Network Automation with Dell Open Automation

A Dell Technical White Paper

Contents

1. The Software Defined Data Center

The concept of a Software Defined Data Center (SDDC) has sparked a revolution that might be the most significant transformation in IT since the invention of the mainframe. This transformation promises to complete today's virtualized computing and storage layers with the final component: a virtualized network stack, while enabling new and agile models such as cloud computing. At the same time, it is vital for the success of SDDC that this transition to a completely virtual data center not bring back the proprietary restrictions and limitations that were the hallmark of the mainframe era.

While initial virtualization efforts have been very successful at consolidating server and storage resources, organizations and the industry in general are just beginning to understand how these virtualization initiatives will impact the networks within their data centers. Many great minds and diverse organizations are grappling with the best way to manage these virtualized data centers – the coordinated operation of virtual machines, virtual storage, and virtual networking devices to help accomplish key application and business goals. The use of virtualization technology results in more complexity – not less – so implementation of effective network automation technology is essential for realizing the full benefits of virtualization.

2. The Challenges of a Software Defined Data Center

To date, the goal of the software-defined data center is being accomplished with virtualization. Conversely, much of the adoption of virtualization technology has centered on consolidation, allowing organizations to better utilize and manage their computational and storage resources. Initial benefits of consolidation through virtualization have included:

- Better utilization of servers and storage
- Simplified provisioning of virtual machines
- Workload balancing by deploying additional virtual resources

However, consolidation is only the first step towards the software defined virtualized data center. The adoption of server and storage virtualization has making IT managers more aware of the impact to their networks, and how the network infrastructure needs to change to allow virtualization technology to realize its full potential. While most physical networks today remain relatively static, virtualized networks must become dynamic to match the characteristics of virtualized servers and storage.

In short, IT managers are grappling with two key questions:

- How does the network need to change so that it can function in this new virtual environment?
- How can virtual servers, storage and network elements be managed together in a cohesive synchronized virtualized environment?

3. Network Automation

3.1 The Promise of a Software Defined Data Center Realized Through Automation

Most large data centers are complex heterogeneous environments that require considerable customization around standard interfaces and protocols. The pressure is on the network to respond quickly to orchestration requests from everything: applications, hypervisors, and management frameworks.

As enterprise networks gain in complexity, network automation is becoming a necessity for IT departments that are pressured to provide results faster while maintaining high standards for quality and service agreements.

At the most basic level, automation must offload the network administrator from repetitive, time-consuming and error-prone manual work. However, evolutionary features are needed in order to implement a software-controlled architecture in response to demands for data centers to become more cost-effective and integrated.

3.2 The Goals of Network Automation

Network Management Systems (NMS) have traditionally been used to operate and manage infrastructure. However, this model can be improved by offering automation right from the infrastructure itself, helping to address some use cases more efficiently. For instance, an advanced use case such as taking actions based on events can be greatly improved if the event filtering and logic are done locally, at the device level.

In recent years, the Development/Operations (DevOps) model has disrupted IT organizations by breaking silos and promoting continuous integration between Development, Quality Assurance and IT organizations. Application developers are demanding dynamic infrastructure changes. In a typical waterfall model, it can take several tickets and numerous iterations to modify the network in order to support new applications. A new selection of automation tools have emerged that facilitate the adoption of DevOps, enabling agility and reliability to IT operations.

Spending on public cloud infrastructure is growing at 2x faster than on private cloud IT. The prediction is that public and private models will co-exist in the form of hybrid cloud architectures for the foreseeable future. A factor that can foster and accelerate the pace of adoption of hybrid cloud-based platforms is network automation which enables a seamless integration between on and off premises workloads and provides consistency when workloads are moved.

Not only does network automation help remove mundane tasks and thus, maximize the investment on infrastructure, but also allows IT organizations to increase their agility and efficiency with a focus on aligning their outcomes with the corporate business goals.

Common use cases are paving the way to network automation.

