ManageEngine
OpManager

FREE E-BOOK

11 BEST PRACTICES TO SAVE YOUR BUSINESS FROM NETWORK PITFALLS

Network administration best practices guide

-Vignesh Karthikeyan

WWW.OPMANAGER.COM

Table of contents

Introduction

- For Quora, Business Insider, Giphy, and many other websites, February 18, 2017 was just another normal day - that is, until their services stopped responding. The reason? These sites used Amazon S3, a popular cloud-based service, which suddenly experienced a five-hour long outage that was so severe even Amazon couldn't update its own AWS status dashboard.

- In May 2017, 75,000 passengers of a globally reputed airline were left stranded - not for a few hours, but for three whole days. A record 726 flights were cancelled and the airline reportedly suffered a financial loss of £80 million, along with a damaged reputation.

- Back in April 2011, a Georgian woman rendered the entire country of Armenia internet-less for five hours when she accidentally damaged a copper cable while searching for scrap metal.

What do all the above examples have in common? They were all instances of network downtime that caused millions of dollars in losses. Just the mention of downtime can bring shivers to customers, management boards, and network administrators alike.

Poor strategy planning, a haphazard hiring process, and management that makes all the wrong decisions — all of these factors are capable of bringing even a successful business down. However, there's one issue that's cause for even greater concern than these : inefficient network management. What the rest of these business concerns could take months or even years to accomplish, poor network management could do in a few seconds.

This e-book presents 11 best practices for network management to help you prevent network downtime as well as other potential losses arising from inefficient network management.

Best Practice #1

REMOVE ALL BUILT-IN CONFIGURATIONS AND RECONFIGURE EVERY DEVICE IN THE NETWORK FROM SCRATCH

Every network device comes with a list of default configurations. While most network administrators remove these existing configurations and reconfigure them for the essential parameters, they tend to skip parameters that aren't required for their network ecosystem. These parameters which are deemed unimportant continue to have default credentials and configurations, turning them into a huge security vulnerability.

Not-so-fun fact: Eighty percent of data breaches in organizations happen as a result of using poor or default credentials.

Consider a critical parameter whose configuration is unchanged because it's not used in the organization. It provides an easy way for external intrusion into the network, leaving the organization's entire network exposed. You need to remove all default device configurations— no "admin," "password," or combination of those credentials allowed, even for configurations you're not using.

IMPORTANT STEPS TO ENSURE DEVICE SECURITY IN NETWORK MANAGEMENT

1. When adding a new device to the network, ensure all the default configurations that come with the device are reconfigured - even the configurations that you are not going to use.
2. Don't allow dictionary credentials for any device configuration, not even for unused configurations.
3. Change the credentials periodically, and not just for the configurations that are used in your network, but also for the unused ones.
4. Enforce a strong password policy to implement points 2 and 3.

Best Practice #2

CHOOSE THE RIGHT PARAMETERS FOR MONITORING BASED ON DEVICE TYPE AND CRITICALITY

Monitoring all the important devices and interfaces in your network is definitely key to protecting your business from network-related pitfalls. However, you need to consider one other important factor: which parameters to monitor for each device and interface.

Not all devices require all parameters to be monitored, and not every parameter that you monitor for a device is important. You need to decide on the right combination of parameters to monitor for each device in your network.

WHAT'S YOUR MONITORING INTERVAL?

Another important factor that contributes to effective network monitoring is the monitoring interval. Keep this interval short for critical devices and parameters, and increase it as you go down the hierarchy of criticality

Two factors must be taken into account when deciding which parameters to monitor in a device:

- **The criticality of the device:** Primary servers and other critical devices must have all their parameters monitored. If a device is less critical, such as a printer or test device, you can monitor the most basic parameters that will only tell you whether the device or interface is working or not. This will reduce the unnecessary load on your management software and reduce traffic in the network.

- **Device type:** Different device types have different basic parameters that must be monitored. For example, temperature is an essential parameter for a CPU since a steep rise in temperature is an indication that the CPU is being overused.

Use the steps below to figure out which parameters you should monitor:

- Create a priority list by categorizing every device in your network in decreasing order of criticality. Classify them as highly critical, medium, and less critical.
- For critical devices, monitor all parameters.
- For medium devices, monitor the essential parameters plus a few additional parameters depending on the device type and vendor.
- For less critical devices (e.g. test or dummy devices), monitor only the basic parameters that will provide info about the status of the device.

