Realtime publishers

The Essentials Series: Network Troubleshooting and Problem Identification

Automating the Top 5 Network Tasks with Configuration Management

sponsored by solarwinds

by Greg Shields

Copyright Statement

Automating the Top 5 Network Tasks with Configuration Management

In the world of the harried network administrator, there are far too many tasks that involve manual intervention. Updating router configs, changing parameters on switches, and maintaining documentation of the environment all require one or more manual steps to accomplish. With only a few network devices in the environment, the manual steps required to keep them operational might not add up to much. But as your environment grows, so do the sheer number of elements that must be correctly managed.

Exacerbating this problem even more is the knowledge that between 60 and 80% of all network issues relate to device misconfiguration. Using CLI tools might display your prowess with your network device's command-line IOS, but relying solely on that functionality for all forms of management is likely causing you more work all the while adding an operational cost associated with the occasional mistake.

For many network administrators, the next step in automating their responsibilities often starts with the creation of homegrown scripts. These scripts enable the administrator to quickly update running configs or query devices for information. But in the case of a job change, homegrown scripts rarely outlast the administrator. When your environment is bandaged together with scores of homegrown scripts that only you truly understand, your departure from your job is likely to also be the end of your attempts at automation.

Management tools are available today that assist with these problems. These tools automate many of the highly manual activities of the network administrator, significantly reducing or eliminating the possibility of error while ensuring that device configurations remain correct. There are a number of improvements to a network administrator's operational workflow associated with doing configuration changes through a centralized tool:

- *Reduction of error-prone text manipulation.* The tried-and-true method for updating network device configurations has long been manual through the command line. Adding lines to a device's configuration file through the command line appears easy and requires little more than the knowledge of the proper command and a remote access utility. However, text-based configurations tend to be highly error-prone. With dozens or hundreds of lines of code scrolling by and even the smallest error potentially having a major impact on functionality, it is easy to see how a segregated tool with database storage and offline manipulation goes far in preventing errors.
- *Eliminates the idiosyncrasies of Telnet/SSH.* Most remote console applications that connect to network devices are designed specifically for command-line access and online config manipulation. However, Telnet, SSH, or other protocols commonly used suffer from usability limitations. Scrolling down may be interactively possible, while scrolling up may only be possible by reading back through the tool's command buffer. If you need to look at one part of a configuration while editing another, multiple connections are usually required. The idiosyncrasies of these tools as well as the complex language of network device configurations make them a challenging learning curve for new administrators.

- *Supportability*. It is likely that your network environment is not entirely homogeneous. Network devices from multiple vendors may have different and completely separated mechanisms for configuration. One device's Web-based configuration may require a completely different set of skills than another's command line-based configuration. Leveraging a centralized network configuration management tool gives you a single place to call when problems occur.

Configuration Management's Top 5 Tasks

There are a lot of administrative challenges that can be overcome by moving away from native interfaces towards a common toolset for network configuration management. In this section, we'll look at five of the top tasks that are commonly assigned to the network administrator and how centralized configuration management toolsets enhance the ability to get the job done. For each, you'll find that the move to centralized configuration management also brings about great levels of automation. With the right toolsets and techniques in place, managing five network devices involves the same processes as managing five hundred.

Config Backups

Network devices are unique in IT in that their configurations are typically stored in a text-based format irrespective of the type of device. Working with and managing change within that format is a large part of the learning curve associated with being a network administrator. With essentially all settings being contained within individual text files, the process to back up a device's configuration is as simple as a file copy. Migrating one device's settings to another involves copying a set of files from the old device to the new.

Although the file format itself is easy to work with, the processes by which files are transferred and ultimately backed up off individual devices is less intuitive. With the majority of file-based storage in an IT environment usually being hosted atop Windows servers, the process of simply getting backups to a storage location can be cumbersome. Even more difficult are the necessary scheduled tasks that back up those devices on a regular schedule.

Needed to resolve this inadequacy with native tools is a segregated, centralized configuration management solution that works across all devices and device classes. Once connected to a centralized configuration management server, virtually every function of a network device can then be managed from the server itself. This includes setting up and managing regular device backups, monitoring their success or failure, and later restoring config files to devices in the case of a failure.

