Operationalizing VMware NSX

Kevin Lees
Devyani Pisolkar

Foreword by
Bruce Davie

Operationalizing VMware NSX

KEVIN LEES

DEVYANI PISOLKAR

Foreword by
Bruce Davie

vmware®

Technical Writer

Rob Greanias

Design Agency

Mitchell Design

Warning & Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an as is basis. This book is based on the VMware Cloud on AWS SDDC version available at time of writing, SDDC version 1.7. The authors, VMware, and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book. The opinions expressed in this book belong to the author and are not necessarily those of VMware.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA
Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.

Table of Contents

List of Figures

List of Tables

About the Authors

Kevin Lees is the field Chief Technologist for IT Operations Transformation at VMware, focused on helping customers optimize the way they operate VMware-supported environments and solutions. He is responsible for defining, communicating, and evangelizing VMware's IT Operations Transformation vision and strategy as it relates tooperational (integrated organization, people, process, and application of VMware technology) approaches and best practices. Kevin also serves as an advisor to global customer senior executives for their IT operations transformation initiatives. Additionally, he is a member of VMware's Global Field Office of the CTO.

Kevin is an industry-recognized IT Operations Transformation thought leader, strategist, author, and evangelist. He was the global services delivery team lead for VMware's Cloud Practice from 2009 through mid-2011 and led many of VMware's early cloud implementations with Fortune 100 customers. Since 2011, Kevin has focused on initiating, building, and supporting IT Operations Transformation as a consultative delivery practice within VMware. Kevin has a combined 35+ years of IT system architecture, design, and integration, IT Operations, and IT consulting experience. He's written extensively on the subject of optimizing operations in a VMware-based environment, including the ever popular "Organizing for the Cloud" whitepaper and the e-books "Operationalizing VMware NSX®" and "Operationalizing VMware vSAN.®"

About the Authors

Devyani Pisolkar is a Product Line Marketing Manager in the Networking and Security business unit at VMware, focusing on networking and cloud solutions. Devyani is passionate about helping customers optimize their hybrid cloud journey and simplify and automate IT operations. She has 13+ years of industry experience in diverse functional roles such as engineering and product management and across a wide range of technology areas. Devyani has an MBA in Strategy and Marketing from Northwestern University (Kellogg) and a Master's degree in Electrical Engineering from the University of Southern California.

Acknowledgements

It takes the knowledge and resources of multiple individuals to successfully create a revision to a guide like *Operationalizing VMware NSX*. Devyani and I would like to thank the following people for their support in developing and reviewing the material included in this revision:

Thank you Rob Greanias (Technical Writer) and Connie Upman (Graphics Manager) for your efforts in completing this book.

We are grateful to Sehjung Hah, Ray Budavari, and Martijn Smit for their valuable contributions. We also want to thank Bode Fatona, Ahmed Al-Buheisi, Karl Furtz, Dee-Dee Atta, Karl Childs, Jing Shi, and James Robinson for their insightful input and review.

Since this is a revision, we don’t want to forget those who made the original version published in 2017 possible:

- Hammad Alam, Mark Schwighardt, and Vyenkatesh Deshpande – without whose contributions and insights the original book would never have come to fruition.
- Bode Fatona, Neil Mansukhani, Paul Wiggett, Chris McCain, and Bill Erdman their critical input and review.
- Kausum Kumar, Romain Decker, Chris Kunselman, Jose Alamo, Geoff Wilmington, and the many others whose work provided the inspiration for different aspects of the original book.

Preface

Operationalizing VMware NSX® offers guidance to management-level decision makers and influencers concerned with the impact of VMware NSX on their organization, staff, and operational processes. It also speaks to engineers and technical decision makers responsible for optimizing operational tooling in a VMware NSX environment.

Operationalizing VMware NSX provides the information needed to optimize the on-going operations of a VMware NSX environment. Specific areas examined include the critical aspects of team structure, culture, roles, responsibilities, and skillsets. Additional guidance is provided for operational processes, monitoring, and troubleshooting in a VMware NSX environment.

Foreword

The idea of network virtualization has been around since at least the early 2000s, but commercial adoption of the technology really took off around 2012. The launch of Nicira's "Network Virtualization Platform (NVP)" and subsequent acquisition of Nicira by VMware brought network virtualization to a broad audience. In 2013, VMware formally launched NSX,™ the network virtualization platform, which is now an increasingly common choice for the delivery of networking and security services.

As it happened, I joined Nicira just before the formal launch of NVP, and I have witnessed the early adoption of NSX through to increasingly mainstream acceptance today. One clear trend over the last five years has been a shift from talking about the architecture of network virtualization to a focus on the operational aspects. In the early days, customers were looking to be convinced that our approach was technically valid, but as adoption accelerated, the discussion shifted to operational issues such as trouble-shooting, upgrades, maintenance, automation, integration with other products and third-party tools, and so on. As a product team, we increasingly focused on building operational capabilities into the NSX product and on exposing APIs that would allow other tools to interact with NSX to provide operational support.

NSX is not like other networking products that preceded it. Networking delivered in software opens up the possibility of moving more operational tasks into software. It also requires organizations to rethink how they operate their network, as it is no longer an independent silo of hardware devices but an integrated component of the software-defined data center. These organizational changes can be harder to achieve then a simple change in technology.

Which brings me to this book. Operationalizing NSX is essential if a customer is to benefit from the capabilities of network virtualization. As with many disruptive technologies, the true benefits accrue when processes change to make most use of new capabilities. This book brings together the lessons learned over five years of changing the way networks are built and operated, and should be read by anyone who is serious about deploying NSX and realizing the many benefits it can bring.

Bruce Davie
CTO
Asia Pacific & Japan

Introduction

The Software-Defined Datacenter (SDDC)—whether as the basis for on-premises VMware Cloud Foundation™ (VCF) or hyperscaler-based VMware Cloud™ implementations—continues to present a nearly unprecedented opportunity for IT to dramatically increase agility and improve time to value in support of business initiatives. VMware NSX™ Data Center and VMware NSX Cloud™ introduced software-defined networking and security and have become core components of the SDDC. However, like the SDDC, they are merely enabling technologies. Simply implementing NSX from a technology perspective alone does not guarantee IT will become more agile or increase the speed in delivering business value.

What does “Operationalizing NSX” mean

Operationalizing NSX refers to what happens after designing and implementing NSX as a software-defined networking and security infrastructure. The term “day-2 operations” often refers to everything that happens after design and implementation of NSX, but to best leverage NSX’s capabilities it is important to think beyond simply ongoing operations.

How best to optimize NSX usage? Is the organization aligned to take full advantage of what NSX provides? What about IT’s operational processes? How might they impact the benefits provided by NSX’s software-defined nature? Could they be optimized to realize the full benefits of NSX? How are new users or new applications brought on board? Are there additional considerations due to NSX? How do developers consume NSX? What are the options? The answers to these questions are central to the concept of operationalizing NSX.

Why IT should adjust the way it operates for SDDC/NSX

As pioneer and leading innovator in "software-defined," VMware is uniquely qualified to help an organization's digital transformation and enable its digital business. To be successful with digital transformation, an organization must shift to a service mindset, aligning IT imperatives with business priorities. IT must also transform to truly deliver on this vision.

According to a CIO paper, "Instead of cost centers that provide capabilities, IT organizations must become internal service providers supplying business-enabling solutions that drive innovation and deliver value… true business partners rather than increasingly irrelevant, cost-centric technology suppliers." (*How IT Organizations Can Achieve Relevance in the Age of Cloud, 2013*).

To become a service provider and ultimately a true business partner, IT must consistently and continuously deliver value to the business at the speed it requires. VMware's software-defined approach provides IT the technical capabilities to enable this agility and speed. Implementing these enabling technologies provides IT the opportunity to change the way it works. Leveraging NSX and SDDC capabilities unlocks IT's ability to quickly respond to changing business needs and provide increased business value.

By working directly with NSX customers, VMware has found that changing the way IT works should be an evolutionary journey across three dimensions—people, process, and tooling—as shown in Figure 1.1.

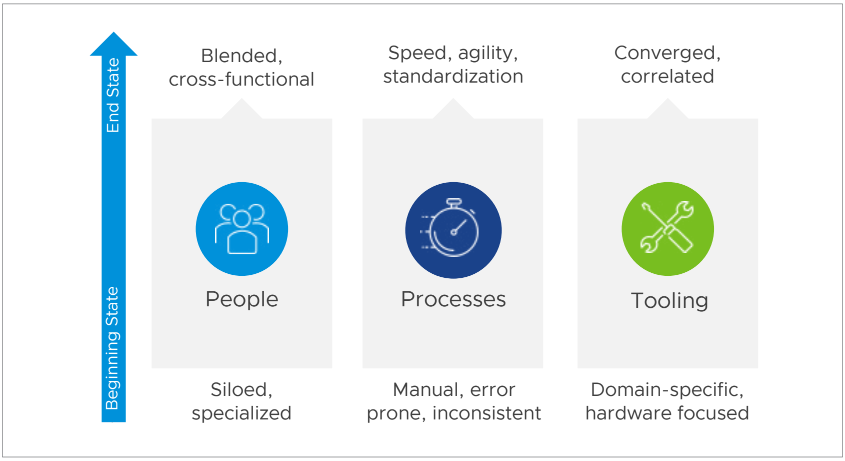

End State
Beginning State
Blended, cross-functional
Speed, agility, standardization
Converged, correlated
People
Processes
Tooling
Siloed, specialized
Manual, error prone, inconsistent
Domain-specific, hardware focused

Figure 1.1 Typical beginning state and target end state

Organizations using a traditional IT operating model of siloed functional teams often struggle with SDDC transition. Structured manual processes and domain-specific tooling can hinder NSX operationalization. It is important to work across these three dimensions: breaking down the siloed teams, automating processes to take advantage of software-defined capabilities, and moving towards stack-aware tooling. This will not only deliver the desired speed and agility but also help realize the full benefits NSX. This change will not happen overnight. Transforming people, process, and tooling to optimize operation of a software-defined environment should be evolutionary, not revolutionary.

