SOLARWINDS WHITEPAPER

Top Tasks for Network Device Management

Tips to ensure proper device configuration & adherence to industry best practices

Share:

solarwinds
The Power to Manage IT

Introduction

The process of infrastructure management involves everyday tasks like maintaining existing infrastructure devices. However, in addition to everyday tasks, there's also the planning and execution of new projects like—preparing infrastructure for new sites, IPv6 deployment, upgrading obsolete equipment, and so on. And don't forget, along with all of these tasks is the responsibility to ensure minimum downtime and cost.

Device configuration management is a major part of infrastructure management and takes up a huge amount of the administrator's time. In smaller organizations, manually managing configuration for only a handful of devices is feasible, but in large organizations with hundreds or even thousands of devices, manual device management can become a nightmare. Some typical tasks involved in device configuration management include, device backup, execution of configuration changes, baselining and archival, bulk password changes, compliance policy enforcement, and so. Now imagine having to conduct these tasks manually for a thousand or more devices. The time it would take to do this is incredibly large and the chance of errors occurring is almost certain.

In large networks, automation of device configuration management is the solution to the nightmare of manual processes. Automation not only facilitates saving time and eases efforts, but also helps achieve consistency and most importantly reduces network outages caused by human errors and misconfigurations.

In large networks, automation of device configuration management is the solution to the nightmare of manual processes.

Understanding Configuration Management

Configuration management consists of a series of routine tasks and the common technologies used to execute those tasks. For example, technologies like Telnet, SSH, and TFTP are used to upload/download device configurations, perform IOS updates, execute file transfer commands, and make secure file transfers. There is also SNMP, which helps gather device information by polling for data.

Many organizations employ the use of script translators, either developed in-house or open source tools, to aid in converting manual CLI based

commands to automated configuration commands. With this approach, all device information collected has to be stored in a common database for easy accessibility. This accessibility is commonly achieved through standard, relational, and searchable databases. To help take the load off the administrator, some organizations also utilize systems that trigger alerts, schedule repetitive jobs, or offer some type of automation.

Here are three of the most common approaches to configuration management:

1. Manual
    - Works for very small environments—less than 20 devices
    - Falls apart quickly with increase in devices, distributed devices, or when the administrator leaves the company
    - Normally accomplished by one individual
    - When the individual responsible for configuration management leaves, the organization is left stranded
2. Patchwork
    - Scripts developed in-house
    - Open source or free tools
    - Point solution tools—many fragments to manage
3. Comprehensive Configuration Management System
    - Automation
    - Efficiency
    - Consistency
    - Security
    - Scalability

If your organization decides to use a configuration management system, keep in mind that the solution you choose should offer automation and multi-vendor support. Also ensure that it is flexible, secure, and reliable.

More than 65% of the network environments were multi-vendor (Cisco ® and a mix of other vendors) in nature.

- SW Survey[2014]

Top Tasks for Network Device Management

Network device management need not be frustrating if the right method and best practices are followed. Listed below are some top best practices for effective device management.

1. Backup Device Configurations

Not having a backup of configurations for your network infrastructure devices, specifically your routers, switches and firewalls, is putting your network at risk. In a network, there are many occasions when a faulty/failed device has to be quickly replaced or a typo in a configuration change like an ACL change or route change causes network downtime. In such cases, you can reduce downtime by quickly replacing the configuration from an archive.

Efficient device management starts with backing up all your device configurations regularly. To achieve this, you can either manually telnet into each device and download the configuration or automate the task by using a tool.

The benefits of using a tool are:

- Automated, periodic backups to secure storage
- Centralized storage for fast recovery/restore
- User based access
- Secure transfer—SSH Options

2. Execute Bulk Configuration Changes

There are some instances when the password for all devices needs to be changed. This could be a case where an employee with access to critical devices leaves the organization, or when password change activity is required to adhere to the 90-day password change policy. Accomplishing this task manually may take days to complete in a large network.

In this scenario, the smart approach would be to push out configuration changes in mass and in a scalable way. To do this, some administrators use scripts developed in Perl, VB, or one of many other platforms used to automate repetitive tasks on multiple devices. Many

Quick Tip

How to Replace a Failed Device, In No Time!

80% of companies experience revenue loss due to network outages; losing around $140,000 per incident on an average - Avaya Survey

administrators are still using this common method today. However, executing bulk configuration changes with an automation tool helps eliminate human error and automatically pushes changes out in a broader way.

Some of the main advantages of using an automation tool include:

- Automatic push for changes to multiple devices
- Create controlled push schedules
- Eliminate human error
- Quickly rollback to previous configuration in case something goes wrong

3. Track & Alert Device Configuration Changes

The administrator responsible for the network must be aware of all changes made within their network. They're required to find a way to keep track of who makes what change and when. It's also important to ensure that all changes are compliant with internal and external policies. These tasks can be accomplished by setting up a syslog server and monitoring the syslog messages or traps. Critical routers and switches can be set up to automatically send syslog messages or traps to notify on instances like configuration changes being made, someone telnetting or SSHing into the device, or a configuration being saved.

These tasks can become much easier with an automated tool. An automated tool will not only help detect the change but also easily download the configuration with changes highlighted. It also allows the admin to automatically rollback to the previous configuration if required.