3.2.1 Virtualization

Virtualization is dramatically increasing the rate and volume of required network changes. Virtualization enables the deployment of new workloads and Virtual Machines (VM) in a matter of seconds. Often times, users are pressured to deliver results which requires the network to be set up and configured instantaneously in order to provide connectivity for these new VMs. This brings more stress to the network administrators who need to know the servers and switches in which the VMs may run and reconfigure them constantly. Automation will help by automatically detecting when and where VMs are created, moved and deleted and configuring the servers and switches accordingly, making the whole process seamless and transparent to end users.

3.2.2 Configuration Management

Network administrators spent a great deal of their time setting and configuring ports and devices to grant and forbid users and applications access to parts of the network. This task can be very time-consuming and more importantly, prone to human errors that can cause severe downtimes. A good network automation tool can determine the objects affected by a change, undertake and monitor the change, and provide a report. Should anything go wrong, the tool can also roll back all changes to the initial known state.

3.3 The Path to Network Automation

As with many technologies, some of the initial vendor-sponsored forays into the automation space attempts to simplify the problem by providing single-source, proprietary solutions. Networking vendors in particular have sought to revolutionize traditional data center operational practices with new architectures that only work with their servers and storage devices, maintaining the market captive to their solutions.

Complicating the situation, effective automation must also be multi-level – allowing everything from applications, to virtual machines, to management systems to participate, as required by the data center. With the high level of customization prevalent in large data centers, it is important that data center managers have a way to define what they monitor and what they automate. In contrast to a one-size-fits-all approach, large organizations require the ability to customize their virtualization and automation solutions to fit their own unique needs.

In large data centers, there is also no presumption that any one vendor has a lock on the network, server, or storage infrastructure, and most are loathe to swap out their existing management infrastructure. Therefore,

viable automation solutions must work with the established environment and interoperate with a wide variety of heterogeneous servers, storage, and networking equipment. Automation technology must also remain agnostic to hypervisor, virtual switch, and server choices, without artificial constraints that include or exclude any particular approach, vendor, or technology. Ultimately, data centers need to be able to own their own intellectual property, from custom-designed operational models to scripts that are used to achieve automation, which requires an open standards-based approach.

Network vendors have taken a variety of approaches. In order to achieve an out-of-the-box operational model, some vendors have chosen proprietary architectures to simplify either the computing and storage stack or the network, or both. Unfortunately, these approaches ultimately constrain adopters to the innovations of a single vendor and limit the ability of the organization to customize their own environment. Some examples of these different approaches to automating virtualized environments include:

- **Vertically-integrated network automation** - This approach involves a highly integrated proprietary architecture that requires the customer to source all elements of the stack (servers, storage, networking, management software) from a single vendor, or a closed system of vendors. This approach also usually assumes management of all layers of the operational stack are done by the network vendor, opposed to modern data center practices.
- **Network-controlled automation** - In this approach, the monitoring, management, and provisioning of virtual environments is controlled from, or by the network, representing a huge cultural and operational shift by data center managers.
- **Open network automation** - Open network automation exploits open industry standards that allow the data center network fabric to be controlled by existing hypervisor or middleware tools. Because this approach is server and application centric (rather than network centric), it is consistent and tracks well with current data center operations.

3.4 Roadblocks to Network Automation

The road to network automation is paved with some major obstacles (Heffernan & Woollacott, 2015):

- Resistance to introduce changes to existing processes. Oftentimes organizations do not have the motivation to transform processes due to high risk, downtimes, and unclear returns on investment associated to changes.
- Silos between IT departments. Some of the new automation tools require tighter integration between the different IT departments. Still many organizations have clear demarcations, responsibilities, and accountability for different pieces of the data center infrastructure.
- Provisioning of networking resources is still a largely manual process. Some network operators still believe that the automation tools do not pose any advantage, or that the learning curve is too steep to justify a transition from the beloved Command-Line Interface (CLI).

4. Dell Open Automation

4.1 Overview

Dell realizes that for automation to be truly successful it must represent an evolutionary (rather than revolutionary) step, and it must work in concert with traditional datacenter operational practices. Through its Open Automation framework, Dell is pioneering a model that delivers innovative, open standards-based automation technology that will enable organizations to transform their virtualized data center infrastructure, becoming more agile, flexible, and efficient even as they develop new ways to deliver applications and services.

The Dell Open Automation framework is designed to transform the data center network into a programmable fabric, and to provide data center managers with greater visibility into how the network is performing. The Open Automation framework comprises Bare Metal Provisioning, Smart Scripting, Virtual Server Networking, REST interface, and DevOps tools, which streamline the network fabric's ability to participate in automated, policy-driven, real-time workload allocation in response to changing application and service demands.

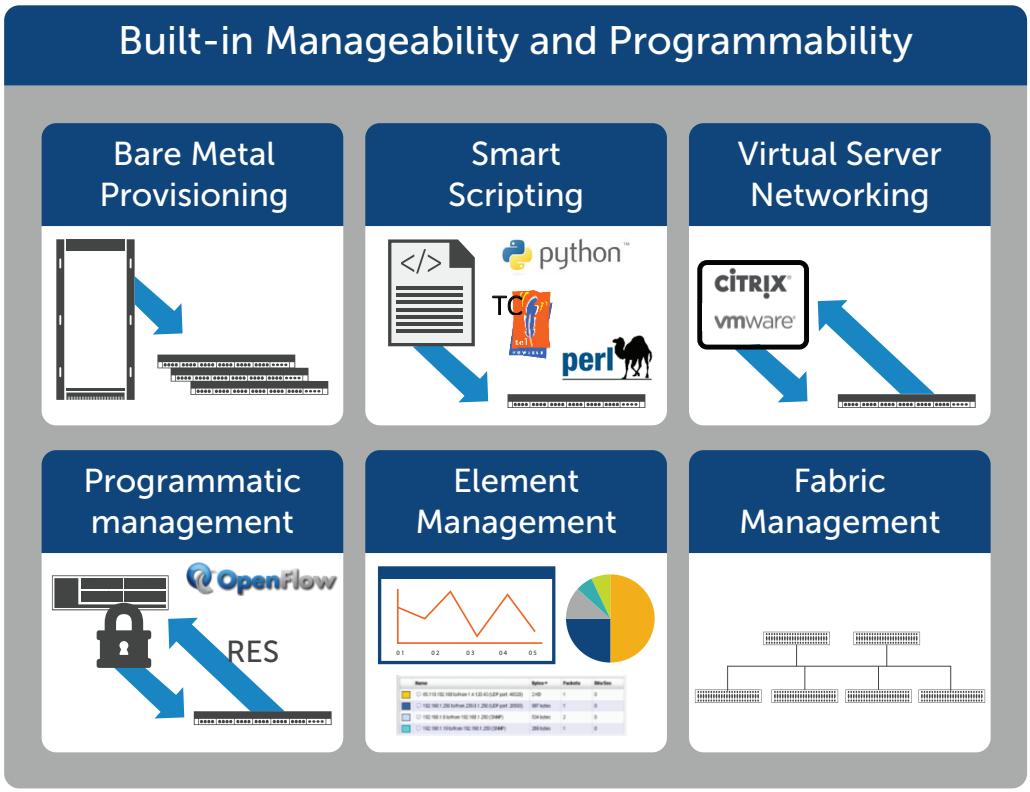


Figure 1: Dell Networking manageability stack

4.2 Bare Metal Provisioning

Automated bare metal configuration reduces operational expenses, accelerates switch installation, simplifies OS upgrades and increases network availability by automatically configuring Dell switches using standard protocols. This eliminates the need for network administrators to manually configure the switch, resulting in faster installation, elimination of configuration errors and enforcement of standard configurations.

Bare Metal Provisioning (BMP) is enabled on selected switches at factory. When a Dell switch is powered up, it will search the network for a Dynamic Host Control Protocol (DHCP) server. The DHCP server will provide the switch with an IP address the address of a file repository, and a set of initialization parameters, such as the operating system (OS) image, switch configuration, and even a script that will be executed before the configuration is applied. Upon reception and validation of the DHCP Server information, the switch will automatically upgrade and apply the configuration or run the initialization script, with no human intervention.