Who the guide is for

This guide is meant both for people new to NSX as well as those who have implemented NSX and are looking to get more out of it. It is intended for:

- Organization-level decision makers who are concerned with the people perspective: organizational impacts, team structure, roles and skillsets, culture and mindset
- Managers responsible for or influential about operational processes such as change and configuration management
- Engineers and technical decision makers responsible for optimizing tooling to be more effective in a software-defined environment

In short, this guide provides a little bit of something for everyone who should be involved in operationalizing NSX.

What it will teach

This goal of this guide is to present an introductory perspective about what is required to operationalize an NSX environment. References to more detailed documentation will be provided where applicable.

Why it matters

For companies who have invested in NSX and the broader SDDC suite, the technology enables them to provide greater value to developers, application owners, and even end users. It is in their best interest to derive the greatest value from this investment. The guidance provided in this book will help individuals understand how best to unlock the business value of NSX and the SDDC. Software-defined solutions are the future; this book can help individuals build onto their career skillset while increasing their immediate personal value to their employer.

How to proceed

Different sections are more valuable to different readers. Organization-level decision makers would benefit from the entire book for context and increased understanding of how to unlock NSX's potential but "Measuring Progress" and "People Considerations" will be of primary interest, followed by "Process Considerations." Managers interested in optimizing operational processes should focus on the "Process Considerations" chapter. Technically-inclined individuals can focus in on the "Consuming NSX" and "Tools for Monitoring, Operations, and Troubleshooting" chapters.

Measuring Progress

Attempting to fit NSX into existing models is not a path to optimal value realization. Changes will be required to fully realize the benefits of NSX and as with any change, it is valuable to track progress and validate results.

Why measure

What good is undertaking the effort to change without measuring to demonstrate progress and return on investment? It is more powerful to back up talk of success with data—detailing the operational benefits and business impact associated with reduced application deployment time—rather than simply stating things are faster.

It is also good to measure progress and results to drive conversations that help teams improve. These efforts should focus on providing positive reinforcement to encourage continuous improvement rather than merely evaluating team performance.

How and what to measure

Begin with a good understanding of the current state of operational performance. Establish a baseline to measure improvement against, tracking progress to ultimately claim success. This book provides suggested key performance indicators to use as a starting point for measurement in specific important areas.

Finding quick wins and with whom to share results

Quick wins are key. Do not try to boil the ocean by making many changes at once. Start by focusing on processes that will deliver the most value to IT or end users with the least amount of effort. Choose a specific application or service for initial focus and create a tiger team as discussed in the "People Considerations" section.

For example, create a load balancer and apply it to the front end of a specific application. How long would it take to perform those steps in the physical world? How long would it take to purchase, burn-in, configure, and deploy a load balancer for a new application? Compare that to defining and deploying a software-based load balancer in NSX. What were the savings in pure deployment time as well as cost of both people and licensing? An examination such as this will help make the concept real.

With whom should results be shared? Up the management chain, down the management chain, and laterally to other teams within IT! This is a new technology and a new way of working with networking and security. Reinforce up the IT management chain how virtualized network and security implementation produces valuable IT and business outcomes. Further incentivize success through acknowledgement and recognition down the management chain. Market success laterally across IT to quiet naysayers and increase involvement as application of the virtualized network and security expands. Finally, do not forget about business stakeholders; actively communicate and market successes where they demonstrate relevant business outcomes.

Takeaway: Focus on quick wins and share the results up the management chain, down the management chain, and laterally to other teams within IT.

People Considerations

Whether a smaller IT organization just getting started or a larger IT organization focusing on truly becoming a service provider to business stakeholders, the ultimate goal is delivering business value. From an IT perspective this business value is most often provided via applications; however, these applications depend on platforms where software-defined networking and security are key enabling components. NSX is such an enabling technology, but to fully realize its potential for contributing to business VMware recommends some operating model optimizations. The starting point is the people perspective – aligning team structures, roles, and skillsets along with affecting cultural and mindset changes are the basis for these operating model optimizations.

Why SDDC (and NSX) changes the people equation

IT organizations are traditionally composed of technically-aligned functional groups. They were previously able to "get by" even as their environments increasingly shifted to compute and memory virtualization-based infrastructure. These organizations may have gained efficiencies and seen improvements in virtual workload deployment times by automating components of their virtual workload deployment process, but these efficiencies were at best incremental. As IT organizations now leverage fully software-defined infrastructures to become service providers and service brokers, "getting by" is no longer sufficient. The highly dynamic capabilities of cloud-based environments coupled with rapidly changing digital business needs demand more. If multiple functional teams are needed to deploy new applications or services the IT organization cannot quickly address modern digital business demands.

The challenge does not stop with technically-aligned functional teams. IT organizations of any size are inevitably organized in plan, build, and run silos. Architects make technical decisions and design solutions; engineering teams build and test the solutions architects provide them; and the solution is handed to IT operations to run. How long does this end-to-end process take? Or worse, how prepared is IT operations to run it?

This can extend beyond putting full solutions in production. One customer applied a subset of this process to developing new and modifying existing vRealize® Operations Manager™ dashboards. The goal was to provide better address monitoring workloads in their VMware Cloud on AWS environment. Operations had to provide requirements to a tools engineering team that provided the dashboards two months later. Once the operations team received the dashboards, they failed to provide what was needed.

Cloud-based infrastructures and platforms, whether on-premise or external, lend themselves to automation by providing fully software-driven and software-accessible capabilities. They allow workloads to be quickly implemented and changed, including the required networking and security constructs. With these additional automation opportunities, IT has the potential to provide previously unheard of levels of business value. This potential will never be reached using existing IT functional grouping constructs. Maintaining these constructs also prevents IT from adopting the Agile methodologies leveraged in application development —methodologies that lend themselves to making IT more responsive to and faster in delivering solutions that meet changing business needs.

Takeaway: Break down silos across two dimensions to be successful: plan-build-run and technically-aligned functional teams.

Team construction

VMware recommends a new team structure to leverage NSX software-defined networking and security capabilities in the context of cloud-based environments and platforms. The goal is a blended or integrated team; a team consisting not only of cross-functional technical skills but cross-domain roles. This is aimed at creating a much closer relationship between architecture, engineering, and operations for a cloud-based environment including NSX. This team will serve as the focal point for all decisions and actions regarding the environment.

The goal in creating a blended team is to break down the cross-functional and cross-domain IT silos, as shown in Figure 3.1, that inhibit agility and execution speed. It intends to replace them with a team built for tight collaboration and focus. Creating such a team results in faster and better decision making, reduced time to problem resolution, and more operationally ready solutions – all of which are critical to meet the demands of a digitally-driven business.

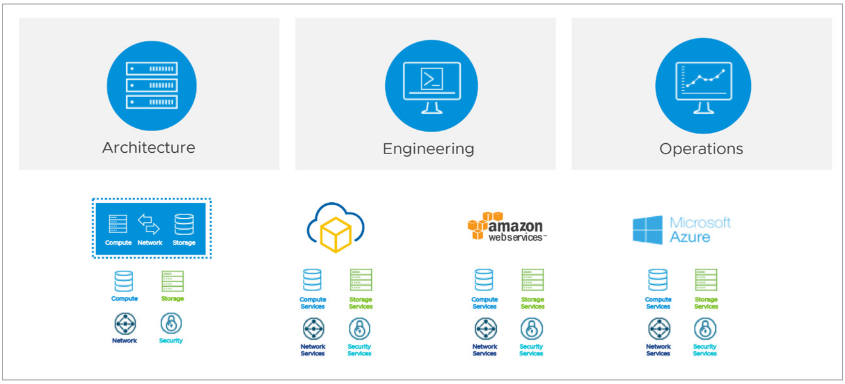


Figure 3.1 Cross-domain and cross-functional silos

Why is creating a blended, cross-domain team important for success with NSX and cloud-based environments? Organizations can no longer afford to have distinct plan, build, and run teams if they want to realize the agility afforded by fully software-defined infrastructures provided by cloud-based environments. Operations teams need to have more involvement in architecture and design decisions; for example, will the resulting cloud-based environment, solution, or service be built with the level of automation needed to support the rapid change in mind? Do the architects and engineers truly appreciate the operational flexibility of software-accessible cloud-based capabilities and services? Architects and engineering functions should wear the operational pager once a month to gain that appreciation. A tight feedback loop is needed between plan, build, and run when working with a software-defined infrastructure. This only works well, especially at scale, when these cross-domain functions are part of a blended team.

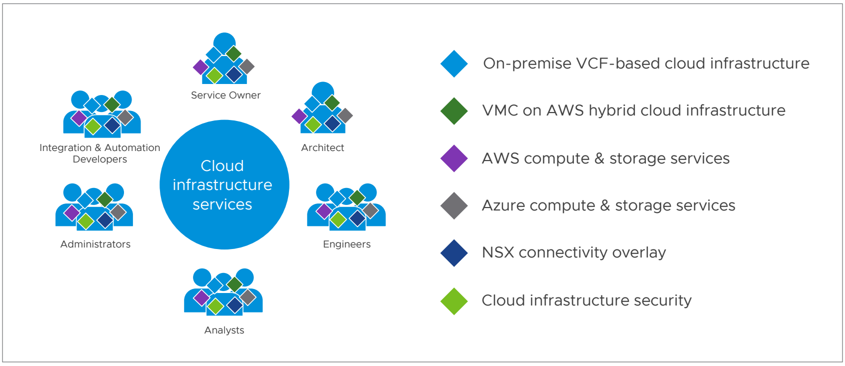

Service Owner
Integration & Automation Developers
Architect
Cloud infrastructure services
Administrators
Engineers
Analysts
On-premise VCF-based cloud infrastructure
VMC on AWS hybrid cloud infrastructure
AWS compute & storage services
Azure compute & storage services
NSX connectivity overlay
Cloud infrastructure security

Figure 3.2 Blended team example

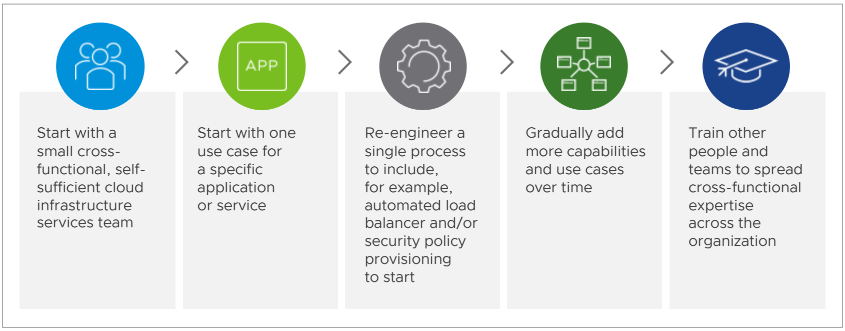
The same is true for breaking down technical silos and creating a blended, cross-functional team. This concept is shown in Figure 3.2. Relying on handoffs between cloud infrastructure services, networking, and security to accomplish a result in a cloud-based environment is antithetical to achieving agility and speed of execution. Where a line of business wants to rapidly begin developing a new mobile application to address customer feedback, waiting for IT to configure infrastructure does not a happy application developer make. For example, functional team-based ticket system-driven and backlog-driven tasking does not lend itself to taking advantage of NSX capabilities when deploying a new application development environment. These approaches must become a thing of the past to be successful in the modern cloud era.

This blended team can be physical or virtual, matrixed or under a single manager. There is no best answer as these decisions tend to be very company-specific and, often involving politics and cultural dynamics. Achieving the guiding principle of creating a blended, cross functional, cross-domain team is what matters, and it can work in various organizational and reporting structures. The common success factors are: the team is built with a clear purpose and shared objectives; they are incentivized on achieving team objectives more so than individual objectives; and they are as self-sufficient as possible with decision authority and the associated accountability to achieve their objectives. In addition to technical and domain skills, it is important to have an enthusiastic team of change agents who can naturally act as evangelists. This is a new way of working in most IT organization; they must embrace this change and make it infectious to others. This is essential to ensuring ongoing success as software-defined networking and security are increasingly critical to leveraging cloud-based infrastructure capabilities.

Takeaway: Forming a blended, cross-functional, cross-domain team is paramount. It is a company-specific decision whether this team is virtual or physical, matrixed or under a single manager.

Team size and specifics are circumstance dependent. Is IT just getting started with leveraging NSX in a new on-premises cloud-based environment? Is it adding NSX capabilities to an existing cloud-based environment or is this part of a larger, strategic multi-cloud implementation? Is the company merely experimenting with software-defined networking and security? Is this an all-in situation with a strategic decision already made to go with NSX?

A process for organizations just getting started with leveraging NSX capabilities or experimenting with software-defined networking and security is presented in Figure 3.3.



Start with a small cross-functional, self-sufficient cloud infrastructure services team

Start with one use case for a specific application or service

Re-engineer a single process to include, for example, automated load balancer and/or security policy provisioning to start

Gradually add more capabilities and use cases over time

Train other people and teams to spread cross-functional expertise across the organization

Figure 3.3 Getting started

Experience shows that an initial tiger team approach works best. For example, create an initiative focused around some aspect of IT automation such as provisioning virtual networking and security for an application development environment using VMware vRealize® Automation.™ To do this, define and create a blueprint, perhaps cloud agnostic, that can be standardized and used repeatedly. This type of effort requires input from the application team and all the infrastructure teams: cloud services, networking, and security. Controlling the resulting automatic provisioning service end-to-end—plan, build, and run—requires involvement from architecture, engineering, and operations. Pull together a cross-functional, cross-domain tiger team to drive this consensus-building initiative. Remember to baseline current and resulting metrics about provisioning networking and security for these application development environments. This will both prove the benefits of a blended team as well as put forth a data-driven argument for making it the standard going forward. Keep the decision-makers informed from the beginning of the initiative. Provide them with regular updates. Schedule a final readout session to sell the value of a blended team based on the data-driven, business-impacting results.

Takeaway: Start with a small, blended tiger team focused on a single use case for a specific application or service, then expand over time.

The approach for constructing a blended team for a strategic cloud-based initiative depends on acceptance of operating model changes. If this is understood and part of the strategic plan, the question comes down to lines of delineation. What does the existing data center networking team continue to support? What is the blended team responsible for the cloud-based infrastructure? What about security? A useful delineation can be the NSX Edge. This can be seen as both a point of collaboration as well as demarcation between the data center networking team and the blended team responsible for the virtualized infrastructure.

The NSX Edge is a logical point of collaboration and demarcation. The data center networking team responsible for physical networks retains responsibility for all physical networking while the network engineers on the blended team have responsibility for software-defined networking within their on-premises, cloud-based environment. It is a natural point of collaboration because it controls the routing between virtual networking environment and the physical networking environment. The NSX Edge pairs with a physical gateway/router using a protocol like BGP. The data center team responsible for the physical networking ensures that information for the networks outside of the virtualized environment propagates to the NSX Edge. The network-related roles on the blended, Cloud Infrastructure Services team ensure that information about the virtualized networks propagates to the physical gateway/router.

From a functional perspective, network, and security should both be represented in the roles on the team responsible for the cloud infrastructure services. The largest challenge here may be including security representation; it is often the more controversial of the two when creating a blended team with all the functional skills represented. The argument is for general IT security policy creation, monitoring, auditing, and enforcement to remain with the IT InfoSec team while the NSX-based implementation, monitoring, and remediation of IT security policy should reside on the blended team for operational agility, efficiency, and speed of execution.

Takeaway: Including a security role for NSX in a blended team may seem less obvious, but its absence will inhibit success.

If operating model optimization is not an inherent component of a larger NSX or cloud-based initiative, fall back on the same approach described to simply get started with NSX. Create a tiger team focused around a single activity or process that addresses the business justification. Create a baseline, track metrics, then sell the results in the context of demonstrable IT and business outcomes.

Creating a blended team is critical to fully leveraging NSX capabilities and achieving game-changing success when becoming an IT service provider. Without the commitment to create a blended team, expectations of dramatic improvements in agility or speed of execution will need to be managed. In this case it is still recommended to move forward with a tiger team exercise while measuring results against a baseline. Use this to champion additional temporary tiger teams to drive business impacting improvements using software-defined network and security capabilities. Following this approach can provide incremental improvements, but the challenge will be sustaining the improvement operationally. Continue toward the ultimate goal of gaining mindshare for creating permanent blended teams.

Roles, Skills, & Training

This section provides guidance on the recommended roles for software-defined networking and security. It also describes key responsibilities, skills, and training associated with each role. It only addresses the software-defined networking and security roles, not all the roles recommended for a fully blended team. For more information regarding the other roles in a blended team please download the “Organizing for the Cloud” whitepaper referenced in Table 8.1 of the “Where to go for more information” section.

Ensuring that teams have the right skills to maximize the value of their network virtualization investments is critical to success. Whether focused on a specific project or planning for a 12-18 month horizon, proactive training plans help right from the start. A good place to start in training plan development is an assessment of current and desired skills.

It is important to remember that this is a discussion of roles, not headcount. In small and mid-size environments, roles may be combined into a smaller number of individuals. In large, business critical environments, there may be multiple individuals performing a single role, perhaps with even greater degrees of specialization.

The recommended approach to a fully blended team in the broader cloud-based environment tends towards full stack knowledge with some specialization. Though it addresses the roles only in the context of software-defined networking and security, this section does provide a description of how they are impacted in an approach to fully blended teams for supporting services provided in a cloud-based environment.

While describing both a network and security architect role, an overall Cloud Architect role is recommended for a cloud infrastructure services blended team. This role would have more general network and security skillsets for a cloud infrastructure services blended team. In that case, focus the networking and security-specific skills respectively in network and security engineers. They will work closely with the cloud architect, providing the needed networking and security subject matter expertise.

Role	Responsibilities	Skills & Training
Cloud Network Architect	• Identify and prioritize use cases and business requirements to address with virtualized networking and security • Design logical network services for availability, capacity, mobility, recoverability, and data protection • Design standards and templates for automated virtualized networking provisioning and configuration management • Verify virtualized network solutions by developing and validating tests to ensure the success of addressing use cases and requirements • Identify modern tools for virtualized network orchestration and automation, and day-2 operations (e.g., observability and troubleshooting) • Guide the virtualized networking implementation strategy and assist operationally with onboarding new applications and services; establish new, optimized processes • Provide level 3 support as needed to work within defined SLA or OLA resolution period • Assist in defining and evolving overall IT network architecture and standards that maximize the synergy, reuse, and value of NSX over time.	• Cross-domain skills (e.g., virtualized network & security, VMware vSphere,® virtual distributed switching, network protocols, VMware Cloud) • VMware Training – Data Center Virtualization Fundamentals – NSX: Micro-Segmentation – Network and Security Architecture with NSX – NSX: Design and Deploy; NSX: Install, Configure, Manage; NSX: Troubleshooting and Operations; – NSX-T Data Center Design; NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations – NSX Advanced Load Balancer: Global Load Balancing Design and Deploy; NSX Advanced Load Balancer: ICM plus Troubleshooting and Operations Fast Track; NSX Advanced Load Balancer: Infrastructure and Application Automation – NSX Hands-on Labs • Certification: VCDX-Network Virtualization (NV) 2020 • Optional: Enterprise Learning Subscription (annual)

Role	Responsibilities	Skills & Training
Cloud Security Architect	• Identify and prioritize use cases and business requirements to address with virtualized security • Ensure compliance with relevant cybersecurity standards • Determine technical security requirements and translate them into security policies and standards; plan and guide the implementation of these security controls and solutions • Design standards and templates for automated virtualized security provisioning and configuration management • Verify virtualized security solutions; develop and implement efficient validation controls and tests • Determine auditing and reporting processes for virtualized security impacting compliance • Provide level 3 support as needed to work within defined SLA or OLA resolution period • Conduct security risk assessments for cloud workloads and infrastructure; provide authoritative advice and guidance on security strategies to manage the identified risk	• Cross-domain skills (e.g., virtualized network & security, vSphere, virtual distributed switching, access control, VMware Cloud) • VMware Training – Data Center Virtualization Fundamentals – Network and Security Architecture with NSX – NSX: Micro-Segmentation – Security Operations for the Software-Defined Data Center – NSX: Design and Deploy; NSX Install, Configure, & Manage; NSX: Troubleshooting and Operations – NSX-T Data Center: Design; NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations – NSX Advanced Load Balancer: Web Application Firewall Security – NSX security-related Hands-on Labs • Certification: VCP- Network Virtualization (NV) 2020 • Optional: Enterprise Learning Subscription (annual)

Table 3.1 Architecture roles

The Network Engineer and Security Engineer roles are key for blended teams, whether they be specifically NSX-focused or broader cloud infrastructure-focused. These network and security specializations are focused on the engineer roles regardless of whether they provide deeper networking and security subject matter expertise to the architect roles or designing profiles, workload blueprints, and policies implemented by the administrator roles.

The Cloud Automation & Integration Developer role is also included in Table 3.2 as it is a critical role in the modern software-defined data center. This role is important regardless of context – either in an NSX-focused or an SDDC-focused blended team. Automation is absolutely key to success going forward. Automation-related workflow development must move beyond administrators writing scripts and toward formal software development. This is a focus of the Cloud Automation & Integration Developer.

Role	Responsibilities	Skills & Training
Cloud Network Engineer	• Low-level design, deployment, and testing of the virtualized network functions that realize the virtualized network service; definition of the virtualized network function configurations; validation of virtualized network services functionality; operationalizing virtualized network services • Supports the Cloud Network Architect role in designing cloud network services and profiles; translating the requirements into blueprints and configuration templates for the network functions • Ensure fulfillment of requirements—including capacity, availability, security, compliance, and SLAs • Deploy, test, validate, and manage monitoring/ troubleshooting tools, processes, dashboards, runbooks • Work with the Cloud Automation and Integration Developer role to design, develop, test and deploy custom workflows and scripts leveraging the virtualized network infrastructure for use with integration, orchestration, deployment, monitoring, compliance, or other routine tasks. • Provide level 3 support as needed to work within defined SLA or OLA resolution period • Diagnose and analyze root cause of issues; apply patches and fixes as needed • Implement routine, approved, and exception changes in the infrastructure • Assess and test upgrades and patches for virtualized networking and security infrastructure and tools	• Cross-domain skills (e.g., virtualized network & security, vSphere, virtual distributed switching, network protocols, VMware Cloud) • VMware Training • Data Center Virtualization Fundamentals • NSX: Design and Deploy; NSX: Install, Configure, Manage; NSX: Troubleshooting and Operations; • NSX-T Data Center Design; NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations • NSX Advanced Load Balancer: Global Load Balancing Design and Deploy; NSX Advanced Load Balancer: ICM plus Troubleshooting and Operations Fast Track; NSX Advanced Load Balancer: Infrastructure and Application Automation • NSX, vRealize Operations, vRealize® Log Insight,™ and vRealize® Network Insight™ Hands-on Labs • Certification: VCP-NV 2020, VCAP-NV Design 2020, VCAP-NV Deploy 2020, VCIX-NV 2020 • Optional: Enterprise Learning Subscription (annual)

Role	Responsibilities	Skills & Training
Cloud Security Engineer	• Translates IT security policies into security controls appropriate to the cloud-based environment(s) • Designs, implements, deploys, configures, and monitors the security solutions and procedures for the cloud-based environment • Assists the Cloud Security Architect role in designing and planning the cloud security architecture, security policies, and security processes. • Works with the Cloud Automation & Integration Developer role to develop the workflows that orchestrate the security controls according to the security policy; develop security monitoring and remediation solutions, workflows and integrations. • Investigate identified security breaches in accordance with established procedures; recommend and implement any required action • Work with the IT security functional team to ensure that cloud security services integrate with existing tools and processes; validate that these fulfil IT security & compliance requirements • Manage security information—including logging, auditing, and reporting capabilities • Diagnose and analyze root cause of security-related issues; apply patches and fixes as needed • Implement routine, approved, and exception security-related changes in the virtualized infrastructure • Assess and test upgrades and patches for virtualized networking and security infrastructure and tools	• Cross-domain skills (i.e., virtualized security, vSphere, VMware Cloud, access control) • VMware Training – Data Center Virtualization Fundamentals – NSX: Micro-Segmentation – Security Operations for the Software-Defined Data Center – NSX: Design and Deploy; NSX Install, Configure, and Manage; NSX: Troubleshooting and Operations – NSX-T Data Center: Design; NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations – NSX Advanced Load Balancer: Web Application Firewall Security – NSX (security-related), vRealize Operations, vRealize Log Insight, and vRealize Network Insight Hands-on Labs • Certification: VCP-NV 2020 • Optional: Enterprise Learning Subscription (annual)

Role	Responsibilities	Skills & Training
Cloud Automation & Integration Developer	• Work with the Cloud Network and Cloud Security Engineers to design and develop code to enable integration with other systems or tools • Work with the Cloud Network and Cloud Security Engineers to establish integration and automation monitoring • Work with the Cloud Network and Cloud Security Engineers to establish automated virtualized networking and security service provisioning; establish event and incident remediation wherever possible and appropriate	• Skills: PowerShell, Python, Ansible), Configuration Management tools (Ansible, Chef, Puppet), Terraform, Orchestration tools (VMware vRealize® Orchestrator™), NSX Network and Security API, vRealize Automation API, VMware vRealize Operations API • VMware Training – Data Center Virtualization Fundamentals – NSX Advanced Load Balancer: Infrastructure and Application Automation – Data Center Automation with vRealize Orchestrator and PowerCLI – VMware Cloud Orchestration and Extensibility – vCenter Orchestrator: Develop Workflows • Optional: Enterprise Learning Subscription (annual)

Table 3.2 Engineering roles

The final two roles are the Network Administrator and Security Administrator. In addition to day-2 operations (e.g., backup & restore, upgrade & patching), the administrator roles are heavily focused on proactively monitoring and remediation of the virtualized network and security infrastructure. They are also responsible for working with the engineer and developer roles to customize the monitoring tools, continuously improving their proactive and predictive capabilities. The goal is to minimize the actual number of incident tickets received by proactively identifying and remediating issues before they become service or application disrupting.

Role	Responsibilities	Skills & Training
Cloud Network Administrator	• Monitor physical and logical network infrastructure and act on events before they affect services • Proactively monitor network performance (e.g., latency, throughput), health (e.g., faults, failures, connectivity), availability, and configurations • Proactively monitor and adjust NSX edge cluster capacity • Update and maintain virtualized networking infrastructure by utilizing alarm/alert mechanisms • Provide level 3 support for virtualized networking; narrow down the problem in physical or logical using modern tools • Investigate and diagnose logical network infrastructure and services incidents • Ensure solutions and fixes are applied to recover from network-related incidents • Implement and apply virtualized network policies designed and test by the Cloud Network Engineer • Backup and restore of NSX Manager data (e.g., system configuration, events, audit log tables) • Upgrade and patch virtualized networking and security infrastructure and tools • Define, develop, and test custom dashboards, super metrics, reports, etc., for virtualized networking infrastructure and services; work with the Cloud Automation & Integration Developer role to implement remediation automation capabilities	• Cross-domain skills (i.e., virtualized networking, vSphere, virtual distributed switching, network protocols, VMware Cloud) • VMware Training – Data Center Virtualization Fundamentals – NSX: Install, Configure, Manage; NSX: Troubleshooting and Operations; – NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations – NSX Advanced Load Balancer: ICM plus Troubleshooting and Operations Fast Track; NSX Advanced Load Balancer: Infrastructure and Application Automation – vRealize Operations for Operators – NSX, vRealize Operations, vRealize Log Insight, & vRealize Network Insight Hands-on Labs • Certification: VCP- Network Virtualization (NV) 2020, VCAP-NV Deploy 2020, VCIX-NV 2020 • Optional: Enterprise Learning Subscription (annual)

Role	Responsibilities	Skills & Training
Cloud Security Administrator	• Cloud Security Administrator • Monitor virtualized security services and act on events before they affect services • Proactively monitor virtualized security services performance, health, availability, and configurations • Engage in escalations affecting security in the SDDC-based cloud environment • Investigate and diagnose security incidents in the cloud-based infrastructure environment • Ensure solutions and fixes are applied to recover from security incidents in the cloud-based infrastructure environment • Implement and apply virtualized security policies designed and tested by the Cloud Security Engineer • Understand, apply, and maintain specific security controls in the cloud-based infrastructure environment as required by corporate security and compliance policies • Assist in the performance of cloud-based infrastructure environment audits • Ensure cloud-based workload and infrastructure comply with organizational standards for logging – including content, format, and location.	• Cross-domain skills (i.e., virtualized security, vSphere, VMware Cloud, access control) • VMware Training – Data Center Virtualization Fundamentals – NSX: Install, Configure, Manage; NSX: Troubleshooting and Operations; – NSX-T Data Center: Install, Configure, Manage; NSX-T Data Center: Troubleshooting and Operations – NSX Advanced Load Balancer: ICM plus Troubleshooting and Operations Fast Track; NSX Advanced Load Balancer: Infrastructure and Application Automation – vRealize Operations for Operators – NSX (security-related), vRealize Operations, vRealize Log Insight, & vRealize Network Insight Hands-on Labs • Certification: VCP- Network Virtualization (NV) 2020 • Optional: Enterprise Learning Subscription (annual)

Table 3.3 Administrator roles

This section described roles, not headcount or individuals. Depending on the scale and business criticality of an environment, multiple roles may be filled by a single individual or multiple individuals may fill a single role. The most important point is that these roles and skillsets exist in the blended team.

Takeaway: Focus on full-stack knowledge with some specialization when filling roles and putting together training plans for blended teams.

Note: Enterprises are increasingly embracing the Site Reliability Engineering (SRE) concepts first developed by Google.[1] While SRE

[1] Benjamin Treynor Sloss. "Introduction to Site Reliability Engineering: How Google Runs Production Systems." Edited by Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Murphy. O'Reilly Media, 2016.

concepts were originally developed in the context of supporting applications, it can be applied equally to IT services[2] including those involving NSX. In the context of the roles described above, SRE Practitioners are a combination of the Cloud Network/Security Engineer and Cloud Automation and Integration Developer roles. The SRE Practitioner is especially applicable in the context of automating NSX operational capabilities, for example, automating networking and/or security capabilities as part of the workload provisioning process or automating NSX day-2 operations.

Culture & mindset

Culture and mindset is the equivalent of the organization's DNA—the values and beliefs that shape how people behave and create the organization's culture. This is the single most impactful factor influencing success or failure for adoption of software-defined networking and security. It is also the most difficult to change. This is one of the first things to assess when getting serious about implementing NSX.

The ideal culture is one that embodies collaboration and is guided by a focus on business outcomes. It consists of a team of full stack generalists with some specialization who are interested in continuous learning and improvement; a team both responsible and accountable for achieving objectives they acknowledge as owning. Many of these characteristics are associated with the Agile culture popular in application development teams. This represents a rare breed of organization, though it is critical for success.

How can an organization move toward this state? There are entire books devoted to answering this question, but some guidance includes:

- Start with leadership. Cultural change must be embraced from the top down, even if it is only realized in the NSX or SDDC blended team.
- Leadership must articulate a clearly defined direction for the blended team and modify incentives to reinforce shared team objectives.
- The team must be given ownership, responsibility, and accountability for achieving the stated purpose and shared objectives.
- The members initially selected for the blended team must be like-minded change agents; they must be open-minded and passionate about instituting the culture.

[2] "Site Reliability Engineering (SRE): SRE with VMware Professional Services," VMware, November 2018, blogs.vmware.com/services-education-insights/files/2018/11/SRE-Paper.pdf

- Team successes must be recognized and advertised; the goal is to make their behavior aspirational for others in IT. What the team is doing and how they are progressing should be actively marketed within IT to key business stakeholders.

Overcoming cultural challenges is the biggest hurdle and should be explicitly addressed from the beginning.

KPIs to measure progress

Key Performance Indicators (KPIs) are used to measure progress towards target state objectives. These objectives, in turn, should clearly communicate the definition of success. Target state objectives are company or organization specific, with their goals tied to distinct IT and business outcomes. Table 4 offers some general purpose KPIs for measuring progress towards establishing software-defined networking and security blended teams. As establishing baselines for comparative measurement further increases value, build these into the KPIs from the beginning.

Objective	KPI	Description
Self-sufficient team	• % of escalations resolved within the blended team • Average time to resolve escalations with the blended team	These KPIs provide a measure of blended team efficiency in resolving issues versus the baseline of how long it previously took to resolve escalations across siloed teams.
Encourage blended teams	• Number of software-defined networking issues escalated to data center networking team	This KPI can be useful if managers are reluctant to embrace the blended team approach. This KPI can be applied to any manager of a siloed team.
Shared objectives	• Team-based annual review criteria as a % of team member's review criteria • Average time to complete cross-functional activities within the blended team	These KPIs provide a measure of a blended team's efficiency in completing cross functional activities (e.g., on-boarding a new application) when they have team-based objectives versus the baseline of completing a similar activity involving siloed teams with competing objectives.

Table 3.4 Sample team structure KPIs

Process Considerations

Intelligent Operations

Most IT organizations cannot break out of firefighting mode; they are constantly reacting to monitoring events and alerts generated in their environment. They are also plagued with laborious operational tasks consisting of error-prone manual steps. Applying this mode of operation to an NSX-based environment will not deliver the full benefit of software-defined networking and security. It will minimize the agility and speed of execution opportunities provided by NSX software-defined networking capabilities. The concept of “intelligent operations” refers to a modern, proactive mode of operation that optimizes and automates processes and workflows to take advantage of software-defined networking and security capabilities. This is contrasted against a more traditional reactive mode of operation with its constant focus on break/fix activities and lack of time for innovation and improvement. It is also about using the right tools for the job – tools purpose-built for achieving a level of intelligent operations in a software-defined infrastructure.

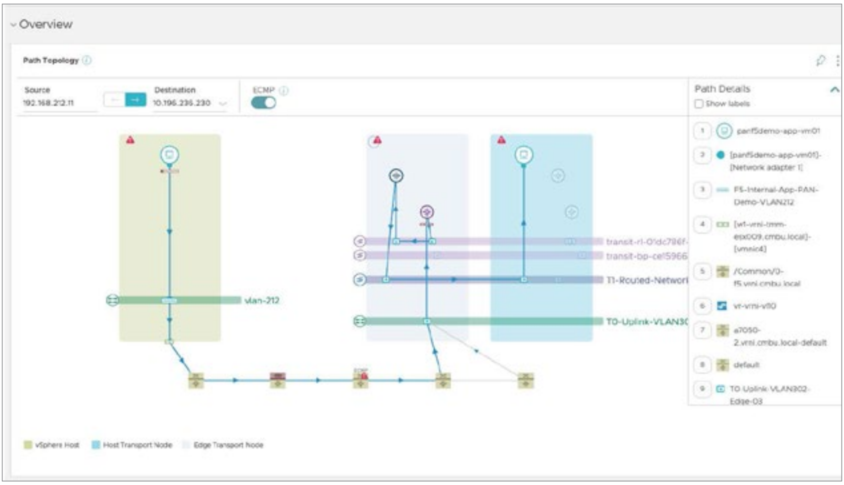
This chapter outlines how the concept of intelligent operations can be applied to software-defined networking and security, focusing on optimizing and automating the activities and processes most impacted by NSX. Examples will be based on VMware’s vRealize tools. Descriptions of general tool capabilities will be used to aid in substitution as necessary.

Proactive monitoring for performance and availability

Proactive monitoring is more about mindset change than technology. It involves proactively monitoring key metrics, analyzing potential issues, and remediating those issues before they become service, application, or end-user impacting. Even when focused on software-defined networking and security, proactive performance and availability monitoring puts more emphasis on monitoring from a service- or application-centric perspective. An example may be Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) provided to application developers or Data Analytics as a Service consumed by lines of business. While implementing proactive monitoring depends on a mindset shift, the selection of proper monitoring tools is also an important factor in its overall effectiveness.

What does it mean to put more emphasis on monitoring from a service- or application-centric perspective? First and foremost, this means monitoring the full, integrated stack where an application or service is running. This involves monitoring the VMs that comprise the application or service, the hypervisor and host, storage, and the end-to-end network path—anything that impacts the application or service if there is an issue in the stack. It includes monitoring common metrics such as CPU performance, memory utilization, network throughput, and storage throughput latency. This is all done within the context of any service level agreements associated with the application or service. If a service level agreement is involved, best practice includes setting monitoring thresholds at some percentage below the service level threshold to provide a buffer, allowing time to troubleshoot before an issue impacts the application or service.

It is worth adding a quick check of end-to-end network health for tier one applications to the daily routine. This is easily done with vRealize Network Insight's topology-based 360˚ visibility and analytics, as shown in Figure 4.1



Source
192.168.212.11

Destination
10.196.236.230

Path Details
□ Show labels

1 panf5demo-app-vm01
2 [panf5demo-app-vm01]-[Network adapter 1]
3 F5-Internal-App-PAN-Demo-VLAN212
4 [w1-vrni-tmm-esx009.cmbu.local]-[vmnic4]
5 /Common/0-f5.vrni.cmbu.local
6 vr-vrni-v80
7 a7050-2.vrni.cmbu.local-default
8 default
9 T0 Uplink VLAN302-Edge-03

Figure 4.1 Example of vRealize Network Insight's 360˚ visibility

What if the NSX Edge providing the load balancing or VPN service supporting an application starts trending towards lower throughput or high latency? One effective tool to monitor the NSX Edge is vRealize Operations Manager. vRealize Operations Manager can monitor the NSX Edge as a virtual machine, taking advantage of vRealize Operations Manager's intelligent analytics engine. The intelligent analytics engine can learn the normal behavior of the VM containing the NSX Edge, then alert when it trends outside of its learned behavior or exhibits anomalous behavior.

While monitoring will identify issues with the VM containing the NSX Edge, it may not be straightforward to link the problem back to the application in the environment. Use of vRealize Network Insight to review the status of all application components in the full end-to-end path will greatly aid in proactively managing application performance and availability.

KPIs

Objective	KPI	Description
Proactive performance monitoring	• Number of performance-related issues detected and resolved before they become service or application impacting incidents • % reduction in performance-related incidents month over month	These KPIs provide a measure of the effectiveness of proactive performance monitoring over time.
Proactive availability monitoring	• Number of availability-related issues detected and resolved before they become service or application impacting incidents • % reduction in availability -related incidents month over month	These KPIs provide a measure of the effectiveness of proactive availability monitoring over time.

Table 4.1 Sample proactive performance and availability monitoring KPIs

Proactive capacity monitoring and planning

Similar to performance and availability monitoring, proactive capacity monitoring and planning involves shifting a mindset to proactively identifying and remediating capacity issues before they become service, application, or end-user impacting. Unlike proactive performance and availability monitoring—which is best approached from a service- and application-centric perspective—proactive capacity monitoring and planning for software-defined networking and security focuses on the NSX components themselves. There are three main areas of focus for capacity monitoring and planning of a software-defined network and security-based environment: NSX Manager/Controllers, NSX Edge cluster, and workload clusters utilizing NSX.

It is important to always monitor NSX Manager and NSX Controllers from a capacity perspective, and especially so in a multi-site environment. When running a multi-site NSX Manager configuration, be certain to monitor inter-site network-related capacity. NSX Managers need to synch with one another in a multi-site NSX Manager configuration, and this ability is directly related to inter-site throughput and latency. There is a maximum supported latency of 150 milliseconds between sites for synchronization. Please note that as of NSX-T Data Center version 2.4, the NSX Manager and NSX Controllers have been merged into a single appliance. The merged capability can manage a remote vSphere host (known as a Transport Node in NSX-T Data Center) as long as the maximum 150 millisecond latency is met.

In a multi-site environment, NSX Controllers interact with remote vSphere hosts. As with NSX Managers, the NSX Controller interaction with remote vSphere hosts in multi-site environment is also dependent on inter-site network throughput and latency. NSX Controllers are also sensitive to disk latency, which should be monitoring in both single and multi-site environments. While the NSX Manager and NSX Controller are merged into a single appliance as of NSX-T Data Center version 2.4, the controller component of the merged appliance communicates with the vSphere hosts.

NSX Edge Nodes are one of the most important components to proactively monitor. NSX Edge services (e.g., load balancing, VPN) have a direct impact on services, applications, and end-users. CPU, memory, and throughput capacity can directly impact load balancer and VPN effectiveness. Valuable metrics to monitor include: CPU Demand, CPU Run Queue, CPU Swap Wait, CPU I/O Wait, Ram Free, Ram Committed, Page-in Rate, and Network Usage. It is also recommended to monitor the number of NSX Edge Nodes per host, ensuring the maximum recommended number is not exceeded. To assist further with NSX Edge capacity, as of NSX-T Data Center version 2.5, new API calls have been added through which the Cloud Network Administrator can monitor the NSX Edge capacity in terms of load balancing instances. In addition, as of the same NSX-T Data Center version, an SNMP manager is used for monitoring using NSX-T Data Center MIBs. As of version 3.0 the ability to send SNMP alarms has been added.

It is useful to proactively monitor distributed firewall memory usage at the host level in workload clusters as firewall rules are replicated across vNICs. If the memory usage maximum is reached, no additional firewall rules can be deployed.

KPIs

Objective	KPI	Description
Proactive capacity monitoring	• Number of capacity-related issues detected and resolved before they become service or application impacting incidents • % reduction in reported capacity-related incidents month over month	These KPIs provide a measure of proactive capacity monitoring effectiveness for example of the Edge cluster. (Requires Proactive Issue Resolution checkbox along with Capacity Incident Category in ITSM tool)
Proactive capacity planning	• Average amount of time in advance of on-boarding a new application or service that requirements for additional NSX Edge cluster capacity are identified • Average amount of unused capacity in the NSX Edge cluster month over month	These KPIs provide a measure of the effectiveness of proactively planning capacity needs for new applications as well as the accuracy of proactive capacity planning.

Table 4.2 Sample proactive capacity monitoring and planning KPIs

Change management

Software-defined networking and security can and will have an impact on change management. NSX is software-based, leading to fewer change management activities in the physical network. This can reduce the overall change scope, lessening the impact on infrastructure and dependent applications and services. Since NSX is policy-based, it can be automated to avoid the most significant cause of change back-outs (i.e., manually applied changes). As NSX is software-defined and policy-based, it is easier to perform validation tests in advance of a change being applied in production.

This is especially true when automatically deploying NSX capabilities via tools with blueprint capabilities such as vRealize Automation. In this model, blueprint changes can be handled through the change control process while workload or application deployment into production is a pre-approved change. This is most applicable where the same blueprint is used repeatedly for deploying workloads or applications into production.

Change management support has been further enhanced in NSX-T Data Center version 2.5. As of this release, firewall configuration copies are automatically saved when a firewall rule is published. The saved configuration can be re-deployed to rollback to an existing state if an issue is discovered in a newly published firewall rule. This has been further enhanced as of version 3.0 with the addition of a GUI to manage timelines and rollback.

Another example of change management process modification is the use of NSX for micro-segmentation. In this example, a firewall policy model for micro-segmentation consists of five types of firewall rules:

- Emergency firewall rules used for quarantine and/or allow rules for example
- Infrastructure firewall rules – global firewall rules applied to common object or services (e.g., AD, DNS, NTP, DHCP, management servers)
- Environment firewall rules, including firewall rules between zones (e.g., production vs development), PCI vs non-PCI, and inter-business unit rules
- Inter-application firewall rules, rules between applications
- Intra-application firewall rules (e.g., rules between application tiers, rules between micro-services)

Based on this example, how might change management be applied in the micro-segmentation scenario shown in Figure 4.2 where each bubble represents an application isolated using security policies?

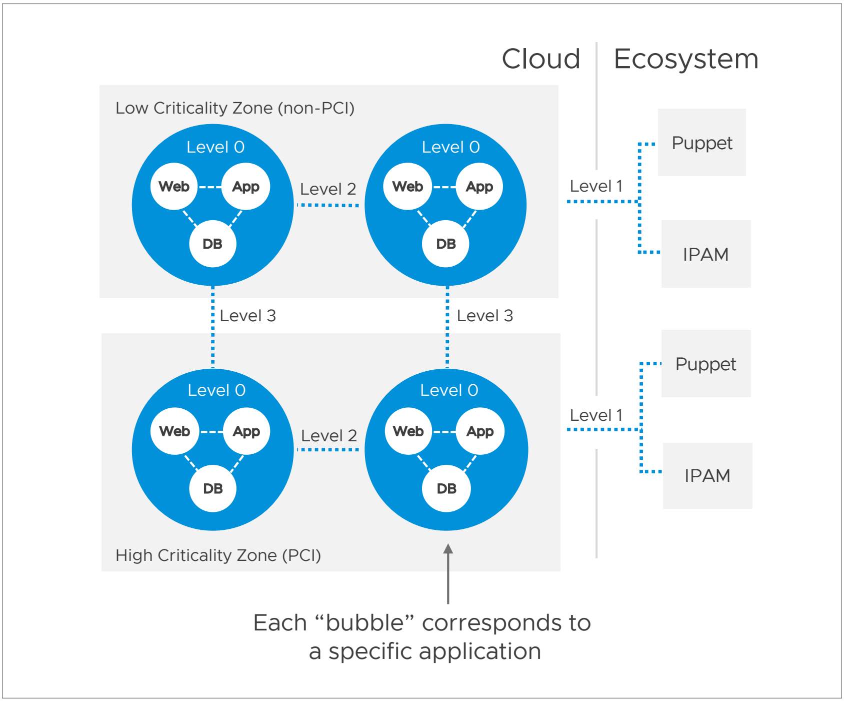


Figure 4.2 Example of micro-segmentation in a multi-application deployment

The following bullets discuss the considerations and impact on the standard change management process for this scenario:

- Level 0 represents isolated, multi-tier applications. Intra-application firewall rules are controlled by application developers and may not require any change approval.

- Level 1 represents infrastructure services defined in the deployment blueprint and accessed at provisioning time. These are controlled and validated by the team providing the IaaS workload. Change management is applied to the blueprint, so deployment from the blueprint is pre-approved.

- Level 2 represents inter-application firewall rules allowing communication between two applications within a low criticality zone. Applying these firewall rules could be pre-approved since they can be extensively validated prior to production deployment. Though pre-approved, automatically creating, filling out, and closing a change ticket when the firewall rules are applied could be done for auditing purposes

- Level 3 represents inter-application firewall rules similar to level 2, but controls communication between applications in different criticality or confidentiality zones. Applying these firewall rules should be subject to standard change control procedures.

The potential impact on change management can have a direct effect on the agility and time to value business stakeholders will experience. Because of the potential impact, it is a best practice to actively monitor the effect of the normal changes as they are being made in production. This also represents another advantage of a blended team model; all team members will be involved by default. They will know to monitor normal changes as they are being made and will be extra vigilant with monitoring when pre-approved changes take place, greatly enhancing the likelihood of successful change management.

KPIs

Objective	**KPI**	**Description**
Positive impact on change management by having a blended team	• Ratio of terminated changes to successful changes	This KPI provides a measure of blended team efficiency in planning and executing changes versus the baseline of the same metric for changes involving siloed teams.
Increase in number of automated standard changes	• Total number of automated changes versus manual changes per month	This KPI provides a measure of the number of automated changes completed, indirectly reflecting a reduction in the cost of operations.
Increase number of pre-approved standard changes	• Total number of pre-approved Standard Changes compared to Normal and Emergency Changes	This KPI provides a measure of what should be an upward trend in the number of standard changes with a downward trend in the number of emergency and normal changes.

