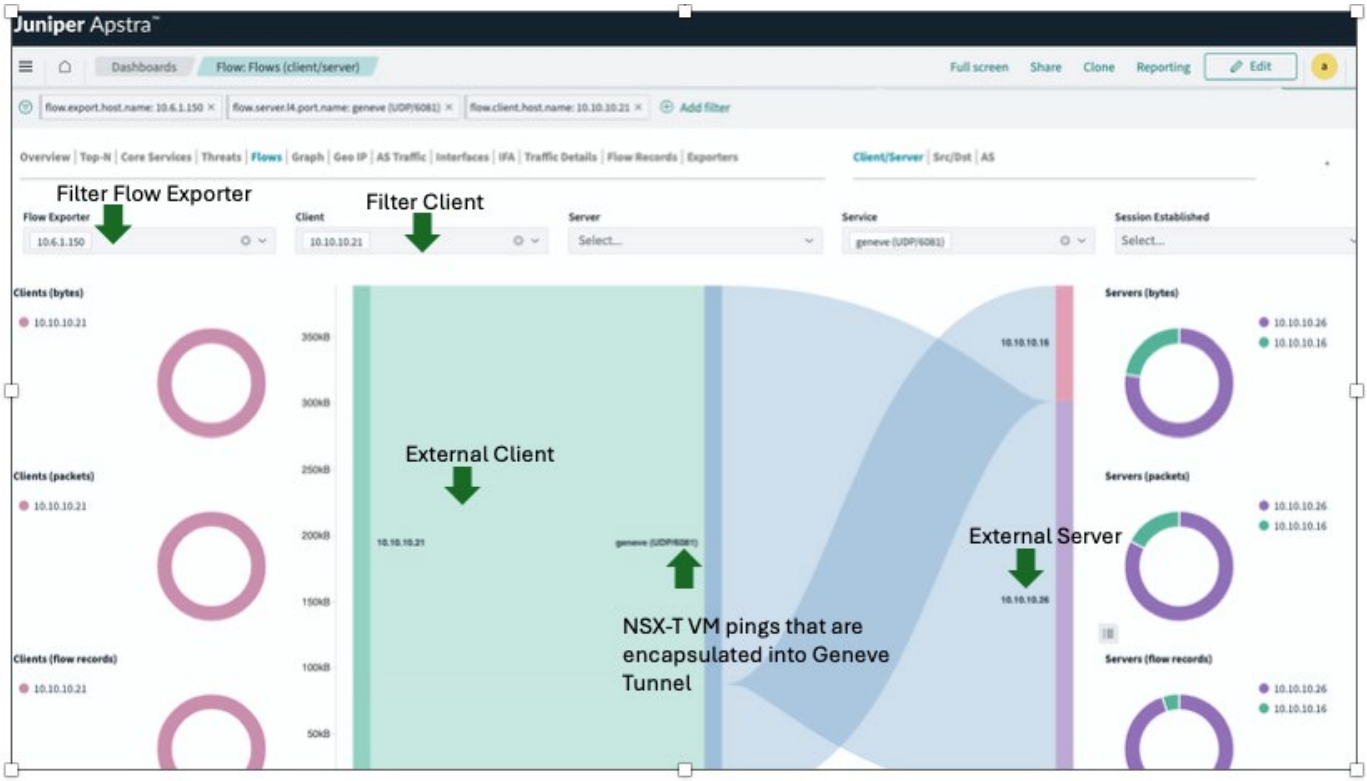
In the example below, the geneve tunnels result from ICMP pings sent from a VM connected to a server leaf switch to another VM in a different data center. Similarly, the traffic between Paragon Active Assurance Test Agents shows the service and conversation between the Client Test Agent that resides within the data center connected to the server leaf and the Server Test Agent that resides in another data center.

Figure 15: Top Conversations showing Clients and servers



The flows from the NSX-T example above can be visualized below. The Flows tab in Figure 16: Flows from Client to Server provides a visual display of the flows. Use the filters displayed here to filter out the flows of interest.

Figure 16: Flows from Client to Server



As discussed in this section, the various Apstra Flow dashboards offer both an at-a-glance view as well as an in-depth view of flows and services that operate within the data center fabric. The primary objective of this document is to ensure that flow data is successfully exported to Apstra Flow and that users understand how to configure sFlows and how to access the Apstra Flow dashboard. This document complements the official Apstra User Guide and Apstra Flow User Guide, which serve as the starting point for users working with sFlow. By following this document, users can expand their understanding of Apstra Flow and leverage it effectively for flow monitoring and operational visibility.

