APPLICATION NOTE

Quick Tips to Create Self-Provisioning Packet Brokers

According to research conducted by Enterprise Management Associates in October of 2016, 47% of IT personnel experience improved productivity from deploying network packet brokers (NPBs). However, NPB choice is critical. The usability of the NPB is what will ultimately determine productivity and total cost of ownership (TCO) savings. Therefore, the system must not only be easy to set up but easy to maintain as well.

If the wrong NPB is selected, IT departments experience the following issues:

- Initial manual provisioning at scale is slow and error prone
- Increased complexity and productivity delays due to misunderstandings and delays between the build team and remote teams (installation, technicians, etc.)
- Post-deployment, ongoing updates to the visibility system are typically slow and error-prone due to complex manual configuration processes

The solution is to choose an NPB that supports zero-touch provisioning. Built in features like a Representational State Transfer (REST) interface allow for automated provisioning systems which reduces start-to-finish programming times to five minutes or less.

Besides the initial programming, this solution can also be adapted to implement a continuous self-configuration system, taking advantage of the flexibility of virtualized tools and cloud-based security analytics tools to monitor.

Overview

This brief reviews techniques to create self-provisioning NPBs for NetSecOp teams.

Additional Resources:

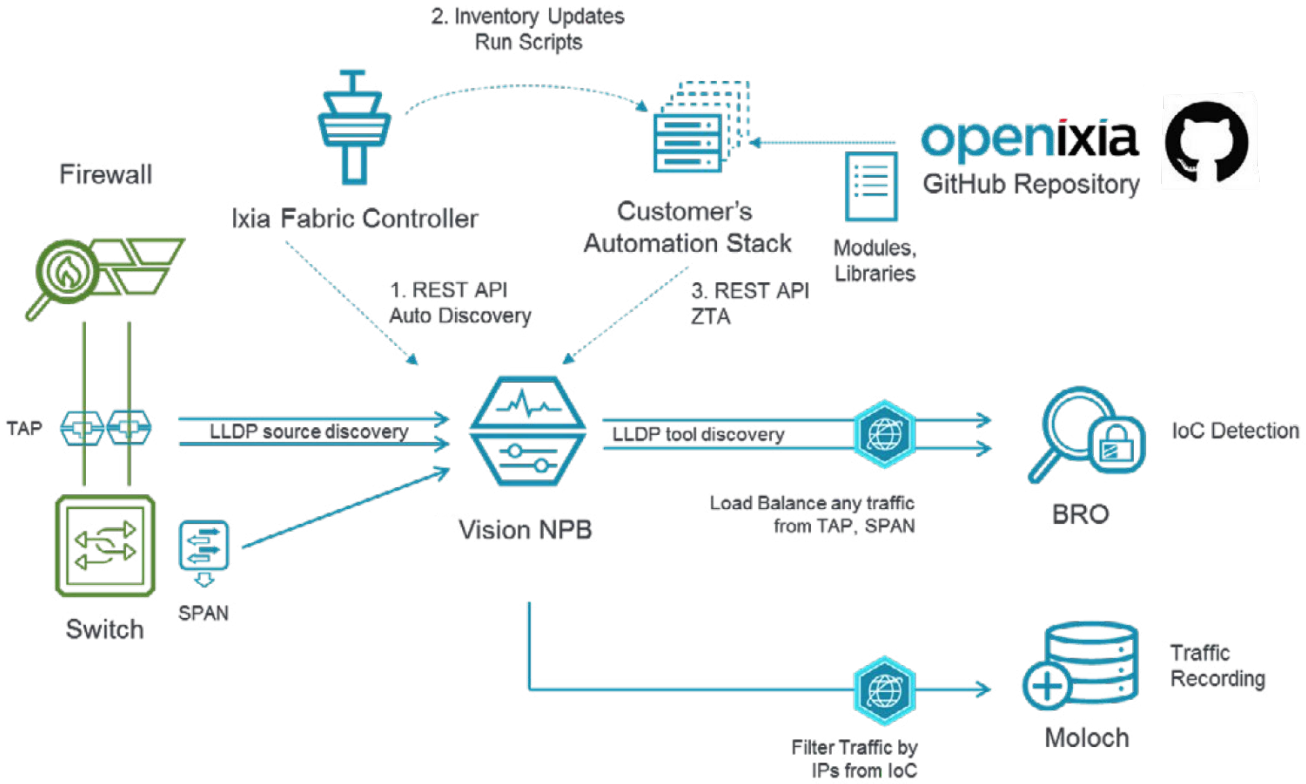
- How to improve network performance Podcast
- Best practices for network monitoring

KEYSIGHT TECHNOLOGIES

The visibility platform should provide comprehensive REST API automation support that is backed by an open forum, like the OpenIxia initiative. OpenIxia is an open, community-based repository on GitHub that extends support to many popular scripting languages and frameworks like Python and Ansible. With extensive material openly available, it's easy to build a self-provisioning system that will set up, update, patch, manage licenses and automatically discover and configure the NPB without manual intervention, based on the connected topology.

In the Link Layer Discovery Protocol (LLDP) based self-configuring example below, the solution detects the link partners that are connected to each port on both the Tools and Taps/SPAN side, decides what configuration to apply, and then automatically puts the port into production. The solution completely eliminates the need to go through a tedious port mapping process. Technicians can simply plug the connection into any available port and the rest is done automatically.

With extensive material openly available, it's easy to build a self-provisioning system that will set up, update, patch, manage licenses, and automatically discover and configure the NPB without manual intervention, based on the connected topology.



Visibility Architecture Solutions from Keysight

In the end, any regulatory compliance strategy is only as good as the quality of data that is being fed to the tools. The most important part of your regulatory compliance plan will be the architecture, as this piece will determine what, if any, policies and procedures are being adhered to.

Keysight's network visibility solution involves using network packet brokers in conjunction with application filtering and taps. Learn more about Keysight's **Taps, Network Packet Brokers, AppStack,** and **Hawkeye** technology along with the solutions that our technical partners offer.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES