SOLARWINDS TECH TIPS

How to Eliminate the No: 1 Cause of Network Downtime

Learn about the challenges with configuration management, solutions, and best practices

Share:

solarwinds
Unexpected Simplicity™

“Through 2015, 80% of outages impacting mission-critical services will be caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues.”

- Gartner RAS Core Research Note, Ronni J. Colville, George Spafford

Configuration errors are the major cause of network incidents resulting in downtime. Studies show that over 80% of network problems are due to improper configuration and change management. These mistakes are costly and can lead to loss of confidential data or business disruption. To prevent configuration errors while still maintaining compliance to standards, it’s recommended to implement proven best practices.

This document takes you through some of these best practices and shows you how they can aid in building better network configuration and change control for your overall IT management. By eliminating network configuration errors, you can quickly drive impactful changes at your organization that will improve network availability.

Need for Configuration Change Management and Control

Implementing a process for configuration change management is one of the best practices recommended by various regulatory and industry standards. Security compliance standards like DISA (Defense Information Systems Agency), STIG (Security Technical Implementation Guide), FISMA (Federal Implementation Security Management Act) and HIPAA (Health Insurance Portability and Accountability Act) require the implementation of certain policies and procedures to protect your devices and your network. Each of these standards emphasize that implementing change management is critical and important. Additionally, the PCI (Payment Card Industry) standard requires that every change has to be documented.

No matter what industry you belong to, be it government or commercial, small or big, networks are vital and downtime has a significant impact on business operations. Organizations and their missions are heavily dependent on network availability, meaning it’s vital to ensure that you protect your network from unauthorized changes that affect security, efficiency, and compliance.

Challenges in Configuration Management

Why is network configuration so error-prone? And why is it important to track, review, prioritize, and double check network configuration changes? As networks become more complex, configurations also become more complex. For example, when an administrator has to make a configuration change to a ten-page access control list that controls the security of firewalls and routers, there is a high likelihood that and error will be made. Digging through pages and pages of complicated information is a very error-prone process. Making a mistake may lead to cutting access to a mission critical application or isolating a remote site. If you’re a service provider, uncontrolled configuration changes can make a negative impact on your network uptime and SLAs (Service Level Agreements). Some factors responsible for erroneous configuration changes are:

- **Heterogeneous Environment:** Networks today are made up of many device types and models from different vendors. There’s a lack of standardization because every configuration looks different and behaves differently. It’s difficult to set a standard template for all devices in the network.
- **Complexity:** Devices are complex and administrators need advanced skills to be able to handle complex configurations. Manual methods are not scalable and the lack of automation methods leads to many human errors.
- **Use of Command Line Interface (CLI):** CLI is the primary mode of device administration and administrators frequently use CLI to create and modify configurations. However, CLI is not easy to use and is error-prone.
- **Single Device Administration Model:** Each device is managed separately making it difficult to visualize the impact of a change from an end-to-end perspective. For example, when there is a change on a router or firewall, it’s nearly impossible to completely understand its effect on the rest of the network. Per-device-management prevents you from having an end-to-end perception of the devices that are impacted by a change.

Network administrators widely use the difficult and error-prone CLI administration method. Some common IOS mistakes include:

- Password reset verification
- Incorrect use of wildcard masks
- Confusion over when to use the Clock Rate vs Bandwidth commands
- Not configuring remote management to use SSH vs Telnet (default)
- Incorrect Ethernet duplex settings
- Confusion over when to use Process-ID vs ASN (autonomous system number)
- Configuring EIGRP auto-summary (defaults changed)
- Configuring split horizon (default settings changed)
- Failure to change default (unsecure) SNMP settings
- Properly configuring switch port security

Best Practices for Network Configuration and Change Control

1. **Inventory and profile network systems**: It's critical to know exactly what you're managing. List the number of devices per vendor and record device details. Having this information along with device end-of-life and end-of-support information is helpful when renewing maintenance contracts with vendors or preparing budgets for device replacement. Device inventory supports network configuration and change control, and therefore is essential to network operations. Classify devices into groups for easy manageability and repeatability, i.e. create configuration templates that can be re-used or modified for many devices. Having a solid inventory is a major step towards sound configuration management.

   Objective: Identify all network devices under management

   - Use network discovery to identify and map network nodes
   - Organize nodes into management groups

   - Create custom node attributes
   - Associate key end-of-life dates with devices

2. **Develop and deploy standardized device configurations**: Try to standardize configurations across all devices. This can be accomplished with tools that detect deviations from baselines and send alerts when deviations occur. Deploy similar configurations in bulk in order to reduce errors and save time.

   Objective: Reduce errors by improving consistency and standardization across device configurations

   - Use standard access properties (e.g. protocols, ports, IDs and passwords)
   - Use configuration templates to build standardize configuration tasks
   - Use bulk deploy to push changes out to devices

3. **Protect configurations against changes**: If you’re in charge of network and router configurations, you need to know if anyone makes an unauthorized change and when it occurs. Use a tool that can notify you in real-time when these changes occur. You should also have the option to go back and see a history of configurations and then revert to or load a previous version of a good configuration.

