BACKBOX

WHITE PAPER

Prioritizing Network Automation Projects Based on Needs

If you're like other network engineers, you're being asked to do more, do it more quickly than before, and without interfering with other business operations. In many organizations, the network infrastructure continues to expand to accommodate growing communications, application, and data storage capacity. At the same time, most network engineering teams are not getting the additional staff members they need to keep up or replace the talented team members who leave.

Add it all up and it's clear why many of these organizations have turned to network automation to keep pace. What follows is a series of suggestions about the technical aspects of these initiatives, as well as the larger business reasons for doing it, which may help you persuade others of the value that network automation tools can provide.

Why network automation has become so critical

Perhaps the best way to illustrate the struggles you face as the head of administering your network is through specific scenarios shared with us by other network engineers.

Scenario X

You're in charge of a small network administration team for a company that is only a few years old but is growing rapidly. The team is talented, but the star is Dave – a code whiz who creates Python-based scripts to handle all the configuration of new devices and platforms. So far, everything is running smoothly. Then one day, Dave says he needs to talk to you.

"I've been offered a job with another company, and they're doubling my salary," Dave tells you. "So I'll wrap everything up in a couple of weeks. Sorry, but I just couldn't turn it down."

You get a sinking feeling in your stomach. Two weeks and Dave will be gone, and no one else on your team can do what he does. Sure, they can code, but they're not Dave. And given the shortage of talented network engineers, you know you're not likely to find another Dave.

So you start thinking about getting a network automation tool – something that will do the work that Dave was doing without being tempted away by a higher salary, while also extending the capabilities of your network team.

Scenario X is just one of several scenarios that highlight the increasingly important role that network automation is playing in modern businesses of all sizes. When your network goes down, you're out of luck. You can't sell products. You can't serve customers. You can't really do much of anything as a business.

The costs can be astronomical. ITIC's 2021 Hourly Cost of Downtime Survey found that for 91% of companies, a single hour of downtime costs at least $300,000 due to lost business, productivity, and remediation. A full 44% of surveyed companies put that figure at $1 million to $5 million per hour.

> Other surveys have shown that such outages are caused by network configuration errors, and those errors are most likely caused by faulty manual work.

Let's look at a couple of other scenarios that might lead you to consider a network automation solution:

Scenario Y

Before Dave leaves, a vulnerability affecting your network infrastructure is discovered. Dave is quick to analyze the situation and sees where your network might be attacked. He discovers malware that has just infiltrated one of your

network devices, quickly shuts it off from the rest of the network, and blocks the malware from doing extended damage. He then downloads a patch from the device's manufacturer and applies it to all of those devices, across the entire network. But you realize that if Dave hadn't been around, no one else would have been able to solve the problem.

Scenario Z

The network goes down at 4 p.m. and Dave has already started his new job. Nothing is functioning – no email, no Zoom, no Slack – so everyone in the office leaves for the day. "You'd better have us back online by tomorrow morning," the CEO growls at you. Frantically you and your junior team members work through the night, painstakingly working to restore the network manually because the automated backups that are normally collected by Dave's Python scripts stopped working a few weeks ago, and he was the only member of the team with deep software development skills.

Thinking about network automation strategically

Let's be honest, you can't go from a largely manual process of network administration to a fully automated, totally integrated strategy in one fell swoop. You need to establish priorities. Those will differ for each company, but they break down into three stages of achievement.

Stage One: You and your team are doing what is required to keep the network operational and provide basic security. This means automation of configuration backups, restore procedures, and policy validation.

Stage Two: You and your team are taking measures to continually run more efficiently and reduce costs. This means automated optimization of your network infrastructure's health, performance, and security.

Stage Three: At this ultimate stage, you and your team are able to focus on managing the automation platform and approving changes, allowing automation to handle the bulk of the work you previously took on yourselves. This means automation of user-requested moves, adds, and changes, as the platform itself responds directly to ServiceNow tickets and user requests.

Of course, you would want to zip ahead as fast as you can, but it's essential to focus first on the practical, essential tasks. If your company can't function for days due to an outage or suffers a major breach that leaks personal information about your customers, you can forget about cost savings and efficiency. Bankruptcy makes those issues moot.

But take heart; you're not alone in relying on manual processes for your network activities. According to Gartner, as of 2022 less than 35 percent of network activities are automated.

So let's look at what network activities need to be addressed, starting with Stage One and then looking at Stage Two. Frankly, Stage Three is so far off for most teams that it is not worth additional discussion at this point.

Backup and restore capabilities

Whatever your network looks like, you'll want to be sure that you can perform the backup and restore functions that keep your operations flowing. This is clearly a Stage One issue. Without automated backup and restore capabilities, you risk significant downtime for your company.

Network automation systems ease the pain of doing backup and restore manually. While the cost-savings aspect might categorize this as a Stage Two activity, the impact of lost business functionality is even more important financially and reputationally, so consider this a Stage One requirement.

Configuration change monitoring

Network automation platforms need to be able to detect when changes are needed or when the network engineer should be notified of changes. Whatever config product you buy for this purpose should be integrated within the overall IT management ecosystem. The base-level requirement is configurability and the tasks associated with it: validation and testing.

An automated config tool greatly enhances the contributions your junior-level network engineers can make. The tool includes built-in safety rails that keep the inexperienced engineer from making damaging errors. Consequently, they can accomplish much more each day than they would have been able to if relying on manual processes. If nothing else, keeping a junior employee from making a serious, consequential error elevates this to a Stage One requirement.

Inventory collection

The network administration group needs to be certain all the devices on the network are properly inventoried so the engineer can see all of them at once, log into them as necessary and perform any interactions. Here, the group's essential task is to establish an exhaustive inventory and a process that allows the organization to keep the inventory current and up to date.

That process will vary from organization to organization, but it should include as a starting point a way of establishing communications throughout the organization so the network engineers are aware of any additions, operational concerns, etc., going forward. It should also have a clear set of principles by which key information is accumulated. For example, naming conventions for devices, databases, services, etc., should be unified to minimize confusion and unneeded future work.

This is a somewhat advanced function, so perhaps consider it an activity for the later portion of Stage One.

Security automation

With the increasing threat of cybercrime, it's important for the network engineer to continually validate the organization's security perimeter – ensuring firewalls and intrusion detection systems are doing their jobs. In addition, the security automation system should integrate with a threat feed, endpoint protection, and XDR platforms. This, too, is Stage One, but security is a never-ending proposition, so it is one task you'll never complete.

Datacenter automation

Modern data centers are a mix of physical and virtual infrastructure and are evolving quickly to operate more and more like a public cloud. Moves, Adds, and Changes (MAC) automation requires the ability to span multiple devices and focuses heavily on automation of the compute infrastructure. The number of MACs required in modern data centers necessitates a comprehensive automation strategy while the risk of any single change is less than that associated with stage one, infrastructure level changes.

Most organizations will benefit from a robust cloud automation implementation, typically spearheaded by their cloud operations, DevOps, or SRE teams. These systems-focused, compute-oriented automation systems can integrate with best-of-breed network infrastructure automation tools to automate the full scope of the required changes.

Another factor to consider: Eventually, the data center along with cloud data are likely to be managed with a service mesh overlay. The trend is toward a single method of controlling physical and virtual environments, and the service mesh concept is the probable methodology that will be employed for that end.

Other elements driving network automation planning

Compliance considerations

A driving external concern for all IT and security departments is complying with relevant regulations. For example, for privacy and security concerns, the engineer may wish to have privileged access management capabilities.

Financial service organizations, telecommunications, media, MSPs, and MSSPs – all of these are examples of organizations that need to be mindful of regulatory issues. The list of industries subject to regulations is only going to grow over time.

Keep in mind the potential legal ramifications for failing to adhere to compliance requirements. A privacy breach could result in a costly lawsuit because the non-compliance becomes strong evidence against your company.

In addition to external compliance, there are internal company compliance matters to consider. For example, you want to ensure that all NTP servers in the configuration of devices are set to 10.0.0.1.

Deployment speed considerations

Relatively few organizations can afford long delays in getting their network automation functionality up and running. Delays only complicate issues and prevent the team from effectively addressing the situations for which network automation tools are designed.

This means sacrificing some customization ability for the sake of rapid deployment. That's a choice that a lot of mid-sized organizations are more than happy to make because they are already overloaded and can't afford further delays. Time-to-value is a driver here.

Network speed considerations

For some businesses, near-instantaneous response times in customer-facing applications are critical. If you're selling an item online in a competitive field, a delay in execution can cause buyers to abandon their shopping carts and log into a rival's site. Here, you might consider tools that allow performance and fault monitoring of your network.

The flexibility of an open API

Rather than being dependent on a single vendor, an open API system allows network administrators to choose which vendors to use for various functions in their system. This also allows organizations to add features as they go and need more capabilities.

And it's simply unrealistic to think that one vendor or proprietary system can address all the needs of your IT infrastructure. Others in your organization are going to have their preferred tools.

> You want to make sure that whatever you buy for network administration can play nicely with them.

Cost considerations

With pressures to do more with less, IT teams need to find solutions that help them get the work done without breaking their budgets. A solution that does what it says it will do, and allows the organization to grow and add more tools as necessary, is an effective way of addressing this issue.

BACKBOX

About BackBox

Backbox is dedicated to empowering our customers to continuously enhance the health, performance, and security of their network infrastructure through intelligent, security-minded automation. We believe that network automation should be easy, attainable, and provide our customers with unprecedented time savings and reduced risk.

Learn more at BackBox.com