A Network Source of Truth Promotes Trust in Network Automation

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER
PREPARED FOR CISCO
BY SHAMUS MCGILLICUDDY
MAY 2020

EXECUTIVE SUMMARY

Many network engineers distrust network automation. One reason for this distrust is a lack of insight into network intent and network state. An authoritative source of truth about the network, with intent and state data, can reverse this lack of trust and lead to network automation success. This white paper draws on market-defining research by Enterprise Management Associates to explore how IT organizations can establish a source of network truth to drive a successful network automation pipeline.

INTRODUCTION

Network automation is not a new concept. IT organizations have been trying to automate infrastructure and operations for decades, with mixed results. Enterprise Management Associates (EMA) research has found that only 44% of enterprises with formal network automation initiatives fully trust that automation.[1]

Why don't more people trust network automation? There are plenty of reasons. Networks have distributed control planes, which makes the job of automation complex. Network automation solutions excel at automating some tasks, but others require more nuance. Thus, network automation solutions applied to complex tasks tend to be immature and risky.

There are several ways to establish trust in network automation, but a source of network truth should be the starting point. EMA research has found that IT organizations are more likely to trust network automation solutions that include an authoritative source of truth for the network. A source of truth for network automation is a comprehensive repository of network data that drives the automation pipeline. This source of truth must be well-governed, meaning that change controls are in place to protect against unauthorized changes. It should also be authoritative, assuring that no other data repositories can supersede it.

A network reliability engineer said it best in an interview with EMA. "Most of the configuration information [that drives our automation] is coming from our [database]. We are exposed to someone making a change in that database that could break the network because we don't have tight controls over those changes. We trust the tools, but we don't trust the data we are using."

A source of truth builds trust because it ensures that the data that drives automation reflects network intent and network reality. In fact, 98% of enterprises say that a source of truth is relevant to their network automation initiatives, and 41% say that this source of truth is essential. With a source of truth, network automation solutions are trusted and more successful.

[1] All data cited in this research was originally published in the EMA research report "Enterprise Network Automation for 2020 and Beyond" in September 2019.

WHAT IS A NETWORK SOURCE OF TRUTH?

A network source of truth is a repository of data that provides network managers and their network automation pipelines with authoritative insight into the intent of the network and the current state of the network. Intent data can be derived from configuration files, device inventory, cabling information, and other sources. The state of the network can be derived from device telemetry, routing tables, and other operations statistics (configuration, etc.).

With an authoritative source of truth, network engineers can drive change through their network automation pipeline with full knowledge of what the network is meant to look like, how it looks at that moment, and how the network will look after the automation tool has made a change. Finally, a source of truth can confirm that the automated change had the intended effect.

ATTRIBUTES OF AN EFFECTIVE NETWORK SOURCE OF TRUTH

EMA has found in its research that enterprises vary widely in their approach to a network source of truth. Some IT organizations build a source of truth in-house, either from scratch or with open-source software components like NetBox. This is especially common with enterprises that are building their own network automation tools. Some enterprises expect their commercial network automation solution provider to deliver an integrated source of truth. Others look to third-party management tools, like network change and configuration management (NCCM), DNS, DHCP, and IP address management tools (DDI), and configuration management databases (CMDB) for their sources of truth. Regardless of one's approach, a source of truth should have a few key attributes.

Make it Authoritative

EMA research has found that enterprises that build a source of truth with data conflicts are the least likely to succeed with network automation. Thus, the source of truth, whether it's one repository or several, must be authoritative. Enterprises have been establishing golden configuration standards for years. The trick is getting that data into the automation pipeline and making sure that it is protected as the authoritative standard for configuration.

Regardless of what repository an enterprise uses as a source of truth, the network automation team must ensure that it is authoritative. If inventory data is part of this source of truth, a network discovery tool cannot automatically overwrite that inventory information without proper controls in place. If a network team has multiple tools for collecting device telemetry, there will ultimately be conflicts between their data stores. The network automation team must designate one of these monitoring tools as the source of truth.

Collect the Right Data

EMA spoke with one network engineer at a Fortune 50 enterprise whose network automation source of truth had a strong view into network intent, but lacked insight into the network state. His source of truth was native to a commercial, off-the-shelf automation tool. After he pushes an automated change to the network, "We wait for [the network operations center] to receive an SNMP trap to tell us if the network went down. If we [pushed a change via automation] and nothing happens after 15 minutes, we know the change was good."

This is a disaster waiting to happen. Thus, a source of truth should include both intent and state.

In its network automation research, EMA asked enterprises to identify the data most valuable to their sources of truth. Their top four responses were:

1. Device state metrics
2. Data from shared services (DDI, Active Directory, etc.)
3. Network flows (NetFlow, etc.)
4. Configuration data that has been normalized into key value pairs

Enterprises that fully trust their automation were more likely to tell EMA that shared services data, raw configuration files, and configuration data normalized into key value pairs are important to their source of truth.

“Device status and inventory data are most important to use,” a network reliability engineer told EMA. “We have a lot of systems referring to these statuses at both device and link levels to define configurations.”

If an enterprise lacks insight into intent or state, it should look for ways to integrate other sources of data into the pipeline. For instance, network automation tools with insight only into network intent should not be waiting for a network monitoring tool to flag a bad network change. Instead, the network team should integrate an operational monitoring tool into his automation toolchain, either directly or indirectly through something like an ITSM ticketing platform. This will allow the network automation team to get an alert faster. This integration might require support from a vendor’s professional services team. If they can’t help, it might be time to look for a new automation vendor.

Data Management is Essential

Collecting data and protecting its quality and security are paramount for a source of truth. EMA asked network automation professionals to identify their top data-related challenges. Security was the number-one problem. Respondents find that the process of collecting certain data from the network presents a security risk. Perhaps this collection requires decryption, which elevates risk. Therefore, the repository must be secure, with role-based access controls and authentication. When possible, the source of truth should also be encrypted.

Scale is the second-biggest data challenge. Engineers will find that a source of truth can contain a massive amount of data, especially on larger networks. Whether building one or buying one, enterprises must plan for the scale that a network automation pipeline may demand from a source of truth.

Finally, data quality is the third leading challenge. Some data collection mechanisms may produce bad data, such as SNMP packet drops, or errors might occur as the data is written to disk. Sometimes, enterprises rely on highly manual data entry for their sources of truth. For instance, an engineer might maintain inventory data in a spreadsheet, which could introduce coding or data entry errors. Enterprises need to minimize these data quality issues, either by upgrading to something more automated or imposing data quality controls.

A “God” Database is Not Necessary

Enterprises shouldn’t expect to cram every class of data that contributes to a source of truth into one data lake. A single repository or database is possible, particularly if it’s supporting a commercial network automation pipeline, but the “god” data repository is rare. Only 26% of network automation initiatives have a single source of truth.

A collection of multiple authoritative repositories of data may be more realistic. This approach is followed by 63% of network automation initiatives. It is especially suitable for an IT organization that is building its own automation pipeline or combining multiple network automation solutions, such as data center network automation, cloud network automation, software-defined WAN, and software-defined LAN.

There can be overlaps of data between these multiple repositories, but the automation team must make sure to tag which repository is authoritative on each class of data in its source of truth. Other, nonauthoritative sources of IP addressing, for instance, should not be allowed to override the authoritative source of truth on IP addresses. The automation pipeline should know which repository is the authority on addresses.

“There isn’t a single source of truth,” a network automation engineer told EMA. “There are systems of record, like IPAM for IP addresses, and DCIM that has a record of all devices on the network. And another that tracks cabling. All of them can be combined to create a system of record.”

EMA PERSPECTIVE

EMA research has found that enterprises with an authoritative source of truth connected to their network automation pipelines are more likely to succeed with network automation. Network automation specialists who recognize that a source of truth is essential to automation were twice as likely to describe their network automation initiatives as successful than those who see no value in a source of truth.

More importantly, enterprises with a strong source of network truth trust their automation. Network automation professionals who fully trust their automation were three times as likely as those that don’t trust their automation to say that an authoritative source of truth is essential to automation.

EMA research has identified three top technical benefits that an enterprise can derive from an effective source of truth. First, their network automation tools are easier to integrate with other IT systems, such as a DevOps toolchain or an IT ticketing system. Second, a good source of truth allows enterprises to be more confident that automated changes won’t create a security vulnerability on the network or leak data. Third, a source of truth enables rapid support of new network features and technologies.

Enterprises can also expect several business benefits from a network automation pipeline with a good source of truth. First, enterprises will reduce security risk. Twenty-five percent of enterprises say this is one of the most important benefits of successful network automation. With fewer mistakes, better control of the network, and a better understanding of intent and state, IT organizations reduce network vulnerabilities.

Enterprises can also expect to eliminate human error (20%) with network automation, leading to fewer outages and service problems. Proactive problem prevention capabilities (19%) are also enhanced by successful automation. With good insight into intent and state, automation can detect and prevent service trouble before the business is impacted.

Finally, EMA research has found that self-service infrastructure (18%) becomes possible with this automation. Application owners and business units are empowered to use the network as a service, to request and receive connectivity and network services on demand.

Regardless of where an enterprise is on its network automation journey, network engineers should be thinking about their own sources of truth. It's never too late to start having conversations with one's team and one's vendors. Network automation vendors should be ready to talk about how they support this essential capability. Vendors should also be ready to adapt to the unique data requirements of enterprises. If they aren't, it is possible to build one's own source of truth, but the earlier one gets started on it, the better. It will be hard to bolt on a source of truth after the fact.

ABOUT CISCO NETWORK AUTOMATION

At Cisco, spending nearly a decade of automating some of the largest service providers and enterprise networks in the world has taught us the value of intent-based tooling that gives you confidence about what is going on with your infrastructure. Without this kind of surety, automation will never truly deliver on its promise. To learn more about how Cisco can help you build a more trusted toolchain, visit cisco.com/go/nso to learn more about intent-based automation and cisco.com/go/crosswork to learn how to build closed-loop workflows.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates® (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com
3985.05182020