Enterprise Framework for Network Automation

Mapping Day 0 to Day 2 for application and cloud modernization

Get Started

vmware®

Getting started

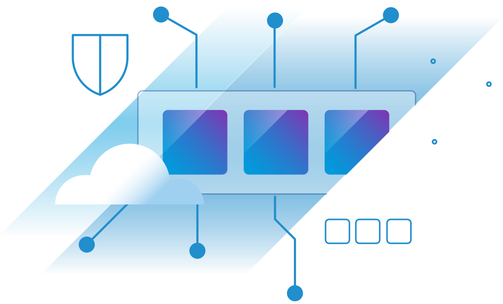
After emerging from the pandemic era, the global economy finds itself grappling with a significant downturn and unprecedented turbulence in the financial market. No sector is unscathed, with businesses struggling to operate more efficiently. They will rely on digital services more than ever to release new and updated applications and services more frequently. This makes IT infrastructure reliability and security paramount.

Many IT organizations have automated compute and storage provisioning. But this has only partially solved business speed and productivity challenges because most organizations have not addressed network and security operations. The network domain is especially perceived to be operating in its own silo, based on a hardware-centric and scripting approach to delivering and managing networking components. Network automation is the key to truly enable organizations to comprehensively automate the infrastructure and application delivery process end to end. Network automation can help enterprises deliver applications more quickly to support the business rollout of new products and services, and to move into new markets. Automation also helps to reduce CapEx and OpEx by making the network more reliable and scalable.

However, not all network automation solutions are the same. What's needed is greater flexibility and reliability across the infrastructure and application delivery lifecycle. A network automation solution should allow different IT teams to use the build tools of choice to programmatically interact with virtualized network infrastructure objects. An ideal solution automates the Day 0 tasks for initial environment creation and fabric preparation, driving configurations, changes, instructions or troubleshooting at scale. Furthermore, the solution should make it possible to create and save network configurations in files that can be version controlled and leveraged later in infrastructure and application templates in Day 1 and Day 2 processes to maximize operational savings and productivity gains across the enterprise.

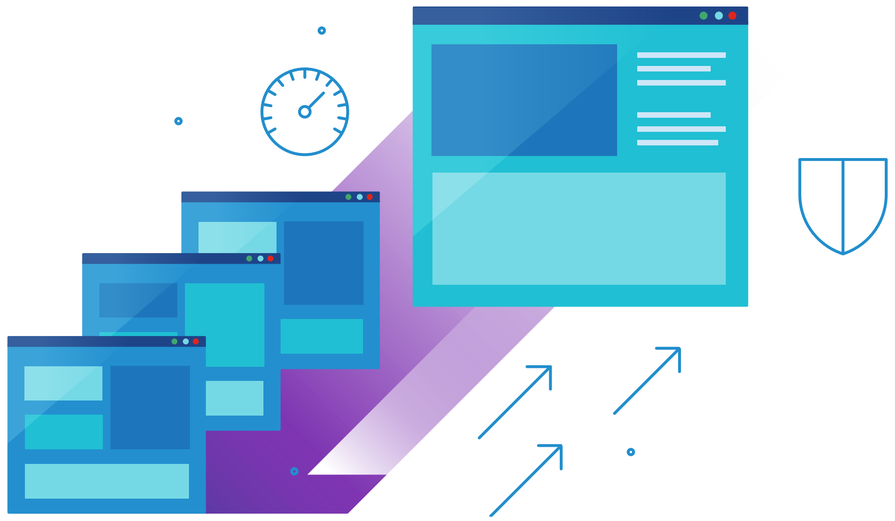
This ebook provides a simple framework for a network automation solution that supports each stage of the IT service delivery lifecycle, as well as guidance on how to implement the solution enterprise-wide.

Map your path to a successful digital transformation with the network automation enterprise framework in this ebook.



Charting the network automation end-to-end process

Network automation can enable multiple parts of the internal IT organization, the provider (of IT services)—from network engineers to cloud admins—to modernize IT processes across the IT delivery cycle from Day 0 to Day 2, supporting the rapid rollout of applications and maintaining business continuity in the new normal:



- **Day 0** is about setting up the network environment and creating the network and security services that will be made available to users, both **providers** (internal IT teams, such as network engineers and cloud admins) and **consumers** (the end users, such as developers, application owners, application users, SecOps and DevOps engineers).
- **Day 1** is about provisioning infrastructure and applications with network and security services via self-service automation with embedded policy management. This gives organizations control over decisions, such as where resources are provisioned and who can request what type of resources.
- **Day 2** is about empowering both consumers and providers with self-service operations management capabilities (e.g., reconfigure, re-provision, snapshot), whether for an individual networking service or a full application stack with networking and security across its lifecycle.

Day	0				1		2	
Lifecycle stage	A. Install and configure the network environment	B. Set up network and security constructs and topologies	C. Establish the network and security in the automation platform	D. Build infrastructure and application templates with the network and security	E. Enhance provisioning and orchestration	F. Enhance DevOps for infrastructure	G. Empower consumers with Day 2 actions	H. Empower providers with Day 2 actions
Primary user	Provider				Consumer			Provider
	Network engineer	Network engineer	Cloud admin	Cloud admin	Developer, application owner/user, SecOps	DevOps engineer	Developer, application owner/user, SecOps	Cloud admin

Day 0

Stage A: Install and configure the network environment

Networking and security are like the digital nervous system of an organization and foundational to all IT services. The first stage of the IT service delivery lifecycle begins with the network environment creation/fabric preparation, driving configurations, changes and instructions at scale.

Typically, organizations are challenged with network failures and downtime due to human error in the initial network infrastructure fabric stand-up. Network engineers face difficulty setting up consistent network infrastructure resources—which enables a multi-cloud strategy and supports both traditional and modern cloud native applications—due to manual, time-consuming, resource-intensive Day 0 network management processes.

Organizations can leverage network virtualization to pool and automate networking for VM- and Kubernetes-based environments. Similar to VMs for compute, virtual networks are programmatically provisioned and managed independent of the underlying network hardware. By leveraging a software-defined approach, network engineers can programmatically automate many of these basic network installation and configuration tasks.

Day 0 – Stage A: Install and configure the network environment

VMware network automation capabilities	Benefits
• Enable network engineers to deploy VMware NSX® Manager™, register with VMware vCenter Server®, deploy a cluster of VMware NSX Controller™ nodes, and prepare the VMware ESXi™ hosts/transport nodes for NSX. • Configure VXLAN or GENEVE encapsulation, specify virtual network interface (VNI) ranges, and create transport zones. • Programmatically orchestrate VMware NSX-T™ Day 0 tasks (e.g., configuring NSX-T manager, NSX-T policies, NSX-T transport nodes, NSX-T transport zone, uplink profiles, IP address pool) with Salt or VMware Aria Automation Config™, leveraging the open source Salt extension modules for NSX-T. Run commands via CLI, or build out state files to call the modules.	• Gain the ability to use the extensibility and configuration management tools of choice to programmatically interact with network infrastructure objects. • Automate the Day 0 tasks around environment creation/ fabric preparation, driving configurations, changes, instructions or troubleshooting. • Maintain proper security and compliance over the use of third-party tools with flexible guardrails, including role-based policies.

Day 0

Stage B: Set up network and security constructs and topologies

With the basic virtual network installed and configured, the network engineer is now tasked with setting up network and security constructs and topologies. This entails configuring logical networking, deploying and configuring network edges, and configuring network and security services. Additionally, a network engineer will determine whether a standalone network data center or a federated environment with multisite network deployments is required.

Similar to Stage A, network engineers are also challenged with network failures and downtime due to human error during this stage. Traditionally, network engineers use CLI to manually process syntax-specific keywords and phrases that are often repeated several times, which is inefficient and creates risk for errors.

With network automation, network engineers can build networks with network as code, applying infrastructure as code in the networking domain. This entails network configuration files stored in source control, versioned, peer reviewed, approved, merged, staged, tested and deployed into production.

Day 0 – Stage B: Set up network and security constructs and topologies

VMware network automation capabilities	Benefits
• Enable network engineers to set up logical switches/segments, logical routers/T0–T1 gateways, NSX L2 bridging, VMware NSX Edge™ services, NSX Edge VPN services, and NSX security services, and build out the NSX deployment topology. • Programmatically orchestrate NSX-T Day 0 tasks (e.g., create T0–T1 gateways, segments) with Salt or VMware Aria Automation Config and the open source Salt extension modules for NSX-T. Run commands via CLI, or build out state files to call the modules. • Provide an extensible framework with standardized APIs and plug-in models to easily integrate with third-party configuration management tools that can also be leveraged to create logical topologies and complex configurations, including setting up routing, switching, and setting up distributed firewall rules.	• Align NetOps with DevOps principles to accelerate application-oriented workflows. • Predictably and repeatably make changes to networks to deliver a more reliable and scalable network. • Attain operational savings and productivity gains with NetOps by being able to create and save network configurations in playbooks or manifest files, which can be version controlled and leveraged in infrastructure and application templates in Day 1 and Day 2 processes.

Day 0

Stage C: Establish the network and security in the automation platform

Once the basic network and security constructs and topologies are set up, the cloud admins can leverage this foundation to define network and security objects into the cloud automation platform, so the rest of the organization can take advantage of networking and security services at scale through automation and self-service. Depending on the scale of the network, both local and global objects (e.g., global segments, global security groups) can be made available to users.

From an organizational view, this can be one of the most challenging stages. In many cases, IT organizations operate in silos. The handoffs and coordination between the network infrastructure teams, the security teams, and the cloud infrastructure automation teams can be manual with long cycle times. To make things more challenging, each team might not fully comprehend or care about the technicalities of the other domains.

Network automation can be used to make this a seamless transition. With network automation, cloud admins can discover existing resources and generate network profiles. They can import existing network and security constructs, and create new on-demand network and security constructs to be leveraged for infrastructure and application template creation.

Day 0 – Stage C: Establish the network and security in the automation platform

VMware network automation capabilities	Benefits
• Enable cloud admins to discover existing resources (network and security constructs) via data collection (resources created out of band via NSX, Terraform, etc.) and set up network profiles. • Create on-demand network and security constructs directly via VMware Aria Automation™ on the endpoint. • Integrate with Infoblox IPAM solutions, or use an IPAM SDK to develop packages that integrate third-party IPAM providers with VMware Aria Automation. • Enable cloud admins to use the VMware Aria Automation Orchestrator™ plug-in to support VMware NSX Advanced Load Balancer™.	• Scale security by supporting firewalls and security policies as template components. • Continuously extend network and security policies automatically to private, public and multi-cloud environments, easing management of the environment for IT teams. • Prevent inconsistency across environments that can slow operations and increase the risk of security breaches.

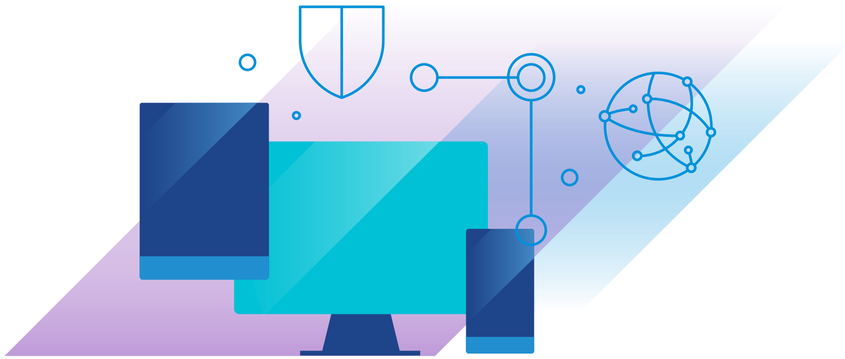
Day 0

Stage D: Build infrastructure and application templates with the network and security

With the network and security objects defined in the cloud infrastructure automation platform, the cloud admin can complete the final Day 0 stage by building infrastructure and application templates.