When the time to upgrade multiple switches comes, it is paramount to have a rollback plan in place. BMP is the first in the industry to provide an automatic rollback feature. If a problem with the new image occurs, reverting to the original state is as easy as disabling BMP and reloading the switch.

BMP can be enabled and disabled easily from the CLI console and Simple Network Management Protocol (SNMP) at will, providing greater control on when the feature should be deactivated, speeding up subsequent switch reloads until the next upgrade.

BMP is compatible with the bootstrap protocol (BOOTP) standard. In addition to Trivial File Transfer Protocol (TFTP), BMP supports File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), Hypertext Transfer Protocol (HTTP(S)), secure copy (scp), Network File System (NFS) mounts, and local access to the Universal Serial Bus (USB) storage device if attached.

4.3 Smart Scripting

Smart scripting increases network availability and manageability by allowing network administrators to deploy custom monitoring and management scripts on selected Dell switching platforms. With this capability, network administrators can implement version control systems, automatically generate custom alerts, create custom logging tools and automate management of network devices. Virtually any function that can be performed through the CLI can be implemented with Smart Scripting.

Smart Scripting provides an on-box scripting environment that supports the most popular languages: Python, Perl, Tool Command Language (TCL) and Ruby, as well as Korn and Bourne Unix shells, making it easy for IT administrators to quickly develop scripts using their favorite scripting framework.

Smart Scripting is complemented with several distinct features:

- A powerful event-driven framework that allows the system to react to events leveraging Smart Scripting and Unix tools
- Productivity libraries such as NetSNMP and SQLite
- An efficient and light weighted Web Server and Web Application framework that can be easily customized to expose custom services

4.4 RESTful Northbound Interface

Programmability greatly improves network provisioning by allowing third party system management tools to manage Dell network devices via a RESTful programmatic interface.

CLI and SNMP have been the de-facto interfaces for yesteryear management applications. The advent of web services applications brought a new paradigm to the software industry, which was eager to adopt a flexible and uniform interface for interacting with resources, while eliminating the overhead and cumbersomeness of legacy models.

Dell's REST Northbound Interface provides a lean, extensible, and highly decoupled API based on standard protocols: HTTP actions and Extensible Markup Language (XML) for data representation. While REST API is a programmatic interface suitable for next generation management tools, it can be used also by network administrators to extract very precise content in a human readable format.

4.5 DevOps

DevOps adoption is gaining mindshare within IT organizations that recognize the benefits of becoming more agile and reliable. DevOps practices improve IT performance. Dell networking is committed to help IT staff embrace DevOps and to use the same tools to manage switches as well as servers, operating systems, and applications.

The introduction of DevOps tools is a significant departure from previous techniques. These novel tools are declarative in nature. Users describe the end desired state and the framework takes care of the inner work. As a result, IT personnel can reduce the time to implement solutions, achieve agility and ensure operations are reproducible.

Dell Switches ship with two agents that implement the DevOps model: Puppet and Open Management Infrastructure.

- Puppet Labs® with its flagship product Puppet Enterprise is one of the front runners of the DevOps tools. The Puppet Agent implements Dell Networking DevOps, which exposes the most common networking resources for server administrators. With the Dell Puppet agent, users have a consistent way to configure virtual local area networks (VLANs, aggregations of links, or physical ports when new VMs and applications are deployed.
  - Dell's agent is a full distribution of the open source Puppet project, including Ruby and Facter. It allows users to execute Puppet manifests directly on the switches which can simplify the implementation of manifests before switches are moved into production.

- Open Management Infrastructure (OMI) is an open source project nurtured by Microsoft that implements a cross-platform management stack open based on standards and compliant with web services management (WS-MAN) and Common Information Model (CIM). OMI was extended to support a declarative syntax called Desired State Configuration, also available on other Microsoft platforms.
  - Dell Switches also include an OMI agent compliant with DSC that supports a rich interface for DevOps professionals as well as for legacy CIM clients. The Dell OMI agent implements the latest DSC Network Switch schema, which includes resources such as VLANs, interfaces, access control lists (ACLs), Border Gateway Protocol (BGP), Internet protocol version 4 (IPv4), Internet protocol version 6 (IPv6), etc.