Best Practice #3

MONITOR THE INTERFACES IN YOUR NETWORK WITH AS MUCH IMPORTANCE AS THE DEVICES

The general definition of network monitoring is **monitoring the devices in a network to prevent downtime and potential business losses.** Most network administrators stick to this definition and only monitor the devices in their network.

Not-so-fun fact: Issues in device interfaces contribute to 25 percent of all major downtime

But here's the catch: Device failure or network faults need not necessarily occur only due to faults in devices. Sometimes the problem might occur in the interfaces that connect the devices with one another, and that's why it's important to monitor interfaces with as much importance as the devices in your network.

Most of today's monitoring tools come with templates for vendor-specific interfaces. Leverage them to get in-depth analysis of the performance of the interfaces in your network.

Don't limit interface monitoring to just checking if an interface is running or not using periodic polling.**Set thresholds for interfaces in your network monitoring tool to get alerts when the parameters of the interfaces exceed the threshold values.**

Be sure to keep an eye on all the important interfaces in your network like Ethx for Linux devices; loopback, ethernet, and uplink for routers and switches; and fibre channel and loopback for storage devices. You would especially want to watch the interfaces connected to the devices that are monitored by your monitoring tool, and monitor them for performance and warning signs of potential trouble. You might want to limit the monitoring parameters for the interfaces that are connected to less critical devices, but ensure that your monitoring tool covers all the important interfaces in your network.

Ensure that the upgrades and changes you make to any of your interfaces are updated in your monitoring tool. This will go a long way in preventing your network from running into trouble due to malfunctioning interfaces.

Best Practice #4

MONITOR FOR SYMPTOMS, NOT PROBLEMS

The goal of network monitoring is to prevent the network from going into network faults or unplanned downtime that might result in a business outage. Most network administrators set up network monitoring tools to monitor for problems in their network such as a server outage or a down network switch.

The trouble with monitoring for problems in a network is that the problem in itself is an effect and not a cause.

To be more precise, every time your network experiences an issue (such as network downtime or lack of accessibility to certain devices), chances are that the issue

didn't jump out of the blue. It's likely that a series of incidents which happened before the issue led to the final problem. If these incidents (triggers) are identified and spotted early, you can take appropriate remedial measures and in most cases, stop these symptoms from turning into the final problem. The monitoring-for-symptoms methodology is a much more proactive approach to network management

How do you monitor for symptoms?

- Set multiple thresholds: Most monitoring tools let you set multiple alert thresholds which can be used to alert you well in advance. Use that feature to set up multiple thresholds for critical devices and parameters.
- Analyze, analyze, analyze: Maintain a history of alerts and analyze them. Search for patterns, especially in reoccurring alerts. There's a high possibility that patterns might point to a common root cause that may have been missed.

Best Practice #5

EFFECTIVELY GROUP DEVICES AND AUTOMATE THE TASK OF ASSOCIATING CERTAIN MONITORS WHILE ADDING A DEVICE TO YOUR MONITORING TOOL

The goal of network monitoring is to prevent the network from going into network faults or unplanned downtime that might result in a business outage. Most network administrators set up network monitoring tools to monitor for problems in their network such as a server outage or a down network switch.

The art of efficient device grouping, if mastered, will provide the following advantages:

- Makes device monitoring and maintenance easier.
- Makes bulk configuration changes and device updates easier.

- Grouping devices based on specific parameters helps in diving deeper into the analysis of network performance.

You need to have multiple groups based on different parameters such as device type, vendor, and high bandwidth consumption. Classify each device under multiple groups for better understanding of device performance.

For example, a Cisco server might be put under the categories of server (device type), Cisco (vendor), and high bandwidth consumption (a custom category that enables you to manage the network better). This kind of classification makes it easier to install updates and perform selective configuration changes.

Every device that's added to the monitoring tool needs certain essential monitors. These monitors track specific basic parameters to offer essential information on the device's status and performance.

Automating the process of enabling these essential monitors for devices while adding a device to the monitoring tool will save a lot of manual effort and time.