The actual effort required to create an infrastructure service can be several hours. However, for organizations that have not automated this process, those hours are spread over days or weeks. This is a snowball effect of time-consuming manual tasks, manual configurations that lead to inconsistencies/errors/rework, and organizational siloes that lead to wait times in slow workflows. Once the infrastructure service is delivered, the application teams need to install, configure, test, and deploy the database, middleware and application components. Delivering applications on top of infrastructure services can take weeks or even months.

A better approach is having the cloud admin model and create a standardized infrastructure and complete multitier application environments for end users as cloud-agnostic templates that include network profiles and security policies. Once modeled, workloads can be deployed in any approved cloud environment. These templates will be made available to consumers via a self-service catalog.



Day 0 – Stage D: Build infrastructure and application templates with the network and security

VMware network automation capabilities	Benefits
• Enable cloud admins to visually drag and drop existing and on-demand NSX logical components on a design canvas, then dynamically build networking and security services into infrastructure and application templates (easily create on-demand networks, load balancers and security groups). • Enable cloud admins to apply an infrastructure-as-code approach via templates editable in YAML code. • Provide configuration management tool files that are available as template resource types (e.g., Terraform configuration files managed as VMware Aria Automation resource types).	• Provide repeatability while reducing manual network and security administration hassles. • Enable IT to automate the creation and consumption of network and security resources. • Enhance security by delivering secure, scalable and high-performing applications on demand.

Day 1

Stage E: Enhance provisioning and orchestration

Once the network environment is set up and network and security services are made available, both consumers and providers can take advantage of these services in Day 1 provisioning via self-service automation with embedded policy management.

One of the major challenges enterprises have traditionally faced is provisioning application-level security firewalls as part of the process to provision a multitier application. Generally, this is one of the last steps conducted in provisioning an application stack. This step alone can add significant time in the form of days or even weeks to the overall provisioning process.

With network automation, when an application blueprint is selected by a user, the application-level firewalls needed to secure the application are provisioned while all other infrastructure- and application-level components are provisioned. Users can also request network and security configurations specific to needs at deployment time.

Day 1 – Stage E: Enhance provisioning and orchestration

VMware network automation capabilities	Benefits
• Enable end users to easily deploy, configure and manage production-ready applications with network and security services from a service catalog, or programmatically via an API or CLI. Users are only able to request and consume services associated with the projects they have access to. • Integrate with a DevOps tool chain, including source/version control tools, CI, testing frameworks, and configuration management tools, including Ansible, Ansible Tower, Puppet, Salt and Terraform. • Trigger configuration tasks, via VMware Aria Automation, as part to the deployment workflow (e.g., Ansible Tower Job Templates).	• Speed up infrastructure and application provisioning from weeks to minutes with faster time to market, while ensuring standardized environments and avoiding configuration drift. • Enable users to quickly request and create a network as part of the application deployment without needing to understand NSX. • Allow developers and IT to consume resources anywhere via frictionless governance. • Boost productivity by eliminating the need to manually provision application-level security firewalls separately. • Enable control over resources under management. • Enable and enhance hybrid cloud and multi-cloud environments.

Day 1

Stage F: Enhance DevOps for infrastructure

Simultaneously, DevOps teams can model the release process for infrastructure and applications with network and security services, using blue/green, canary or the rolling update delivery methods.

Infrastructure and applications are delivered by moving artifacts (e.g., application code, configurations, etc.) through stages. At a minimum, this includes development, test and production environments. Some organizations have already adopted continuous integration and continuous delivery (CI/CD) tools to build pipelines that model the software release process for their DevOps lifecycle, delivering infrastructure or software rapidly and continuously. However, without network and security automated, consumers will end up waiting for the networking and security resources to be separately and manually provisioned, wasting the overall benefits to be achieved by DevOps.