4.6 Virtual Server Networking

Virtual environments require that the network infrastructure be dynamic in order to ensure network connectivity and security policies are maintained through the lifecycle of VMs. Virtual Server Networking (VSN) facilitates the communication between Dell switches and Virtual Machine management software to orchestrate and automate VLAN provisioning when VMs are instantiated, migrated, and finally disposed. This is a powerful capability that greatly simplifies many of the tasks associated with virtualized computing environments for system administrators.

In addition, network administrators also benefit from VSN exposing on the CLI vital information of the VMs, including virtual Medium Access Control (MAC) addresses, name of the VMs, current physical ports allocated to VMs, and virtual switch details.

The current version of VSN supports VMware™ vSphere® 5.x and Citrix® XenServer 5.6.

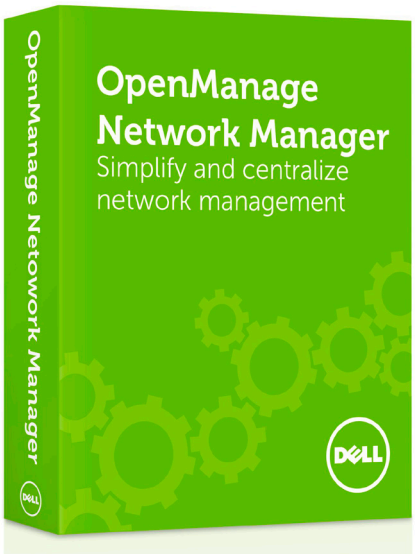
5. Dell OpenManage Network Manager

Growing networks can be a headache for today's IT organizations. Keeping track of the devices in the network and how they relate to each other and to other parts of the infrastructure can be difficult and time consuming. Dell OpenManage Network Manager (OMNM) is designed to make it easier to plan and manage Dell, Cisco™, HP®, Juniper Networks® and Brocade® network devices.

IT groups can unify network element management and simplify deployment of Dell and third-party networking environments with the rich suite of tools available in OMNM, an integrated management console for all important network management functions.

OMNM's centralized management solution for Dell networking environments provides discovery, configuration management, monitoring and reporting for the entire Dell Networking family of products and select third-party products — right out of the box. OMNM provides the following advantages:

- Automates the discovery of network devices, and provides detailed information on the devices and their connectivity, including the ability to draw physical and logical topology maps
- Provides the ability to easily configure and manage groups of network devices; configuration changes and firmware deployments can be made to multiple devices in one operation, and many network operations can be scheduled for pre-determined times
- Enables the network administrator to monitor the health and performance of their network, allowing the creation of dashboards to capture important events and trends, and display them over time



- Helps reduce TCO by proactively monitoring for network problems, automating common configuration actions and enabling easy firmware deployment, allowing network administrators to focus on more critical activities

