ManageEngine

EBOOK

5 WAYS TO ENSURE BUSINESS CONTINUITY IN THE WAKE OF NETWORK DISASTERS

A guide to efficient network disaster recovery plan.

-Arjun Premkumar

Introduction

It's common knowledge that managing networks isn't easy. However, some people might not know that many minor inconveniences faced in work environments can be traced back to a network issue. At first glance, many of the everyday IT problems might look like a bunch of random, unfortunate events that could happen any day at work. But it's possible that all of these random issues are connected.

As a network admin, you need to understand that many IT issues can be narrowed down to something like a single faulty modification made to a device or a vulnerability left on an unchecked device. Only after fully analyzing your network and identifying any existing loopholes can you fix an issue and restore your network to complete operational status.

Managing a disaster-free network requires various segments of your network infrastructure to be maintained and scrutinized. However, approaching this work manually is a surefire way of encountering a network outage. This e-book will outline a few ways in which an outage or network disruption can occur and how Network Configuration Manager, a configuration management tool, can help.

A bandwidth hog in the network

Organizations often invest a lot of money into acquiring large amounts of bandwidth for their business-critical applications. This bandwidth is usually shared among every user in the company's network. When someone in the network uses an application that consumes a large amount of bandwidth, it might make the network unavailable to the other users in the network. If the application in question is being used for non-business activities, it brings down the ROI for the organization's allocated bandwidth budget.

In order to solve this, manually looking into each user's bandwidth consumption isn't the best thing to do when you're already pressed for time to fix a network issue. Instead, you should be putting a cap on how much bandwidth every user can use. Doing so will ensure your organization's bandwidth is evenly distributed among every user and that the overall productivity of your organization doesn't take a hit when a single user consumes an inordinate amount of bandwidth.

According to British IT security company Sophos' global survey entitled The Dirty Secrets of Network Firewalls, "On average, 45% of network traffic is going unidentified. As a result, it cannot be controlled."

Limiting bandwidth for each user can be achieved with access control lists (ACLs). ACLs can be used to control how much bandwidth each IP address can consume. You can restrict the bandwidth consumption of multiple devices in your office by creating and executing an ACL configlet with Network Configuration Manager. This configlet should specify the bandwidth limit for each IP address. If needed, you can also block certain IPs from accessing your network, allowing users to experience a hassle-free connection.

A violation of industry standards

In the network industry, certain standards have been laid out to prevent network devices from becoming vulnerable. Any violation to these standards could lead to issues like data breaches, outages, and loss of reputation to the business. This is why when network admins are making changes to their network, they have to keep in mind that their organization's devices must be compliant to all of these standards. PCI DSS, HIPAA, SOX, and CiscoIOS policy are some of the most important standards that need to be adhered to. When you want your network devices to adhere to some additional rules that aren't present in the previously

mentioned policies, you can create a custom compliance policy with Network Configuration Manager.

According to a Newscycle Solutions Survey, "An in-depth March 2015 PCI Compliance study by Verizon found that 80% of businesses fail their first PCI compliance assessment."

For example, a general recommendation from the network industry is to avoid using TELNET. This is because unlike other communication protocols, TELNET isn't encrypted, making it highly insecure. This lack of security in the protocol makes devices using it vulnerable to hacks, which will eventually lead to a network outage. You should be instantly notified if someone enables TELNET in your enterprise network, which is where compliance checks become life savers.

Performing regular compliance checks will help you get better visibility into devices on your network and identify the ones that violate established policies. With Network Configuration Manager, you can run compliance checks on the devices associated to each policy. Alternatively, you can choose to run ad hoc tests on devices that are suspected to be vulnerable.

You can also create custom compliance policies as a preventive measure against network outages that occur because the TELNET protocol is enabled. This custom policy must include a rule that checks for devices that have TELNET disabled. When compliance checks are run for this policy, any devices that use TELNET will be identified, allowing you to quickly remediate the situation. Fixing a violation like this normally means you'd have to search through a huge list of configlets and then execute the right one. With Network Configuration Manager, however, you can instead associate each rule with a remediation configlet. Whenever a violation is identified, all you'd have to do is run the predefined remediation configlet, and Network Configuration Manager will take care of the rest.

A change gone wrong

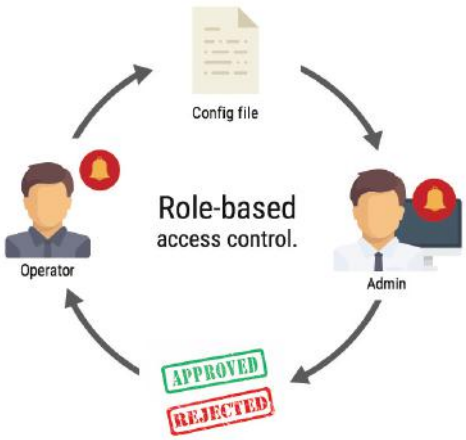
As a business grows, so does its business needs. To accommodate these ever-growing needs, network admins should make changes to the network device configurations on a daily basis, but doing so can create loopholes. These loopholes become a gateway that can cause vulnerabilities, eventually leading to productivity loss and performance degradation. One of the common mishaps

that occur during network change implementation is shutting down interfaces. Shutting down an interface can render a group of devices on the network inaccessible, causing users to be disconnected from the network. Prevent mission-critical applications from disconnecting by integrating change notifications, role-based access control, and a rollback mechanism for configurations into your change workflow. Let's quickly go through how each of these work.