Network automation can help make a seamless process for standardized artifacts and configurations—from development, test, staging and into production—by ensuring standardized environments and avoiding configuration drifts.

Day 1 – Stage F: Enhance DevOps for infrastructure

VMware network automation capabilities	Benefits
• Enable end users to automate the release process at each stage of the infrastructure or software delivery pipeline with network and security services. • Integrate with existing software development, testing, artifact management and build systems to orchestrate tasks that need to be performed in the development process with network and security services.	• Realize productivity gains from quickly modeling the entire release process with network and security services, from simple to complex, without a bunch of scripting. • Increase operational savings from resolving issues quickly without large troubleshooting efforts by easily rolling back code that includes network and security services to earlier versions.

Day 2

Stage G: Empower consumers with Day 2 actions

After Day 1 provisioning, the IT delivery cycle moves on to Day 2, and consumers might find the need to update configurations post-deployment. This can include updating network and security configurations, such as snapshot, delete, reconfigure, re-provision, and retire network and security entities (template objects).

Very much like the previous stages, if consumers end up waiting for the provider to make simple changes to networking and security resources upon making a request, this can lead to wasting the overall agility and efficiencies gained up to this point. At the same time, careful consideration is required in determining how much access to changes is given to consumers. Making unintended changes to a deployment used by many users can have a disastrous impact on the organization.

Network automation can empower consumers with Day 2 actions. For example, consumers can request updates to networking and security configurations after deployment. Administrators can choose to limit the options available to the consumers, or allow broad self-service options that consumers might require for their projects. When required, a simple update to the template or network profile and redeployment will update the configurations.

Day 2 – Stage G: Empower consumers with Day 2 actions

VMware network automation capabilities	Benefits
• Apply NSX distributed firewall rules to a VM or a container, and change network configurations for provisioned networks and VMs. • Enable end users to take Day 2 self-service actions, governed with approval policies. • Enable the project administrator who manages deployment for teams to review all changes to the deployed catalog item.	• Reduce complexity and the time it takes to change configurations post-deployment, while simultaneously lowering the cost of IT operations, by empowering users to take self-service actions. • Reduce the administrative overhead with support for the environment.

Day 2

Stage H: Empower providers with Day 2 actions

As the business environment continues to evolve, providers will also find the need to update configurations post-deployment to adapt to business changes.

With business success and brand reputation at stake, providers must be prepared to continuously monitor ongoing operations to ensure quality of service and compliance. Beyond the initial provision and deployment of applications, ongoing operations throughout the application lifecycle remain a primarily manual set of tasks.

When application policies need to be updated, when applications need to be moved around, and when they need to be retired, the manual steps involved in doing so inhibit the ability of the business to be agile in responding to new shifting customer demands, compliance requirements and so on. Manually changing policies for an application negates the advantages gained from automating the initial provisioning and deployment process, and manual retirement often leaves behind a sprawl of stale firewall rules that can compromise the overall security of the environment.

Network automation enables providers to update both infrastructure and application templates with updated network and/or security profiles and policies. Even as applications are moved, changed and retired, their policies automatically get moved, changed and removed in lockstep.