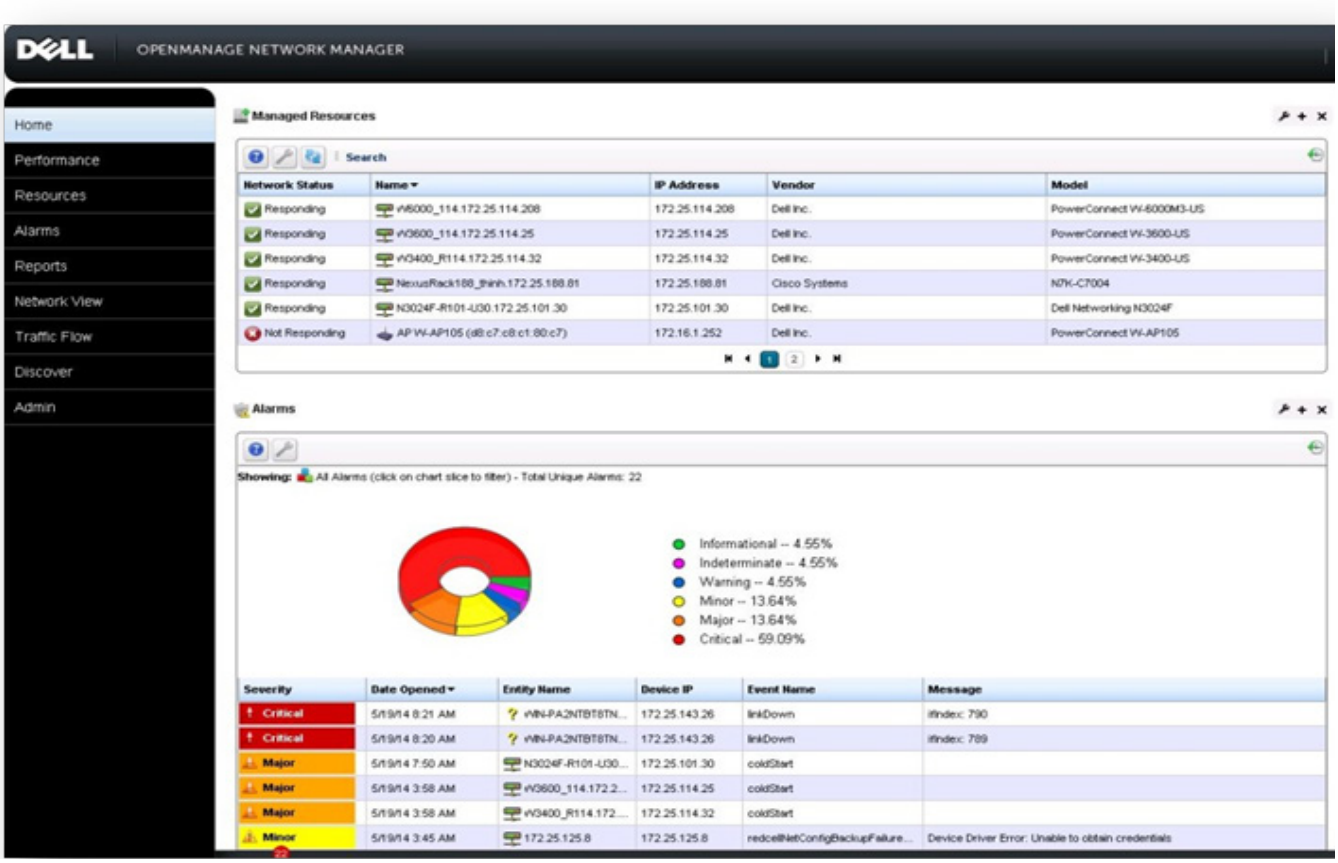
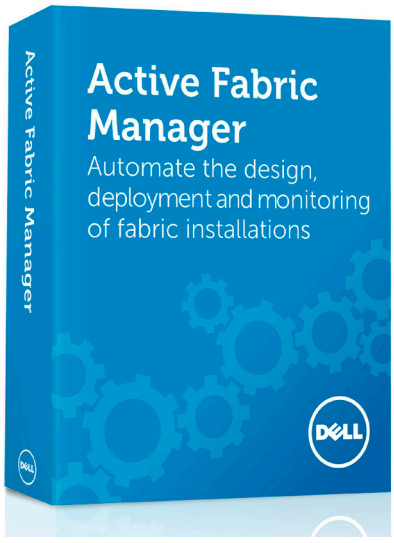


Figure 2: Dell OpenManage Network Manager

6. Dell Active Fabric Manager

Dell Active Fabric Manager (AFM) is a direct answer to the rapidly changing dynamics that challenge today's enterprise and offers compelling benefits to enterprise IT for delivering powerful new capabilities that drive the business bottom line. AFM enables enterprises to immediately deliver a highly-automated SDN-enabled Ethernet fabric with ease. By leveraging the latest innovations in SDN and network programmability, AFM can automate the design, deployment and day-to-day operations of data center fabrics, reducing fabric deployment time by up to 86% compared to manual configurations while eliminating costly configuration errors that account for the majority of outages today.



