Frequently Asked Questions - Apstra AOS 3.1

Apstra AOS – General Questions

Q: 1. What are the reasons behind developing AOS 3.1?

A: Companies are embracing business and digital transformation to improve on customer experience, gain competitive advantage and increase market share. Yet they are unable to realize the full benefits due to several factors. One key inhibitor is the network. First and foremost, there is no industry solution to address unified automation and policy across any vendor, any workload, and any cloud. Second, customers who deployed NSX don't have a scalable solution that bridges the integration gaps between the physical underlay and overlay NSX holistically and efficiently. Specifically, the visibility is limited as traffic traverses underlay and overlay networks, customers are unable to validate, detect and remediate underlay network requirements in order for NSX to work correctly, and unable to enforce security policy across VMs and bare metal. Lastly, there is no industry solution to remediate network issues across the fabric instantly.

Q: 2. What are the major capabilities and benefits announced in AOS 3.1?

A: The enhanced capabilities have an impact on business and IT. Our customers were able to reduce operational expenses by over 80%, accelerate MTTR by 70% and speed up the delivery of business services. These enhancements include:

a. A tight, seamless integration with NSX-T that instantly and automatically synchronizes network requirements with NSX-T needs. Also, the integration provides dynamic enforcement of distributed security policies across VMs and bare metal*.

b. Boosted multi-domain unified group-based policy that offers granular policies down to the IP endpoint, hierarchical policy enforcement, what if "policy scenario", and visualization of entire security policy posture.

c. Advanced, cloud-scale Intent-Based Analytics and root cause identification accelerating MTTR by 70%. A simplified, enriched view of anomalies, predefined probes for external network connectivity, customizable probes to fit the needs of any environment, and expanded root cause identification mapped to implicated anomalies.

d. Expanded multi-vendor and enterprise-class features-set fortifying network access support options and accelerating deployments.

NOTE:

THIS DOCUMENT IS FOR EXTERNAL USE FOR APSTRA CUSTOMERS, PRESS AND ANALYSTS.

THE DOCUMENT PROVIDES QUESTIONS AND RECOMMENDED ANSWERS RELATED TO APSTRA'S AOS 3.1 RELEASE.

Q: 3. What is different about AOS 3.1?

A: Apstra AOS is the first and only vendor that provides tight and seamless integration with NSX by bridging the gap between physical network and NSX/virtual network across any-workload and any cloud and data center in the following ways:

- **Automation** - AOS automates and enables consistent network and security policy for physical and virtual workloads across the physical and virtual/NSX infrastructure. As a result, businesses are more agile, and IT is able to respond faster to business needs.
- **Hardware Agnostic** - AOS integrates with any networking hardware vendor including Arista and Cisco enabling NSX to deliver consistent service-intent across the entire infrastructure. It enables businesses the flexibility to deploy an infrastructure of their choice that meets their budget and requirements without being locked-in to one vendor.
- **Scale** - AOS brings cloud-scale, 5-stage CLOS, deployment and operation to any physical and NSX virtual infrastructure. Businesses that are consolidating their data centers or are going through mergers and acquisitions are able to scale deployments across thousands of switches with no performance impact.
- **Visibility and auto-remediation** - AOS bridges the visibility gap in traffic traversing physical infrastructure and NSX enabling faster root-cause analysis and anomaly correlation. In situations where there are performance degradation, intermittent services or possible maintenance on leaf switches, AOS enables network team to quickly take appropriate actions ensuring virtual services are not impacted.
- **Closed-loop validation** - AOS goes beyond automation. It delivers a full integrity and continuous validation into the service-intent policy defined by NSX-T. Thus eliminating complex troubleshooting procedures. Businesses are able to accelerate resolutions and increase application availability.

Q: 4. In which vertical markets has AOS been deployed?

A: Apstra's Intent-Based Networking and Intent-Based Analytics have been deployed across large-scale, major organizations including the energy, financial and manufacturing segments.

Q: 5. How does AOS 3.1 compete with existing solutions?

A: Apstra AOS is the first Software-First Intent-Based Networking and continues to lead the industry offering a full life-cycle automation that adapts to a dynamic environment across a multi-vendor infrastructure. Apstra is the only vendor that provides a single source of truth that accelerates deployments and simplifies on-going operations. Other solutions in the industry are either a vertically integrated stack with disjointed management tools that locks customers in a specific hardware or a fragmented solution that tends to be complex and costly to deploy and maintain.

Q: 6. I'm an existing customer, can I upgrade for free?

A: Yes

Q: 7. Where can I go for upgrade?

A: Download the new version of AOS at **https://docs.apstra.com/**. Contact Apstra support for assistance.

Q: 8. Where can I learn more about AOS 3.1?

A: Access datasheet **here**

Additional Information:

This document is intended for external Apstra audiences. It contains frequently asked questions that customers, press or analysts may ask, regarding the AOS 3.1 solution.

For more information contact us at **apstra.com/contact-us/** or visit our website at **apstra.com**