Table 4.3 Sample change management optimization KPIs

Configuration management

The software-defined nature of NSX simplifies configuration management when coupled with automation. When using vRealize Automation to perform workload deployments, all the software-defined, logical components are tracked in blueprints that can be put under version control. Configuration information can be automatically inserted, updated, and marked as decommissioned or deleted in a CMDB as part of a vRealize Orchestrator workflow invoked from vRealize Automation. Either in conjunction with vRealize Automation blueprints or used standalone, Puppet manifests, Chef recipes, or Ansible playbooks can be used to keep NSX-related configurations consistent. Any of these configuration management tools can automatically check for and remediate configuration drift.

An example of using an Ansible playbook to manage NSX logical switch state can be found in the "Automation Leveraging NSX REST API" link in Table 8.1.

If there is no corporate CMDB or it does not include NSX network or security configuration information, there are still solutions for auditing configuration changes. NSX components can send their logs to remote syslog servers or vRealize Log Insight. Using vRealize Log Insight makes it easy to filter audit log files for configuration change instances. These can then raise security alerts or generate reports. The NSX Controllers also keep track of all deployed software-defined networking components. These can be extracted and reported on through the NSX Manager REST API.

KPIs

Objective	KPI	Description
A change record should exist for any configuration changes	• Number of configuration changes without a corresponding change record	Whether updating a blueprint, Puppet manifest, Chef recipe, Ansible playbook, or creating or changing a configuration item in a CMDB, there should be a record in the change management tool. The change record could have been manually or automatically created.

Table 4.4 Sample configuration management optimization KPI

Provisioning NSX capabilities

Many organizations have focused on automated provisioning of virtual infrastructure and workloads. This may involve offering IaaS to users or simply expediting the deployment of virtual infrastructure and workloads by IT on the user's behalf.

Without the capabilities of NSX, networking and security aspects must still be provisioned manually. This slows down the provisioning process, impacts user wait times, and increases the probability of introducing human error. Human errors account for at least 40% of network failures.

These errors can lead to misconfigurations that result in an unusable environment and further user wait time as the misconfiguration is corrected. The software-defined nature of NSX helps avoid such problems, allowing IT to fully automate the networking and security aspects of virtual infrastructure or workload provisioning.

As organizations adopt micro-segmentation, much more granular, application-specific security policies need to be deployed. This further reinforces the importance of automation; manual processes fail as scale increases. This is especially problematic when trying to maintain a consistent production environment throughout an Agile application development lifecycle.

The NSX REST API is used by several Cloud Management Platforms (CMPs) to automatically provide NSX services (e.g., vRealize Automation, VMware vCloud Director,® OpenStack, and VMware® Integrated OpenStack). vRealize Automation is of particular interest due to its tight integration with NSX.

vRealize Automation provides native consumption of both pre-built and on-demand NSX network and security services. As of vRealize Automation 7.1 and NSX 6.2, as well as vRealize Automation 8.1 for NSX-T Data Center, organizations can provide end users the ability to automatically deploy a completely secure and compliant application topology utilizing NSX networking and security services. As of vRealize Automation 8.1, organizations can provide on-demand networking and load balancers for on-premises SDDC environments, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). This is defined through vRealize Automation blueprints as shown in Figure 4.3.

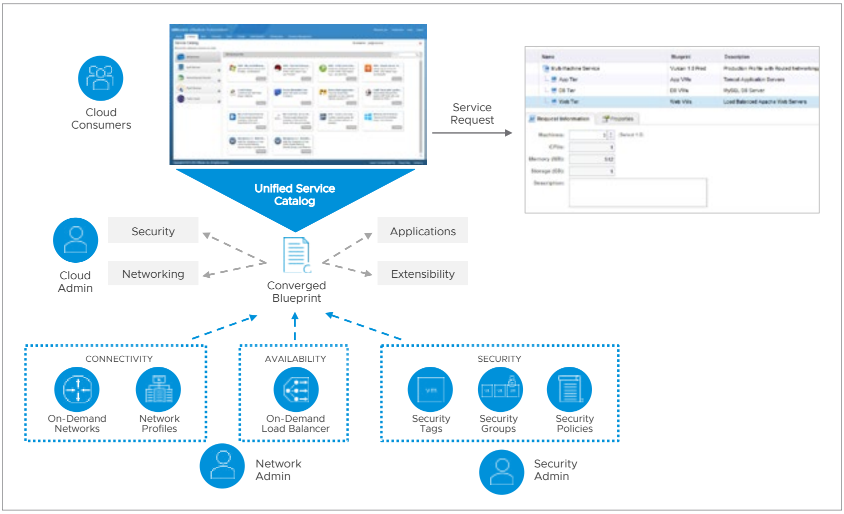


Figure 4.3 vRealize Automation and NSX

The blueprint design canvas in VMware Cloud Assembly™ allows graphical design of end-to-end blueprints from virtual infrastructure up through a multi-tier application topology. For NSX, this includes creating:

- On-demand routed and NAT networks using network profiles
- Connections to pre-created external networks via existing NSX logical switches
- On-demand NSX logical switches and connecting them to pre-created NSX distributed logical routers
- In the case of NSX-T Data Center, on-demand tier-1 logical router and connecting it to a tier-0 logical router
- An application-based security group with a default policy permitting traffic between tiers while blocking all inbound and outbound traffic for application isolation
- On-demand NSX security groups based on NSX security policies
- Membership in existing NSX security groups by specifying pre-defined NSX security tags
- An on-demand NSX load balancer in one-armed mode or in-line mode as well as specify existing load balancers

This results in an integrated capability as shown in Figure 4.4. It also reinforces the need for blended teams as described earlier. Success with this level of integration and automation requires close cooperation between virtual compute, network, security, and storage resources.

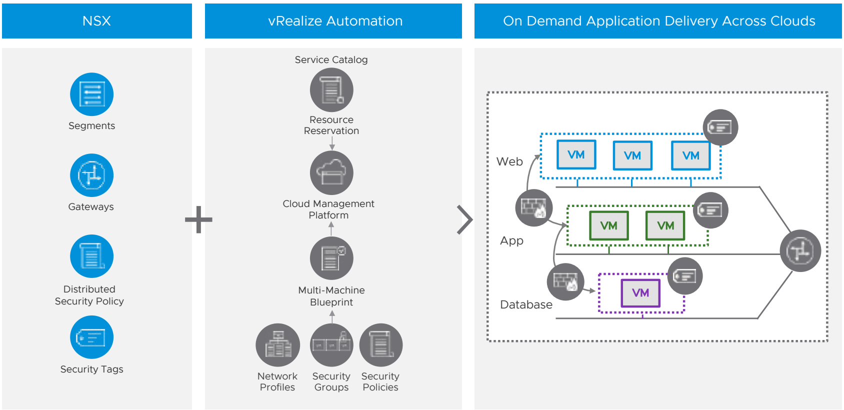
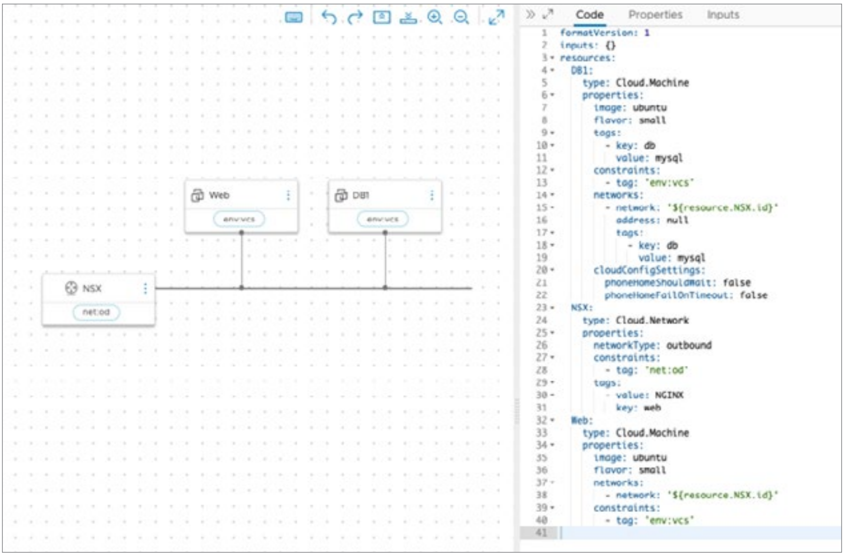


Figure 4.4 vRealize Automation and NSX integrated capability

vRealize Automation uses vRealize Orchestrator and, as of vRealize Automation 8.0, Action Based Extensibility (ABX), allowing for out-of-the-box integration using the Event Broker Service and XaaS features of vRealize Automation. The Event Broker Service allows subscribing vRealize Orchestrator workflows or ABX actions to specific events, modifying the behavior of the NSX native integration. XaaS allows publishing of vRealize Orchestrator workflows in vRealize Automation which can then be directly invoked from the VMware Service Broker™ catalog. In addition, as of vRealize Automation 8.1, there is an IPAM SDK which is a toolkit for enabling integration of third-party IPAM providers with vRealize Automation.