Test Objectives

As discussed in this document, the objective is to qualify sFlow functionality using Apstra Flow. The Juniper switches discussed in this document are deployed as ERB architecture with EVPN-VXLAN data center network. Refer to the **3-stage EVPN-VXLAN JVD document** for details. The goal is to ensure a well-documented design that delivers a reliable, predictable deployment for the customer.

Test Goals

The test goals for this JVD extension document are to validate:

- 3-stage JVD blueprint deployment
- Incremental configuration pushes/provisioning using Apstra configlet
- Telemetry/Analytics validation
- Performance/convergence characterization
- Failure mode analysis
- Verification of host traffic
- sFlow operation validation checks on each device
- Apstra Flow dashboard validation against network traffic

From Apstra Flow validation perspective below are the test goals:

- Build Apstra Flow and collector
- Apply license on Apstra Flow.
- Apply SFLOW configuration on the switches including the SNMP community setting that is required for Juniper Switches and the collector.
- Validate SFLOW with Apstra Flow and verify by simulating an SFLOW flow on the dashboards:
    1. Flow Exporter Dashboard to validate all switches are sending sFlow traffic
    2. Flow Records to view the sFlow record fields.
    3. Top-N dashboards for Conversations between Client and Servers (Internal and External destinations)
    4. Top-N dashboards for Services
    5. Top-N dashboards for Client to Server flow

Test Non-Goals

The JVDE qualification does not include the following:

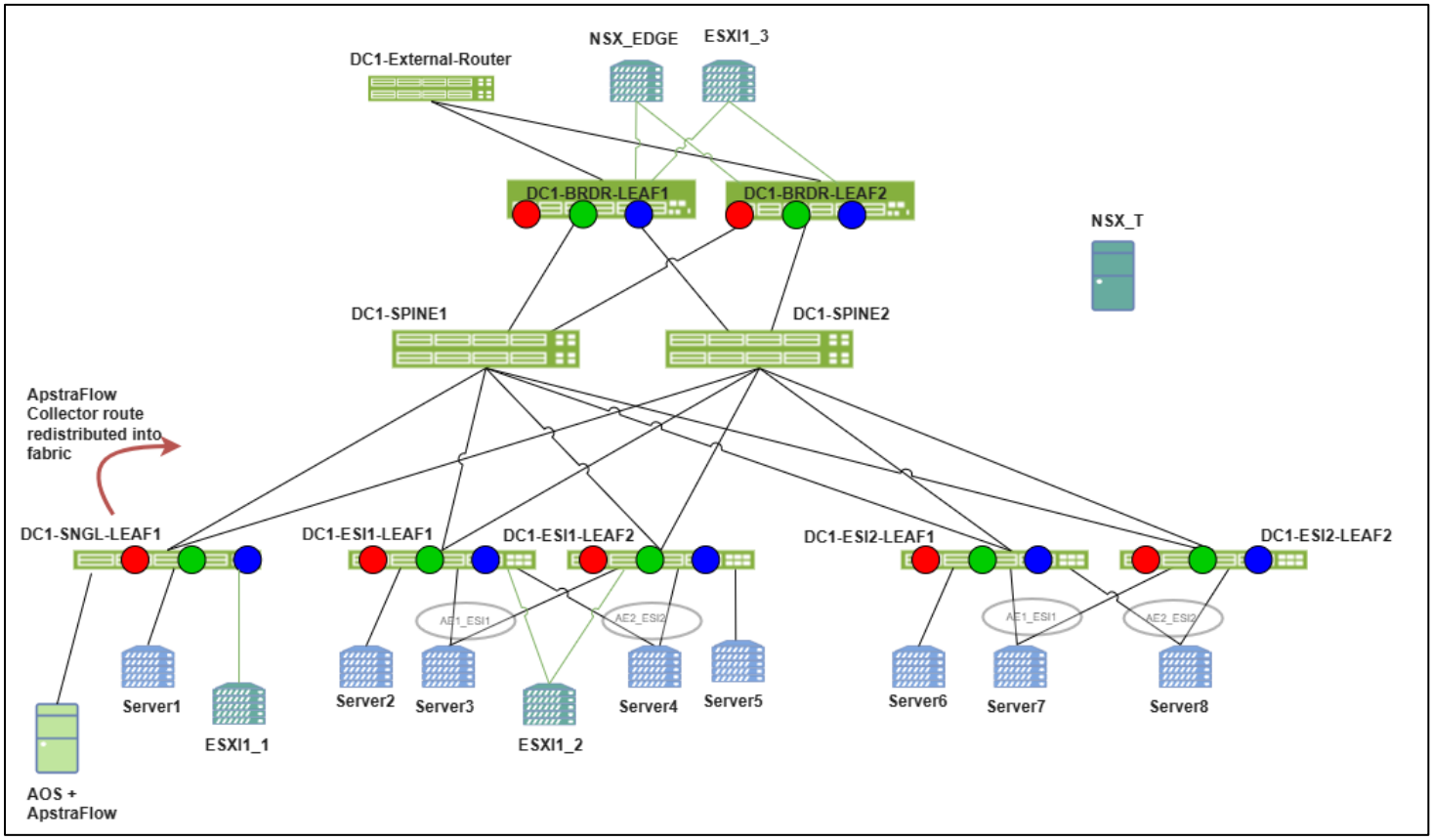
- DCI (setup and basic test as there will be separate JVD for DCI)
- Management VRF
- Apply pristine configs to devices