In short, an automated tool helps:

- Catch unauthorized or bad changes
- Maintain policy compliance
- Detect unauthorized access
- Find problematic configuration changes quickly
- Validate if procedures are being followed

Quick Tip

How To Quickly Recover From a Configuration Error.

4. Maintain Device Inventory List

Managing devices from an infrastructure perspective is a tough job in itself, but on top of that is the responsibility to maintain a device list complete with serial numbers, chassis ids, IOS versions, and so on. These inventory reports are necessary when it comes to renewing your device maintenance contracts.

Maintaining all your device information manually in a document like a spreadsheet is a difficult job to undertake. It's also not easy to write a script that collects this information and there are currently no open source solutions available for this task. Most automated configuration management solutions come with device inventory reporting features.

Many of these features allow you to:

- Control maintenance contract costs
- Know what device you have and where
- Track and report for end-of-life or scheduled refresh cycles
- Budget with improved accuracy
- Improve security—Is there a new device connected you should know about?

5. Adhere to Compliance Policies

All organizations are required to comply with internal and external policies. These policies play an important role in security, especially the security of critical devices like firewalls, edge routers, and switches. It's mandatory to confirm that these critical devices adhere to compliance policies set by the organization.

To monitor current device status, and continually maintain compliance over time, there needs to be a process or system in place for taking inventory of devices and generating reports on policy violations. Based on the reports generated, organizations should take remediation actions to correct non-conformances. Adhering to compliance policies manually for a large number of devices is next to impossible. Here again, an automated tool is the best option.

Quick Tip

60% of participants felt the need to switch from manual Network Configuration and Change Management to an automated tool.

- SW Survey [2014]

Automated tools help you easily:

- Enforce HIPPA, SOX, DISA, STIG, FISMA, PCI, Custom Policies
- Avoid costly penalties for non-compliance or no verification
- Detect and remediate policy violations
- Maintain common compliance elements including SNMP community strings, password strength, SNMP public, ACL permissions, forbidden protocols, and user access

6. Regularly Change SNMP Community Strings & Passwords

Just as users change their system passwords regularly, the same rule applies to network devices. To enhance security and comply with policies, it's good practice to rotate your SNMP community strings every 30-60 days. To do this manually, you would create templates for commonly executed changes and store them in a common repository for easy access.

Most configuration and change management tools provide:

- Execution of complex configuration changes through a simple wizard-like interface
- Access to standard and tested templates from a shared repository
- Automated and bulk execution of repetitive tasks
- Avoidance of typos in the configuration while executing bulk tasks

7. Update Device IOS/Firmware

In a multi-vendor environment, it's difficult to keep track of required IOS/ firmware updates for all devices. Individual vendors regularly release patches for security vulnerabilities. When this occurs, it's difficult to manually determine which of your devices are vulnerable and require the patch. Even if you maintain an updated inventory list, complete with IOS version details, it's still a daunting task to physically track and then upload updates to each device through a TFTP server.

Quick Tip

Use tested and verified configuration change scripts and device templates from thwack

How does an automated tool help ease this process?

- Quickly search and identify devices that need to be patched
- Save time and easily perform bulk updates on multiple devices
- Upload and download IOS images, scheduled or real-time, with a built-in TFTP server

8. Develop and Deploy Standardized Device Configurations

It's best practice to standardize configurations across all devices. This can be accomplished with tools that detect deviations from baselines and send alerts when they occur. Reduce efforts by creating standardized and reusable device profiles that define access attributes like connection type, ID, password, etc. To decrease errors and save time, you can deploy similar configurations in bulk and automate the configuration change process.

Advantages of using an automated tool for this task are:

- Eliminate complexity, improve standardization, and reduce human error
- Quickly configure devices and reduce deployment time

These are some of the best practices to ensure proper device configuration and management in your organization. Efficient management along with compliance to these best practices helps protect your network from unnecessary network downtime. However, before any configuration change, whether manually or using a tool, it's always advised to take a full backup of configurations and schedule device configuration activities during off-business hours.

Automatic Device Configuration Backup, Configuration Comparisons & Rollback, Multi-vendor Device Support, and Real-time Configuration Change Alerting were identified as MUST HAVE features

- SW Survey [2014]

SolarWinds® Network Configuration Manager (NCM) is our automated network change and configuration management solution that you can try free for 30 days. With SolarWinds NCM, you can take a full backup of all your configurations, record inventory details for all devices in the network, check for policy compliance and remediate violations, check and upgrade firmware, execute required bulk pushes, and more.

Learn More:

1. Whitepaper
   - Why Every IT Practitioner Should Care About Network Change & Configuration Management
2. Tech Tip
   - Automate Configuration Management with SolarWinds NCM
3. Video
   - 5 Best Practices: Network Configuration Management

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with *unexpected simplicity* through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, **thwack®**, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at **http://www.solarwinds.com/.**

For product information or to purchase SolarWinds products, visit solarwinds.com, or reach out to us at:

Americas

Phone: 866.530.8100

Fax: 512.857.0125

Email: **sales@solarwinds.com**

APAC

Tel : +65 6593 7600

Fax : +65 6593 7601

Email: **sales@solarwinds.com**

EMEA

Phone: +353 21 5002900

Fax: +353 212 380 232

Email: **sales@solarwinds.com**

3711 South MoPac Expressway, Building Two, Austin, Texas 78746