Day 2 – Stage H: Empower providers with Day 2 actions

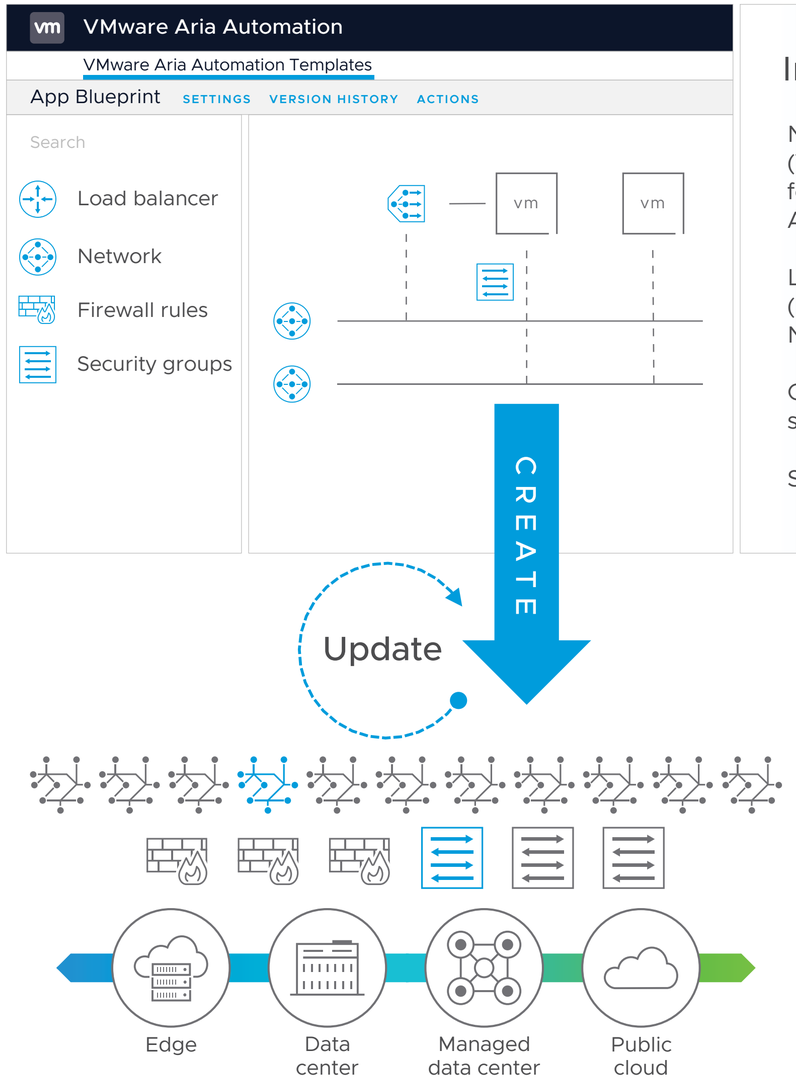
VMware network automation capabilities	Benefits
• Enable the project administrator who manages deployment for teams to review all changes to the deployed catalog item. • Enable cloud admins to change a network configuration or security policy for a set of applications via template updates as changes occur within environments and applications. Any application using the updated template will automatically be updated to reflect the modified configuration.	• Gain operational savings by simplifying ongoing configuration management. • Enhance security with security policies that also get retired with the workloads/applications to which they apply, ensuring there isn't firewall rule sprawl and that stale firewall rules don't pose security risks.

Discover network automation from VMware

With users worldwide communicating, collaborating and transacting through business-critical applications and services, organizations everywhere are pursuing new and differentiated business models and revenue sources that require a modern, agile IT infrastructure. Organizations will need to release innovative new and updated applications and services more frequently, and with enhanced reliability and security. Network automation is the key to integrating multiple parts of the IT organization—from network engineering to cloud operations—and modernizing IT processes across the IT delivery cycle to gain a competitive advantage.

VMware has a unique and powerful network automation solution that enables faster deployment and complete lifecycle automation of traditional and modern applications with networking and security services. By enabling consistency across clouds, VMware helps organizations achieve faster time to market, operational savings, productivity gains, and business resiliency.

VMware network automation automates VMware NSX with VMware Aria Automation. It combines the VMware Aria Automation modern infrastructure automation platform with NSX network virtualization to enable rapid application rollout with networking and security services. By applying DevOps principles to network infrastructure delivery, this solution ensures network policies are managed with workloads to eliminate operational bottlenecks in the application lifecycle. This solution enables fast, consistent networking and better security for VM- and container-based workloads across private, hybrid and multi-cloud environments.



Infrastructure as code

Network
(VMware NSX® Data Center for vSphere®, VMware NSX-T, AWS, Azure)

Load balancer
(NSX Data Center for vSphere, NSX-T, Azure)

On-demand and existing security groups

Service-defined Firewall

Get Started Today

Find out how your organization can benefit from VMware network automation.

LEARN MORE

Join us online:

vmware®