You can create pre-rules in your monitoring tool to automatically enable select monitors when a particular type of device is discovered. This, however, depends on the tool that you use for network monitoring; most tools support automation, but a few free tools and basic versions do not provide support for automating tasks.

Best Practice #6

USE SYSLOGS AND TRAPS TO YOUR ADVANTAGE

Syslogs and traps are information sent by a device to the monitoring tool. Unlike other data the monitoring tool fetches by periodically polling devices, syslogs and traps are automatically sent by a device to the monitoring tool.

What can syslogs and traps do to improve the efficiency of your network monitoring?

Most parameters and devices in a network are monitored through periodic polling in which the monitoring tool polls the device in a particular interval to check its status. The problem with this technique is that

- Not all device faults are visible during periodic polling.
- The alert notifications for certain faults need to be triggered immediately when they happen. This cannot be done in periodic polling.

For example, consider a situation where your monitoring tool polls a device for its availability every two minutes. The graphical data you'd see on your monitoring tool would be the status of the device in the second minute, fourth minute, and so on. Now suppose that the device goes down in the third minute and comes back up half a minute later. The processing in your network for that half a minute wouldn't have happened, and yet the graph in your monitoring tool wouldn't show even the slightest traces of that downtime ever happening, let alone its impact.

What would you do in a situation like this? This is where syslogs and traps come into play. When downtime happened in the third minute, the device would have sent the monitoring tool a trap and the syslog information would have recorded that the system stopped functioning.

You can use these traps and syslog messages to your advantage by configuring your network monitoring tool to issue an alert whenever such a trap is received or the syslog received contains an error message.

By configuring your network monitoring tool to leverage the data provided by syslogs and traps, you can catch errors that you might have otherwise missed.

Best Practice #7

THE DEVICES YOU AREN'T MONITORING ARE JUST AS IMPORTANT AS THE ONES YOU ARE

Most network administrators do not monitor every single device. They either monitor only critical devices, or at least leave the non-critical out of the scope of the monitoring tool. The reason is that licensing for most monitoring tools is based on the number of devices being monitored, and hence it's a common opinion that adding non-critical devices will unnecessarily add to licensing costs.

While this licensing argument is valid, it also has a huge loophole. Any experienced network administrator will tell you this:

You can never predict when a device might become critical.

Not-so-fun fact: The average hourly cost of network downtime for small and medium-sized business is approximately $42,000. And the number one cause of network downtime is hardware failure.

It's important to keep track of the devices that are not added to your monitoring tool, like test machines and non-critical devices, too. Whenever you're adding additional functionalities to such devices, immediately add the device to your monitoring tool if you feel the addition of the functionality might make it critical.

When you add a previously non-critical device to your monitoring tool, you might want to limit the number of parameters you monitor, but ensure that they're being monitored nevertheless. Your monitoring costs will be overshadowed by the losses you can prevent in case those devices become highly critical and cause any potential trouble.

Best Practice #8

PLAN CHANGE IMPLEMENTATIONS BASED ON AVAILABILITY AND CRITICALITY

Any change must be effected with minimal downtime, and must not affect crucial business operations. Planning the changes to your network plays a critical role in managing your network efficiently. Usually the best practice is to implement any changes in your network during non-production hours. This will ensure that there are no negative business-level implications, and will also give you time to roll back the changes in case something goes wrong.

However, knowing when to implement a change depends on four factors:

- **Criticality of the change:** If the change is a critical security bug fix, it needs to be made as soon as possible.

- **Duration of the change:**A critical bug fix that will only take a few minutes to implement and will not damage the existing system can be effected within production hours. A critical bug fix that will need a few hours has to be implemented during non-production hours.

- **Network size:** If your network is small and doesn't have backup servers, even the most critical changes have to wait until non-production hours.

- **Recovery time:** How long will it take for your systems to recover if something goes wrong during the change implementation process? No matter how small the change may be, ensure that the downtime that you set for the change also includes time for recovery.

Have an approval hierarchy: A change approval hierarchy is a set of people upon whose approval any change is implemented. The hierarchy must start with the person implementing the change at the lowest level, and then go all the way up to people in upper management. The intermediate levels can be filled by people with a mixture of domain knowledge and networking knowledge who can understand the implications of the change. Every change, regardless of its criticality and impact, must be implemented only after it goes through the change approval hierarchy.