Change Documentation and Audit Trails

In an environment in which security needs and compliance regulations mandate the logging of all user and administrator activity, knowing "who did what" is a critical component of a secure IT environment. Network devices have historically enjoyed fairly limited access by IT personnel. Relatively few IT staff members are usually granted access to view and manipulate device configurations. Because of this, the capabilities associated with administrator activity logging at the individual device level have been relatively undeveloped.

Security and regulatory requirements along with the desire to track which administrator made which change drive the need for a greater level of logging. That logging must include at a minimum the administrator who logged in; the time, date, and location of access; and detailed information about the individual configuration change completed. This data also assists with the troubleshooting process in the case where a misconfiguration causes a problem. By identifying the changes made immediately prior to a failure, it is possible to quickly back out those changes to return the environment to normal. An effective configuration management solution will provide audit trails for every activity made by an individual within the system. Particularly effective ones will provide mechanisms for alerting administrators when changes are made.

Implementing Mass Changes

If an issue or a problem in the IT environment requires the update of a router configuration for resolution, making and testing that change requires only a short amount of time. But if the resolution to that issue or problem requires updating configurations on dozens or hundreds of routers, the manual update process could take hours or days. Repeating that update across hundreds of devices also introduces the potential for error, which exacerbates the problem rather than assists.

Centralized configuration management tools are by definition automation enablers. They provide a way to incorporate a change across multiple devices all at once. Effective centralized configuration management tools usually incorporate a database of device configurations taken from the last round of backups. This database houses the actual configurations of all devices across the enterprise. Making a mass change across each of those devices when their configuration is known and stored in a local format enables a mechanism by which the administrator can update every device at once.

This capability grows even more valuable when integrated with fault or performance management features intrinsic to the configuration management tool. Consider the situation where a device misconfiguration trips an alert based on a fault or performance issue. Within the same tool, the network administrator can quickly identify the location of the fault, drill down into the specific configuration problem to find a solution, and push that update to all affected devices. Each of these activities occurs without the need to directly log in and manipulate a single network device.

Identifying Inappropriate Configurations

With large or even moderate numbers of devices in service within an IT environment, it is likely that each device will have specific customizations that are unique to the device. One device will allow certain traffic while another is configured to prevent it. One set of devices is set to route in a particular direction while another set routes in a completely different way. Defining and managing these configurations is one of the biggest tasks of the network administrator.

But even across dozens or hundreds of unique configurations, there are elements of similarity. Each configuration has portions that correspond to the device's configuration template. Finding deviations in those portions and comparing the configuration of one device to another is challenging using native tools. As discussed previously, trying to line up two configuration files in two remote console windows is a painful process at best.

Good configuration management toolsets provide mechanisms by which config file differences between devices can be highlighted for review by an administrator. These differences provide a visual mechanism for the administrator to seek out and fix problems or incorrect configurations. Best-in-class configuration management solutions integrate fault and performance management capabilities into the same toolset. This integration enables a direct linkage between problem occurrence, administrator notification, and suggested resolution.

Network Problem Notification and Remediation

This integration between configuration management and fault and performance management is key to maintaining the highest levels of network uptime. The monitoring and database storage of real-time performance statistics ensures that today's performance is at least as good as yesterday's. Changes in performance can be traced over periods of time and against known configuration changes to identify the problem's source. Fault identification and alerting immediately alerts administrators when devices, services, or even network applications stop responding. And since the system that alerted on the fault is the same that is used to resolve it, that interface can quickly lead the troubleshooting administrator to a suggested resolution.

From Highly Manual to Highly Automated

The right configuration management tools in the hands of network administrators give them the integrated interface they require to best serve the needs of business. Implementing such a system for use by network administrators eliminates the need for manual update tasks and administrator-specific homegrown scripts. With a database-driven backend, automated actions directly initiated from the tool itself, a rich interface for making and applying configuration changes across the board, and granular notifications and alerts, an effective network configuration management solution is a must-have for the proactive IT environment.