   Objective: Protect stable configurations from an unauthorized change or catastrophic device failure.

   - Backup device configurations for failsafe restores
   - Monitor device configurations in real-time for unintended changes and respond immediately
   - Use tools to identify specific changes to a configuration
   - Maintain a change audit trail to always know who made changes

4. **Audit configurations for compliance to standards**: Having the right tool can save you hours and hours when preparing reports for an audit. Every organization has its own list of standards

to apply. It takes a lot of discipline and manual effort to ensure that these standards are efficiently implemented.

Objective: Policy compliance

- Assess configurations against organization risk, industry regulatory, and best practice standards
- Create or modify compliance rules to reflect internal best practices

5. **Use change control to manage updates**: With a second pair of eyes to review configurations you'll be able to find mistakes that could have been missed. Have configuration baselines set and ensure a proper workflow for accountability.

   Objective: Keep configurations protected while adapting to evolving organization needs.

   - Create configuration baselines
   - Use automation to perform routine tasks
   - Use workflow to ensure proper change request review and approval
   - Track and manage device end-of-life

Using these network configuration and change management best practices you'll be able to minimize network disruption and deliver impactful benefits like:

- Improved network MTBF and MTTR
- Improved network security and compliance
- Increased standardization and efficiency
- Improved operation efficiencies and margins

What Do You Need from a Configuration Management Tool?

The top four use cases for a network configuration management tool are:

- **Know and protect working configurations:** Every administrator needs to know what he is managing. Having a process, tool, or product that will furnish device information makes this task much easier. Automated methods give you an inventory of devices in the network and help retrieve configuration for these devices so that you can store them as a backup. So, if something goes wrong and the reason is an unauthorized configuration change, you can use this configuration to restore and revert to a previous stable configuration.

- **Know what changed when:** It's important to record the configuration changes made so that in case of an issue, you can easily identify and correlate events. If a network problem occurs after a configuration change was made, you can quickly identify the change as the cause of the issue and replace the faulty configuration to fix things. It's also a good idea to have a tool that helps put both configurations side by side for an on-screen comparison to analyze the problem.
- **Know when configurations are not compliant with standards or best practices** - DISA STIG, NIST/FISMA, and HIPAA - are some of the standards that organizations follow depending on their line of business and operations. These standards are becoming more and more ubiquitous as is company regulation to comply with them. From time to time, network administrators are faced to show documentation to auditors and prove compliance to standards. Automated reports save a lot of time in preparing for these audits. Being able to detect when these configurations become non-compliant, or even get recommendations on policies, is a requirement to effectively implement compliance policies.
- **Reduce the time taken to recover from problematic changes or catastrophic device failure:** This is of utmost importance and the critical task here is being able to maintain regular backups of configurations and store them for later use. You should be able to schedule backup jobs that can automatically run and then use it to fix a bad configuration change whenever required.

How SolarWinds® Can Help

SolarWinds Network Configuration Manager (NCM) is an efficient configuration management and change control tool. NCM provides a single-pane-of-glass view on the three building blocks of IT management, i.e. **configuration**, **performance**, and **fault management.**

For example, imagine you see a reduction in the performance of a particular device and NCM notifies you that a configuration change made. When this occurs, you can correlate the information to identify that this change impacted the performance of the device. You can then retrieve the previous configuration from the archive and compare side-by-side to see the differences and then rectify errors.

Key Benefits of SolarWinds Network Configuration Manager

- **Automatically discover and import devices** into the NCM database regardless of vendor. No manual effort is required to individually add devices to be managed.
- **Quickly fix a bad configuration change** by replacing a known good configuration from a backup. You can easily schedule automatic backup jobs as required and maintain an archival history of baselines and stable configurations.
- **Monitor unauthorized and erroneous changes to quickly fix network issues** and reduce downtime. Be notified every time a configuration change is made.
- **Easily prepare reports for capital budget forecasts and device replacement plans**. Maintain device inventory details and record end-of-sale and end-of-life dates for your Cisco® and Juniper® devices.
- **Save time and reduce errors** by automating and executing bulk configuration changes on real-time or as scheduled tasks.
- **Effectively implement security, risk, and regulatory controls.** Create policies and be alerted on policy violations.

Use NCM to bring down the number of network configuration errors and reduce network downtime caused due to erroneous and unauthorized configuration changes.

LEARN MORE »   DOWNLOAD FREE TRIAL

References

Gartner RAS Core Research Note, Ronni J. Colville, George Spafford:
http://img2.insight.com/graphics/no/info2/insight_art6.pdf

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many 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 at http://www.solarwinds.com.

solarwinds
Unexpected Simplicity™