AFM includes many innovations that eliminate manual tasks associated with fabric design and deployment. AFM includes a customizable design wizard that makes the process of designing an end-to-end network fabric simple. The wizard

prompts the user to provide inputs required for the fabric design in an intuitive fashion.

In the background, AFM carries out all necessary calculations to present the most appropriate fabric topology, eliminating guesswork and errors that are common in network design and implementation. The designs are derived from a set of over 100 pre-defined templates that have been tested and validated for enterprise deployment. Additionally, for complex topologies, AFM has an advanced mode that enables users to customize their designs to a greater extent.

The AFM reference architectures include Layer 2 and Layer 3 spine-leaf and converged local area network (LAN)/storage area network (SAN) fabrics with Fibre Channel and Fibre Channel over Ethernet (FCoE) topologies and underlying technologies such as Dell's Virtual Link Trunking (VLT) and stacking.

Once the design phase is complete, AFM provides complete device configurations and powerful tools that enable the user to customize the deployment. Network administrators can complete all tasks from AFM's web graphical user interface (GUI) without having to issue a single CLI command. AFM generates unique configurations for all switches and automates the subsequent provisioning. The deployment process also validates the cabling and any mismatches are flagged with remedial actions. If there is a need to edit the AFM-generated configurations, it can be done easily from the AFM console. Auto-generated configurations can be

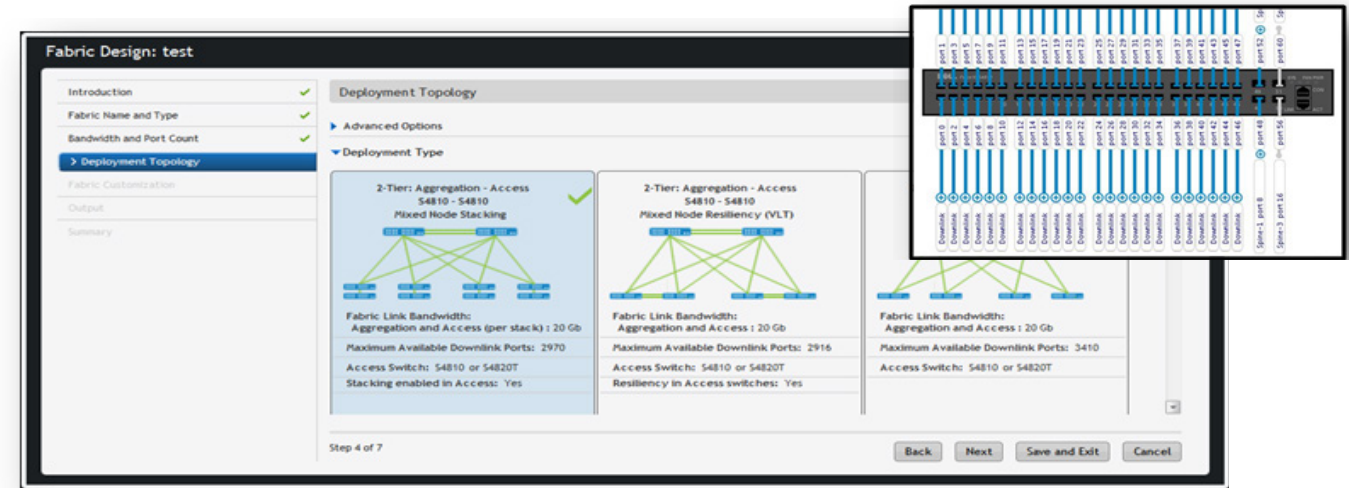


Figure 3: Dell Active Fabric Manager

edited by the user and stored in the deployment template.

7. Automation Use Cases

7.1 Bare-Metal Provisioning

When deploying or managing a large number of switches, it is often desirable to rapidly and automatically provision network resources. Doing so in an automated fashion helps to:

- Reduce deployment time
- Minimize human error
- Enforce standard and/or secured configurations

Similar to existing server capabilities, e.g., pre-boot execution environment (PXE) boot, network administrators can use BMP to automate the upgrade of selected Dell switches. Through this process, the switch can be upgraded to the latest release, but it can also be provided with the configuration only. Some network administrators might prefer to centralize the configuration of all switches in a central repository. BMP will help this purpose allowing each switch to receive its particular configuration from the file server.