Results Summary and Analysis

The test report details all the validations performed for the purposes of this qualification.

Test Topology

Figure 17: 3-stage Design with ApstraFlow Topology



Platforms Tested

Table 1 lists the platforms and Junos OS release that were tested for this initial qualification

Platforms, Controllers, and Roles

Tag	Role	Model	OS	Line Card	Routing Engine	Fabric	VC	Helper/DUT
R0	Spine1	QFX5220-128c	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R1	Spine2	QFX5220-128c	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2	NA	NA	NA	NA	DUT

Tag	Role	Model	OS	Line Card	Routing Engine	Fabric	VC	Helper/DUT
			Junos OS Evolved 23.4R2-S5					
R0	Spine1	QFX5220-32c	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R1	Spine2	QFX5220-32c	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R0	Spine1	QFX5120-48YM	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R1	Spine2	QFX5120-48YM	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R2	DC1-SNGL-LEAF1	QFX5120-48Y-8C	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R3	DC1-ESI1-LEAF1	QFX5120-48YM-8C	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R4	DC1-ESI1-LEAF2	QFX5120-48YM-8C	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R3	DC1-ESI2-LEAF1	QFX5110-48S	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R4	DC1-ESI2-LEAF2	QFX5110-48S	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R3	DC1-ESI2-LEAF1	ACX7100-48L	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R4	DC1-ESI2-LEAF2	ACX7100-48L	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R5	DC1-BRDR-LEAF1	QFX5120-32c	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT

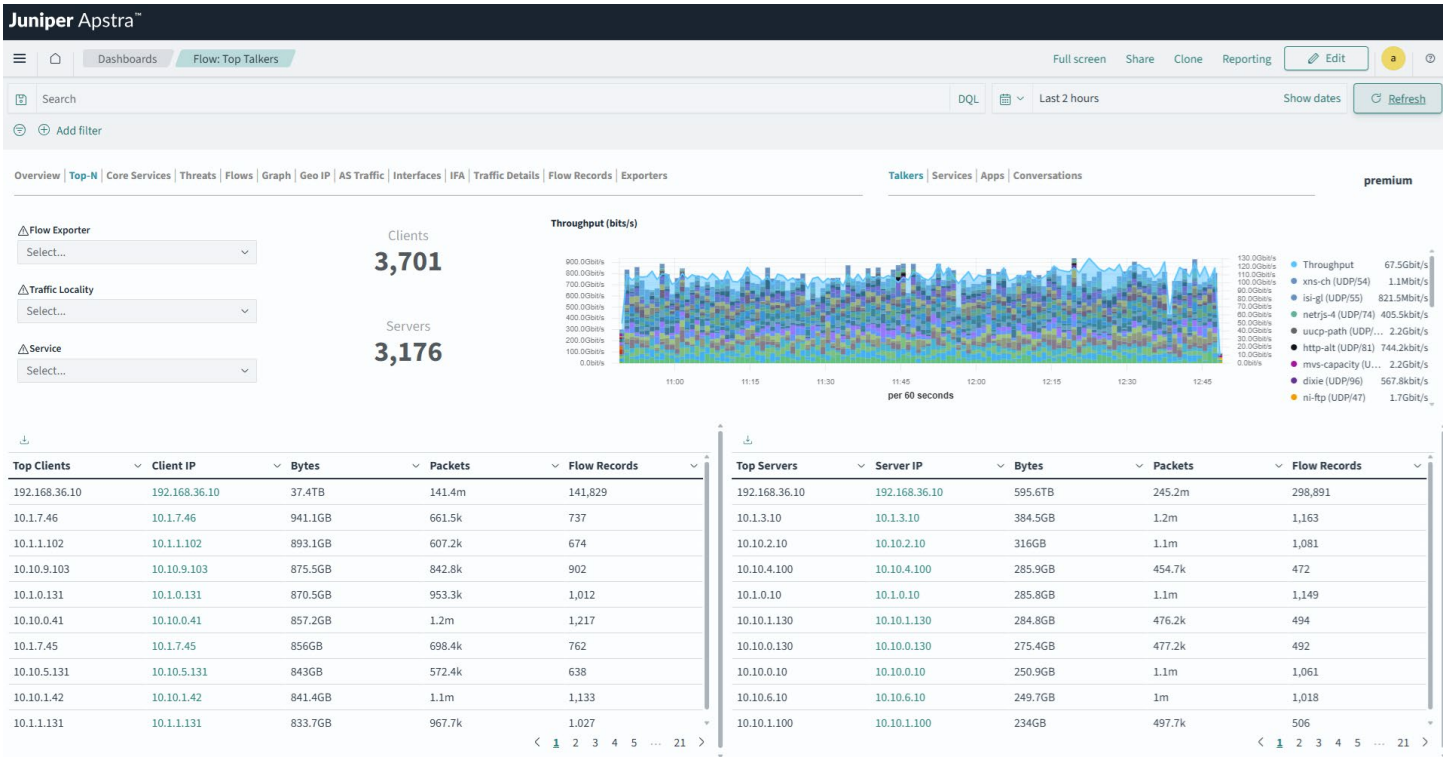
Tag	Role	Model	OS	Line Card	Routing Engine	Fabric	VC	Helper/DUT
R6	DC1-BRDR-LEAF2	QFX5120-32c	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	DUT
R5	DC1-BRDR-LEAF1	QFX5130-32cd	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R6	DC1-BRDR-LEAF2	QFX5130-32cd	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R5	DC1-BRDR-LEAF1	QFX5700	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R6	DC1-BRDR-LEAF2	QFX5700	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R5	DC1-BRDR-LEAF1	PTX10001-36MR	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R6	DC1-BRDR-LEAF2	PTX10001-36MR	Junos OS Evolved 24.4R2 Junos OS Evolved 24.2R2 Junos OS Evolved 23.4R2-S5	NA	NA	NA	NA	DUT
R9	External_Gateway	MX304	Junos OS 24.4R2 Junos OS 24.2R2 Junos OS 23.4R2-S5	NA	NA	NA	NA	Helper
RT0	Tgen Access hosts / DHCP	Spirent	SpirentOS	NA	NA	NA	NA	Helper

Scale

Scale Numbers for hosts and VLANs are presented in the 3 Stage Data Center Design with Juniper Apstra guide.

Performance Data

Longevity Testing



High Level Features

Feature	Node	Description
sFlow via default routing-instance	All Devices	sFlow records are exported to the collector on WAN ports; collector IP address is known via the fabric routing-table
ApstraFlow Collector	All Devices	ApstraFlow is used to collect and analyze the sFlow data
WAN fabric port statistics	All Devices	sFlow records for all the fabric links (i.e. leaf-spine ports)
Access port statistics	All leaf devices	sFlow records for all host and external gateway access links
SNMP ifIndex translation	All Devices	Collector translates interface ifIndexes into interface names for easy readability
Control Protocol traffic in sFlow Records	All Devices	Control protocol packets are also represented in ApstraFlow
IPv4 and IPv6	All Devices	Overlay Host Connectivity
Variable Sampling Rate	All Devices	Sampling of 1 out of every N packets. Collector can calculate actual traffic rates based on the sampling value