Best Practice #9

DON'T IGNORE MINOR UPDATES

Due to the mere complexity of the process of implementing a change in a network and managing the risks involved in it, most network administrators don't make changes unless they involve a critical update, bug fix, or configuration change. With this risk aversion mindset, network admins have a natural tendency to ignore small updates provided by device vendors.

Not-so-fun fact: Not installing non-critical updates increases device vulnerabilities. For this reason, most vendors don't allow installation of updates until all the previous updates have been installed.

While you might be saving unnecessary downtime and change processes by skipping the insignificant updates, here's the problem: Though not every update issued by a vendor is critical, vendors usually issue multiple small updates before a critical one. Some parts of those small updates will be necessary for the critical update to run.

So, the next time you skip the small updates and jump directly to the critical update for a device, you're indirectly causing the critical update to be installed improperly. Sometimes, by skipping those small updates, you might actually be turning the critical updates into a huge security vulnerability.

Here are a few tips on how to keep up with even the smallest updates without having to schedule downtime every day:

- Read the specifications of every update (device-specific and vendor-specific) that the device manufacturers issue. This will help you understand the purpose of the update.
- Delay installing critical updates but ensure you never skip updates.
- Group multiple small updates and install them in one go. You can schedule weekly downtime during which you install all the small updates issued by manufacturers.

Best Practice #10

AUTOMATE TASKS WHEN YOUR NETWORK IS SMALL

> Not-so-fun fact: One in every five network administrators revealed that they wish they had automated basic tasks when their organization's network was one-fifth of its current size.

It's easy for organizations to manage their network while it's still small. In the early stages of a network, most network management tasks (like scheduling downtime and installing device updates) are done manually by network administrators. Most organizations only think to leverage automation when their network gets bigger.

Any experienced person in the network management domain will tell you this approach towards network management is highly flawed. Why? Because first, **the manual approach is highly error-prone and secondly, as the network scales up and becomes more complex and heterogeneous, it becomes increasingly difficult to implement any kind of automation**. Hence, even if you don't feel

a need for it, leverage the power of automation wherever possible, even in the minutest of tasks—you'll thank yourself later.

Here's a list of things you can automate in the early stages of your network that'll help you in the long run:

- The process of adding new devices to your network monitoring tool.
- Planning and scheduling downtime for network devices.
- Performing maintenance tasks and remote operations.
- Performing actions when any device crosses a particular threshold limit for a certain parameter.
- Backing up databases as well as device-level and network-level configurations.
- Repolling devices to check their availability.

Best Practice #11

CHOOSE THE RIGHT NETWORK MANAGEMENT APPLICATION

Of all the best practices given in this e-book, this is the most important. No matter what your requirements are, how large your network is, or what strategies you follow for network management, successful network management ultimately boils down to one thing: choosing the right network management application.

There are many different network management applications in the market. Each comes with its own features as well as pros and cons. Choosing the right network management tool for your organizationcan be done only through a careful evaluation of your monitoring requirements and analysis of the tools in the market.

Failing to choose the right network management application is akin to hiring the wrong person for the job. It'll not only complicate your work as a network admin, but will also land you in networking pitfalls.

Here's how you can save yourself from jumping into the wrong tool for your network:

- First and foremost, be clear with your goals and requirements.
- Most applications have a free trial period. Try them out.
- Ask for a demo. Read the reviews.
- Check out their support forums.
- Analyze their ease of setup and usage versus their features.
- Try running trial versions of different applications in parallel to determine the right fit.

At the end of the day, the line between usability and complex functionalities is thin and if you overdo either, you'll pay for it. If you have any questions about choosing the right tool, feel free to email us at support@opmanager.com, and we'll be more than delighted to help you make the right choice.

CRITICAL METRICS TO HELP YOU ARRIVE AT THE RIGHT NETWORK MANAGEMENT SOFTWARE

- Do your primary requirements match the application's features?
- Are your primary requirements easily configurable within the application?
- Does the number of devices the application supports match your network size?
- Does the application support all the different kinds of devices in your network?
- How is the technical support?
- How are the online forums and user groups?
- What about scalability?
- Does the pricing work for your company?