In a more advanced use case, administrators might use the pre-configuration and post-configuration scripts

during the switch initialization to download a configuration template that will be customized on the fly for each particular switch. Post-configuration scripts can be used to verify that the resulting configuration is valid, or to notify administrators of any particular condition.

7.2 Network Automation with Smart Scripting

Large complex data centers typically have their own unique needs and requirements for monitoring and managing their network infrastructure. Using Smart Scripting on Dell switches, IT administrators can create custom Python, Perl, TCL, or Ruby scripts to manage and interact with their Dell switches.

While the scripts can be executed from the CLI console, the Web Server can be used to expose the results in a friendlier manner.

A wide variety of automation tasks can be implemented, including:

- Automatically archiving the configuration of switches in a central repository after changes have been committed
- Creating new CLI commands, for instance, to combine information from different sources (SNMP, CLI, etc.) and provide the output in a familiar CLI style
- Creating custom logging messages, for instance, when a particular port is enabled or used out of the allowed work hours
- Executing tasks at given times or periodically
- Storing and reporting operational information, for example, to find out the top busiest interfaces

7.3 Cross-functional Configuration Management

In many organizations, network operators maintain the health and connectivity of the network, while system administrators are responsible for deploying new services and applications.

Traditionally, changes requested by system administrators have been processed by network administrators using some sort of change ticketing system.

In the past, when new services required new physical infrastructure, the hours or even days taken by network administrators to make changes seemed commensurate with the rest of changes. With the advent of virtualization, today it is possible to deploy a new virtual machine in minutes. System administrators need similar tools that can help them provision the network for VM connectivity.

Puppet is one such tool. Puppet is used by administrators to configure VMs, operating systems, applications and services. With Puppet, these administrators can provision Dell switches using a common framework. A common practice is to maintain a CMDB to centralize the configuration of each device. Puppet allows users to keep the configuration bits centralized. When a change is made, that configuration is then pushed to all of the appropriate switches.

7.4 VM/VLAN Auto-Provisioning

For applications to operate seamlessly across a VM migration event, network configurations must become a part of the process. Associated VLANs must be made available on the physical switches where VMs will be located in advance of moving the virtual machines.

Dell Virtual Server Networking can be used with features such as VMware vSphere® vMotion®, configuring a VLAN and port on the destination switch and pruning the VLAN on the origin device in order to accommodate a virtual machine migration. In this scenario, a management application such as VMware vCenter would use Vmware vSphere vMotion to move the virtual machine. VSN incorporates the VMware SDK, which runs directly on the Dell switches. VSN uses this SDK to register with vCenter® to subscribe for notifications. When vCenter

initiates a vMotion event, the switch is alerted and adds or deletes VLANs accordingly in real time.

As a result, system administrators no longer need to open tickets with network administrators, which will reduce the downtimes associated with live migrations.

8. Conclusion

Realizing a return on virtualization investments means deploying effective automation techniques that can simplify the virtualized environment and allow a policy-based deployment model. While many network vendors have chosen a proprietary path to automation resulting in lock-in, Dell's approach is to utilize open and industry-standard technologies based on an extensible and modular operating system across the range of the heterogeneous Dell switch portfolio.

Rather than forcing organizations to rethink their entire computing, storage, and networking stacks, Dell Networking is committed toward operating as seamlessly as possible as part of a heterogeneous data center. This open and innovative approach gives large complex data center IT departments the control and flexibility they need to deploy powerful Dell switches without disrupting the existing infrastructure, operations, or policies that drive their organizations – and meeting their bottom lines.

9. References

Heffernan, P., & Woollacott, G. (2015, April 6th). Transformation speed bump delays automation adoption. Technology Business Research Special Report. Retrieved from http://www.tbri.com