Events and Triggers Test

Test	Details
Provision the 3 stage blueprint with sflow configlets	Apstra Deployment Step as Documented in JVD
Provision External Gateway at Border leaf devices and sFlow access port at Leaf1	Apstra Deployment Step as Documented in JVD
Intra-VLAN, Inter-VLAN, Inter-VRF Traffic Validation	Host Emulation via Test Traffic
Enable sFlow configuration on Apstra Flow Server and Fabric Devices	Apstra Deployment Step as Documented in JVD
Deactivate and Activate sFlow Configuration at Global Level on Apstra Flow Server	Reconvergence and restoration of sFlow
sFlow Interface Up/Down from Shell on Apstra Flow Server	Reconvergence and restoration of sFlow
Restart sflowd on Apstra Flow Server	Reconvergence and restoration of sFlow
Verify if control packets are generated and mirrored to the sFlow collector	sFlow packet inspection
sFlow - Router Reboot	Reconvergence and restoration of sFlow
sFlow - Restart Routing Process	Reconvergence and restoration of sFlow
sFlow - Deactivate and Activate sFlow Interface	Reconvergence and restoration of sFlow
Disable sFlow configuration on Apstra Flow Server	Reconvergence and restoration of sFlow
sFlow Ingress/Egress Sampling of VXLAN Bridged Traffic at spine-and-leaf Network Ports	sFlow packet inspection
sFlow Ingress/Egress Sampling of Host Traffic at Single Access Port	sFlow packet inspection
sFlow Ingress/Egress Sampling of Host Traffic at aggregated Ethernet Access Port	sFlow packet inspection
Verify sFlow IPv4 Datagram Header on ApstraFlow Server	sFlow packet inspection

Test	Details
Check sFlow Polling and Sampling Rate on Apstra Flow Server	Accuracy of Collector Reports
Longevity Testing	System Stability

Traffic Profiles

Traffic Flow	Type	L4	Packet Size
red_all_p1_to_red_all_p3	Intra-VLAN	UDP	Random 256-1200
red_all_p1_to_red_all_p3_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200
blue_all_p1_to_blue_all_p3	Intra-VLAN	TCP	Random 256-1200
blue_all_p1_to_blue_all_p3_v6	Intra-VLAN (IPv6)	TCP	Random 256-1200
green_all_p1_to_green_all_p3	Intra-VLAN	UDP	Random 256-1200
green_sub_p1_to_green_sub_p3	Intra-VLAN (IPv6)	UDP	Random 256-1200
red_all_p1_to_red_sub_p4	Inter-VLAN	TCP	Random 256-1200
red_all_p1_to_red_sub_p4_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
blue_all_p1_to_blue_sub_p3	Inter-VLAN	UDP	Random 256-1200
blue_all_p1_to_blue_sub_p3_v6	Inter-VLAN (IPv6)	UDP	Random 256-1200
red_all_p1_to_external_p6	Inter-VRF	TCP	Random 256-1200
blue_all_p1_to_external_p6	Inter-VRF	TCP	Random 256-1200
red_all_p2_to_red_all_p5	Intra-VLAN	UDP	Random 256-1200
red_all_p2_to_red_all_p5_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200
blue_all_p2_to_blue_all_p5	Intra-VLAN	TCP	Random 256-1200

Traffic Flow	Type	L4	Packet Size
blue_all_p2_to_blue_all_p5_v6	Intra-VLAN (IPv6)	TCP	Random 256-1200
green_all_p2_to_green_all_p5	Intra-VLAN	UDP	Random 256-1200
red_sub_p2_to_red_sub_p4	Intra-VLAN	UDP	Random 256-1200
blue_all_p2_to_blue_sub_p5	Inter-VLAN	TCP	Random 256-1200
blue_all_p2_to_blue_sub_p5_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
red_all_p2_to_external_p6	Inter-VRF	UDP	Random 256-1200
blue_all_p2_to_external_p6	Inter-VRF	UDP	Random 256-1200
red_all_p3_to_red_all_p1	Intra-VLAN	UDP	Random 256-1200
red_all_p3_to_red_all_p1_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200
blue_all_p3_to_blue_all_p1	Intra-VLAN	TCP	Random 256-1200
blue_all_p3_to_blue_all_p1_v6	Intra-VLAN (IPv6)	TCP	Random 256-1200
green_all_p3_to_green_all_p1	Intra-VLAN	UDP	Random 256-1200
green_sub_p3_to_green_sub_p1	Inter-VLAN	UDP	Random 256-1200
blue_sub_p3_to_blue_sub_p5	Inter-VLAN	TCP	Random 256-1200
blue_sub_p3_to_blue_sub_p5_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
red_all_p3_to_red_sub_p2	Inter-VLAN	TCP	Random 256-1200
red_all_p3_to_red_sub_p2_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
red_all_p3_to_external_p6	Inter-VRF	UDP	Random 256-1200
blue_all_p3_to_external_p6	Inter-VRF	UDP	Random 256-1200
red_all_p4_to_red_all_p1	Intra-VLAN	UDP	Random 256-1200
red_all_p4_to_red_all_p1_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200

Traffic Flow	Type	L4	Packet Size
blue_all_p4_to_blue_all_p1	Intra-VLAN	UDP	Random 256-1200
blue_all_p4_to_blue_all_p1_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200
green_all_p4_to_green_all_p1	Intra-VLAN	UDP	Random 256-1200
red_sub_p4_to_red_sub_p2	Inter-VLAN	TCP	Random 256-1200
red_sub_p4_to_red_sub_p2_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
blue_all_p4_to_blue_sub_p5	Inter-VLAN	UDP	Random 256-1200
blue_all_p4_to_blue_sub_p5_v6	Inter-VLAN (IPv6)	UDP	Random 256-1200
red_all_p4_to_external_p6	Inter-VRF	UDP	Random 256-1200
blue_all_p4_to_external_p6	Inter-VRF	TCP	Random 256-1200
red_all_p5_to_red_all_p1	Intra-VLAN	UDP	Random 256-1200
red_all_p5_to_red_all_p1_v6	Intra-VLAN (IPv6)	UDP	Random 256-1200
blue_all_p5_to_blue_all_p1	Intra-VLAN	TCP	Random 256-1200
blue_all_p5_to_blue_all_p1_v6	Intra-VLAN (IPv6)	TCP	Random 256-1200
green_all_p5_to_green_all_p1	Intra-VLAN	UDP	Random 256-1200
green_sub_p5_to_green_sub_p1	Inter-VLAN	TCP	Random 256-1200
blue_sub_p5_to_blue_sub_p3	Inter-VLAN	TCP	Random 256-1200
blue_sub_p5_to_blue_sub_p3_v6	Inter-VLAN (IPv6)	TCP	Random 256-1200
red_all_p5_to_red_sub_p2	Inter-VLAN	UDP	Random 256-1200
red_all_p5_to_red_sub_p2_v6	Inter-VLAN (IPv6)	UDP	Random 256-1200
red_all_p5_to_external_p6	Inter-VRF	UDP	Random 256-1200
blue_all_p4_to_external_p6	Inter-VRF	TCP	Random 256-1200

Traffic Flow	Type	L4	Packet Size
external_to_red_all_p3	Inter-VRF	UDP	Random 256-1200
external_to_red_all_p3_V6	Inter-VRF (IPv6)	UDP	Random 256-1200
external_to_red_sub_p2	Inter-VRF	TCP	Random 256-1200
external_to_red_sub_p2_V6	Inter-VRF (IPv6)	TCP	Random 256-1200
external_to_blue_all_p4	Inter-VRF	UDP	Random 256-1200
external_to_blue_all_p4_v6	Inter-VRF (IPv6)	UDP	Random 256-1200
external_to_blue_sub_p5	Inter-VRF	TCP	Random 256-1200
external_to_blue_sub_p5_v6	Inter-VRF (IPv6)	TCP	Random 256-1200

Scale and Performance Data

This document might contain key performance indexes (KPIs) used in solution validation. Validated KPIs are multi-dimensional and reflect observations from customer networks or reasonably represent solution capabilities. These numbers do not indicate the maximum scale or performance of individual tested devices. For uni-dimensional data on individual SKUs, contact your Juniper Networks representatives.

The Juniper JVD team continuously strives to enhance solution capabilities. Consequently, solution KPIs might change without prior notice. Always refer to the latest JVD test report for up-to-date solution KPIs. For the latest comprehensive test report, contact your Juniper Networks representative.

Recommendations

We recommend using a dedicated revenue or WAN port for exporting sFlow traffic, rather than the management interface. Isolating sFlow traffic from the management plane helps preserve the integrity and performance of out-of-band management operations in production environments.

Apstra Flow provides detailed, low-level packet insights by leveraging sampled sFlow data across the data center fabric. Apstra Flow ingested sample flow traffic cannot be used for precise bandwidth metrics. Its strength lies in flow-level analytics and enables operators to trace traffic paths, identify anomalies, and validate policy compliance. When used with the Apstra Telemetry dashboard, network operators can troubleshoot traffic issues using the flow behavior and interface statistics.

Revision History

Table 3: Revision History

Date	Description
February 2026	Removed QFX10002 as leaf device. Added additional validated Junos OS and Junos OS Evolved releases – 24.2R2 and 24.4R2.
September 2025	Initial publish

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Send feedback to: design-center-comments@juniper.net V1.1/260212