Simplifying the DevOps Model

CISCO NEXUS SERIES SWITCHES AND PUPPET AUTOMATION

Why Automation with Puppet Labs?

Organizations that operate in environments where manual processes and scripting are used for repetitive tasks tend to experience issues such as noncompliance and reduced productivity.

And as most IT organizations operate in silos, it takes multiple tickets between server and network administrators to communicate required changes in the network to support application requirements. This manual process and scripting often takes days to get the networking set up, causing delays in application deployments.

In addition, most organizations use a CLI or GUI approach to manage and configure individual devices on the network. This approach has been the de facto for many years—but networks are changing, complexity is increasing, and new applications are being deployed to support evolving business models that require faster delivery and response time of the network.

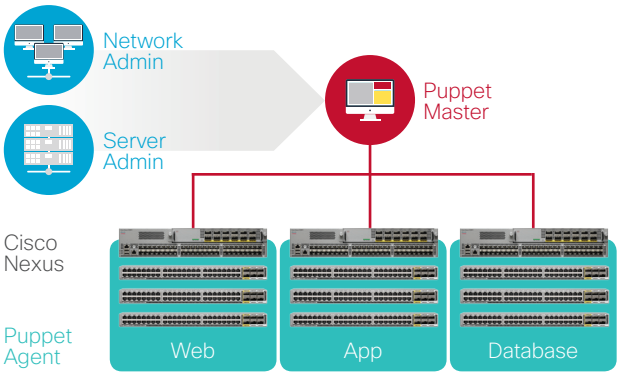
In order to move away from manual provisioning and reduce errors, automation tools including Puppet software can alleviate many current challenges by allowing IT professionals to manage a large number of devices quickly and accurately, do more with less, and respond faster to business needs.

Automating Cisco Nexus Series Switches

Cisco Nexus® Series Switches are being deployed in data centers across the globe. Our goal is to automate manual- and error-prone tasks using Puppet software to give DevOps teams the ability to accelerate application delivery and enable the creation of an agile infrastructure that meets changing business needs. Our customers—whether Web 2.0, small or large enterprises, or service providers—will experience tremendous benefits in automating network provisioning, image and patch management, configuration tasks, and security policy management. We'll examine these use cases in more detail in the next section.

The network automation model follows what has been done in the compute/server world by creating software plugins in the Cisco Nexus Series Switches to expand its programming functionality (Figure 1).

Figure 1



The Puppet declarative model for automation describes the desired end state, and the Puppet agent translates the request to concretely render the policy intent on the actual infrastructure. This benefits the DevOps teams by abstracting the complexity of network programming and simplifying its development. It also provides an audit trail for compliance, and documents the intent for future troubleshooting situations that may need to know the original intent behind the configurations that exist.

Now, compute, application, operating system, or network teams can use the same industry-leading tool to collaborate on new deployments and changes to top-of-rack switches, and updates to operating systems can be rolled out in minutes instead of days or weeks.

In collaboration with:

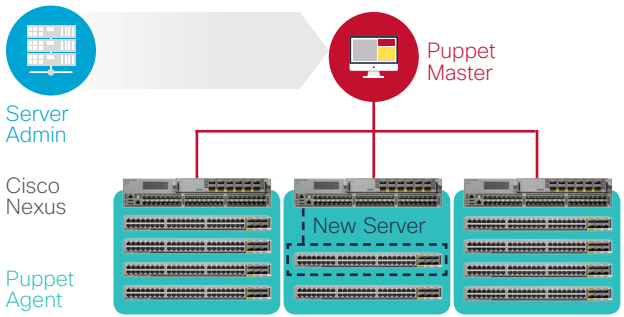
Use Cases

Embracing DevOps Model:

Challenge: Network has impeded software/application delivery due to complexity of configuration to support new, changing applications. For example, server administrators need top-of-rack switch configuration for every new server/VM they bring on board. This is a manual process that involves change request tickets.

Solution: Puppet Master software is used to put the new server/VM in the right VLAN/segment and apply appropriate ACLs. Integration of the network in DevOps tool chain/workflow cycle ensures delivery of applications in a timely fashion and allows organizations to innovate faster (Figure 2).

Figure 2

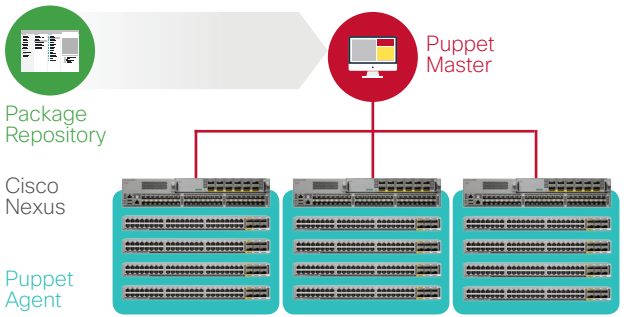


Image/Patch Management and Configuration:

Challenge: Bringing new switches to the network manually is time consuming and allows for configuration mistakes. Manual patching on networking devices also doesn't integrate with customer's operational tool chains, causing inefficiencies in the operational model.

Solution: By leveraging Puppet Enterprise agents on Cisco Nexus Series Switches, customers can now manage initial provisioning, images, and patches in the same way packages are managed on compute nodes, which allows for rapid integration into customer's operational tool chains (Figure 3). Using this process, a large scale of switches can be provisioned in minutes.

Figure 3

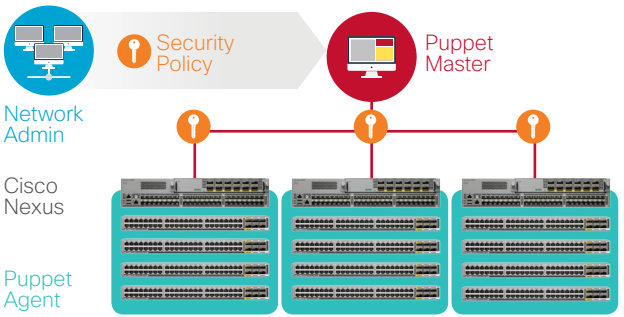


Security Policy Management:

Challenge: There is no audit trail, consolidated record of changes, or centralized enforcement of configurations. In addition, manual security configuration is required for network devices every time a new switch is added or changes are to be made to accommodate application requirements. This can cause delays in deployment and allows the potential for error when configuring, which may lead to security breaches.

Solution: Network administrators create centralized security policies in the Puppet Master by defining the desired end state required to accommodate application requirements that will be distributed and enforced with an audit trail across Cisco Nexus Series Switches. Network administrators can also identify all noncompliant configurations and remediate. (Figure 4).

Figure 4



Why Cisco?

Adding Puppet Labs software to Cisco Nexus Series Switches can drastically accelerate integration into a customer's operational tool chain. And with a near-future roadmap to integrate the Puppet Enterprise agent, Puppet Labs enables additional configurations of trunk/vPC, BGP, TACACS, SNMP, NTP, Syslog, image upgrade/patching, and more. The Puppet declarative model enables policy-driven automation of all IT infrastructures, complementing the transformative policy-driven operational model provided with Cisco® Application Centric Infrastructure (Cisco ACI™). The automated provisioning of these rich, configurable capabilities leads to higher network reliability and security while further simplifying the DevOps model and accelerating application deployments.

C45-XXXXXX-00 10/11