Change notifications alert admins whenever an operator has requested to change or upload configurations to specific devices on the network, allowing admins to approve or disapprove these changes at will. These notifications also allow the operator who requested the change to receive an alert when their requests are processed.

For critical devices that you want to prevent operators from making irreparable changes to, the best approach would be to configure a rollback mechanism. A rollback mechanism can be configured to bring a device's configuration back to either a previous version or to its baseline configuration. The baseline configuration is often the most stable configuration and reverting to it typically helps in network recovery and reducing productivity loss.

Dunn & Bradstreet claim that 59 percent of Fortune 500 companies experience a minimum of 1.6 hours of downtime per week, which equates to a weekly cost of $896,000 for lost labor alone.



Network Configuration Manager has user management and role-based access control to aid in change management. User management gives you a look into each user's log info and provides you the option to add or delete users, as well as set their scope of access. Scope of access must be set according to what device group the user typically deals with. For example, if a user should only deal with Cisco devices, their scope of access can be restricted to that device group alone. Network Configuration Manager comes with predefined access levels that dictate the scope of each user by defining the actions permissible to those users.

With role-based access in place, you'll receive notifications every time a configuration upload is requested by an operator. If at any point it seems like an approved set of changes is disrupting your network's function, you can instantly roll the device back to a baseline configuration. Rolling a device configuration back to a trusted version should make the network instantly recover, which will help your organization achieve business continuity.

Loss of changes made to network devices

As we've seen earlier, many businesses require frequent network changes to cater to their growing needs. Any change made to a device is applied to the running configuration of the device; which means these changes have to be written on to the startup configuration to avoid having the changes be erased due to power loss or a reboot.

Let's say a network admin creates policies that enable routers to access the internet through the service provider. While updating these configurations, the admin forgets to write these changes over the startup configuration. The admin comes in the next day only to realize that there was a power outage that caused the devices to reboot. This outage resulted in the changes being lost and several users experienced downtime due to loss of connectivity. Had the admin synced these startup and running configurations immediately after implementing them, they could've retained all of the changes after the power outage and prevented any downtime.

According to a study by University of California, Irvine, it often takes an average of 23 minutes to refocus and get your head back in the game after an interruption.

The process of syncing configurations is made a whole lot simpler with Network Configuration Manager. Network Configuration Manager gives you a look into all the devices on your network that don't have their startup and running configurations in sync. You can choose to either look at a report to see every device that has a conflict or view each device's status from the inventory list. Not only does the inventory list give you information about which devices have a configuration conflict but it also allows you to sync configurations. Configuration syncs can also be scheduled from the inventory to occur monthly, weekly, daily, or just once.

A hardware failure

While we've seen how configuration changes can disrupt a network, it's equally important to look into some key hardware aspects of network devices. A device that has become obsolete can do as much damage as a faulty configuration change or a compliance violation. End of support, end of sale, and end of life are some of the factors that a network admin has to seriously consider when it comes to managing their network devices. But on a network that includes hundreds of network devices, it's incredibly difficult for an admin to keep track of such information.

End of support (EOS)	End of sale (EOS)	End of life (EOL)
◆ End of support is when all technical assistance for a product is discontinued from a vendor.	◆ End of sale is when a vendor stops selling a product.	◆ End of life is when a product has reached the end of its useful lifespan.
◆ Using unsupported devices puts a network at risk due to a lack of new security updates.	◆ Replacement parts often continue to be sold, so using such devices often occurs.	◆ These devices are usually obsolete, so using them is strongly discouraged.
◆ An admin can sometimes choose to purchase extended support, but this is expensive in most cases.	◆ These devices can also be purchased from third parties, but doing so comes with the risk of being sold faulty or counterfeit devices.	◆ Admins must decommission these devices before they can cause any security or performance issues.

Network Configuration Manager comes with built-in EOL/EOS reports that an admin can use both for creating records and auditing purposes. Network Configuration Manager matches SysOIDs with the dates given by each vendor and automatically populates the reports with each device's EOL/EOS dates. If the reports do not carry the dates for a device, an admin can request an end of life, end of support, or end of sale update from the Network Configuration Manager support team.

According to a white paper by Avaya's emergency recovery expert Joey Fister, "52% of the network outages happen due to hardware failure."

Replacing a device when hardware failure occurs can be quite simple if the admin had a repository of device backups. With Network Configuration Manager, taking device backups is made a whole lot simpler. You can perform both manual and scheduled backups with Network Configuration Manager. Once you've created a repository of backups for all of your devices' configurations, you'll be confident in replacing an old device with a new one. Whenever you need to upload a new configuration file to a device, you can choose one from the database. Also, the backup option isn't limited to configuration files, you can choose to backup entire databases with Network Configuration Manager.

Recovering from network disasters

With all that said, sometimes disasters are inevitable. Being prepared to resolve a disaster is just as important as preventing one. That is why every business, irrespective of its size or industry, needs to have an efficient disaster recovery plan. A well-organized network disaster recovery plan must include recovery mechanisms and enhanced device security for ensuring business continuity. Any application that is responsible for the successful execution of your plan must be able to prevent, predict, and mitigate disasters. Network Configuration Manager is one such tool, as it adopts a holistic approach for ensuring that your network is well-protected and remains resilient against network disasters. Don't take any risks with your network—execute a foolproof network disaster recovery plan now.

Interested in learning how to apply these to your network? Register here and get a free demo of Network Configuration Manager from our technical experts.

Get hands-on experience of an efficient Network Disaster Management tool. Download Network Configuration Manager with a fully-functional trial license.