Blueprint-based integration between vRealize Automation and NSX allows deployment of full application stacks from the Service Broker catalog. This provides users with the benefit of quickly deploying a fully configured, secure, and networked application stack within the framework of a standardized and repeatable process. An added benefit of using blueprints is the ability to treat infrastructure as code, allowing version control as part of an overall lifecycle management strategy. An example of infrastructure as code including NSX and its associated graphical representation is shown in Figure 4.5.



```
formatVersion: 1
inputs: {}
resources:
  DB1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      tags:
        - key: db
          value: mysql
      constraints:
        - tag: 'env:vcs'
      networks:
        - network: '${resource.NSX.id}'
          address: null
          tags:
            - key: db
              value: mysql
      cloudConfigSettings:
        phoneHomeShouldWait: false
        phoneHomeFailOnTimeout: false
  NSX:
    type: Cloud.Network
    properties:
      networkType: outbound
      constraints:
        - tag: 'net:od'
      tags:
        - value: NGINX
          key: web
  Web:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.NSX.id}'
      constraints:
        - tag: 'env:vcs'
```

Figure 4.5 Example of infrastructure as code

KPIs

Objective	KPI	Description
Decrease average end-to-end workload provisioning time due to automating and continuously improving network and security-related steps.	• End-to-end monthly average workload provisioning time	This KPI should show a decrease in pre-provisioning and post-provisioning due to automating what had been manual network and security-related activities.
Increase workload provisioning success rate due to automating network and security-related steps.	• Monthly workload provisioning success rate • Monthly cost of provisioning failure	• Monthly workload provisioning success rate tracks total number of workloads requested, total number of workloads successfully provisioned, and total number of workload provisioning failures month over month which should reflect an increasing trend in the success rate. • Monthly cost of provisioning failure tracks the estimated or actual cost of workload provisioning failures which should decrease over time due to fewer failures.

Table 4.5 Sample integrated NSX provisioning optimization KPIs

Incident Management

Incident management is also impacted in the context of operationalizing NSX. A number of tools and advanced capabilities can be applied to NSX; the section "Tools for Monitoring, Operations, and Troubleshooting" will provide additional details on these possibilities. Some, like vRealize Log Insight, have content packs available to explicitly include NSX metrics and events. Others, like vRealize Operations Manager, can apply their advanced capabilities (e.g., dynamic thresholds, predictive analytics) to NSX components. Tools such as vRealize Network Insight have been purpose-built for NSX to provide additional benefits (e.g., correlating physical and virtual network constructs). A new tool as of NSX-T 2.5 is VMware NSX® Intelligence.™ This tool simplifies security incident and policy configuration troubleshooting by providing a complete inventory of workloads along with continuous layer 7 analysis and visualization of every flow between workloads. Used separately or together, these tools can significantly streamline troubleshooting and resolution across the software-defined networking and security infrastructure.

NSX is software-defined with a REST API, easing integration with orchestration engines (e.g., vRealize Orchestrator) or intelligent operations tools (e.g., vRealize Operations Manager). This also allows for integration of NSX directly with 3rd party ITSM tools such as ServiceNow, an aspect particularly useful in the context of intelligent operations. A goal of intelligent operations is to identify and resolve issues before they impact a service or application. To help track the effectiveness of adopting an intelligent operations mindset, it is useful to track the ratio of issues resolved reactively (i.e., traditional incident management) against those resolved proactively. One strategy for this is to add the capability to mark entries in an ITSM tool's incident management module as "Resolved Proactively." vRealize Operations Manager can then invoke a vRealize Orchestrator workflow that creates an incident ticket with the pertinent information and is marked as "Resolved Proactively." This streamlines tracking the ratio of incidents resolved proactively to those resolved reactively for an NSX-based infrastructure.

Implementing the blended team model described earlier also streamlines incident management. A blended team acting collectively with shared knowledge is able to resolve issues much faster than the traditional model of siloed team hand-off and communication. This is especially valuable when there is pressure from a critical severity incident.

KPIs

Objective	KPI	Description
Decreased time to troubleshoot and remediate an incident due to blended team	• % of escalations resolved within the blended team • Average time to resolve escalations with the blended team	This KPI provides a measure of how effective the blended team is in resolving incidents.
Increase in the number of issues proactively resolved	• Number of NSX-related issues detected and resolved before they become service or application impacting incidents • % reduction in NSX-related incidents month over month	This KPI provides a measure of how effective proactive monitoring is in identifying and resolving issues before they become service or application impacting.

Table 4.6 Sample incident management impact KPIs

Compliance management

Isolation of applications for security or regulatory compliance is a major use case for NSX micro-segmentation and distributed firewalls. Integration of NSX distributed firewall rules with Active Directory allows for granular application access based on AD user groups. NSX distributed firewall rules can control application communication, allowing communication between application tiers while simultaneously restricting external inbound access based on port groups and other attributes. Distributed firewall rules are defined in NSX security policies and can be applied using NSX security groups. These security groups include all tiers associated with a multi-tier application, simplifying comprehensive application isolation. For an excellent treatment of NSX micro-segmentation—including designing and defining NSX security policies and security groups—see Wade Holmes' "VMware NSX Micro-segmentation: Day 1." A URL for this book is provided in Table 8.1.

Once security policies are created and applied to security groups, how are they managed on an ongoing basis? How best to monitor access and communication activity while supporting audit requests? There are several recommended solutions depending on the tools available in the environment.

At the most basic level, access log entries are generated by distributed firewall events on a vSphere host, NSX Manager, or through the vSphere Web Client. The distributed firewall operations are run directly from the vSphere hosts.

Distributed firewall packet logs can be viewed locally on each vSphere host:

- Distributed firewall packet logs can be found at **/var/log/dfwpktlogs.log**
- Distributed firewall User World Agent (UWA) logs: **/var/log/vsfwd.log** (NSX Data Center for vSphere only)

System events for distributed firewalls are accessed by downloading the tech support logs from:

- NSX Manager administration GUI at Home -> Download Tech Support Log (NSX Data Center for vSphere)
- NSX Manager GUI at Systems -> Settings -> Support Bundle (NSX-T Data Center)

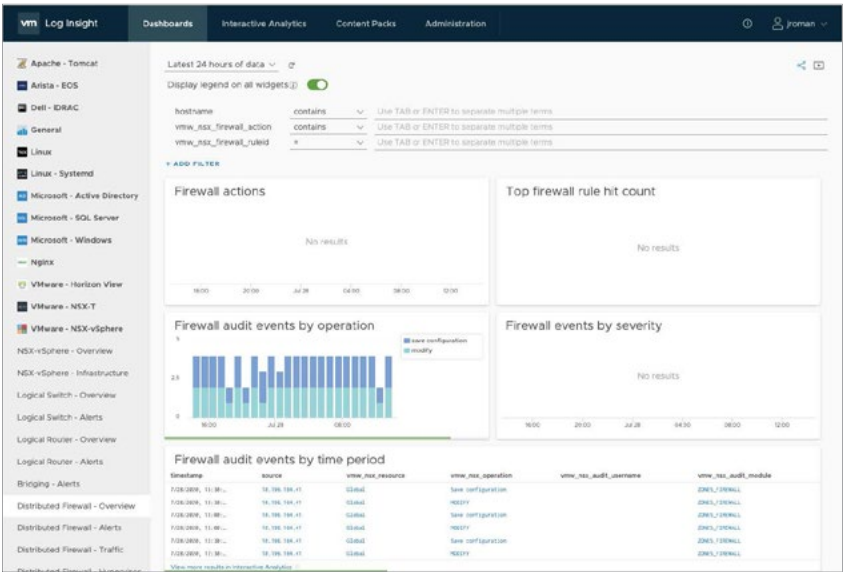
This will generate a gzip file that can be downloaded for viewing/ troubleshooting. Logs can also be sent to a remote syslog server (e.g., vRealize Log Insight) for easier analysis.

Audit logs associated with a specific vSphere host, including access control and firewall events, are viewed through the vSphere Web Client in the Networking & Security -> NSX Manager menu. This interface can display raw audit log details as well as just the properties whose values have changed for a selected operation within an audit log.

The next level of distributed firewall auditing for compliance includes access monitoring. This can be done via the vSphere Web Client at Networking & Security -> Activity Monitoring. The following audit capabilities are available:

- User access (e.g., monitoring all VM access activity from Active Directory groups)
- Application access (e.g., monitoring access from VMs to a specific application)
- Inter-VM access (e.g., monitoring user- or service-to-application and VM-to-application access)

vRealize Log insight can perform more advanced distributed firewall auditing. It provides an easy yet powerful way to monitor and analyze distributed firewall rule events. A sample of out-of-the-box dashboards used to view summary-level distributed firewall events is shown in Figure 4.6.

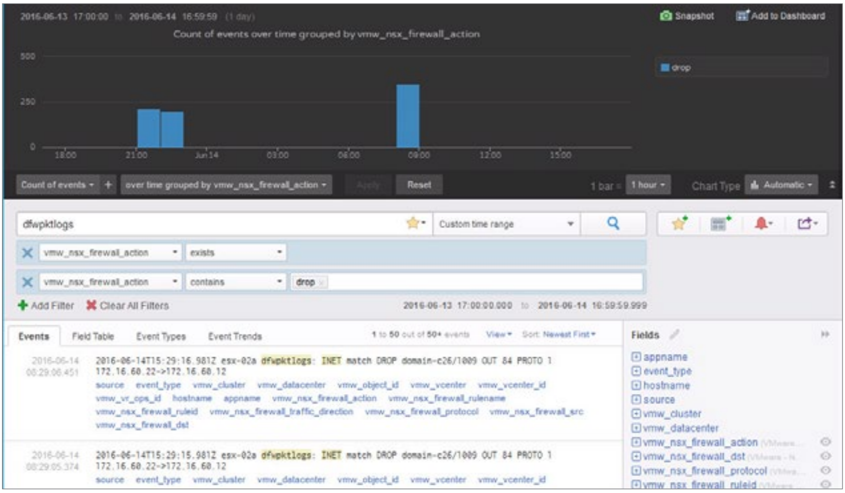


hostname	contains	Use TAB or ENTER to separate multiple terms
vmw_nsx_firewall_action	contains	Use TAB or ENTER to separate multiple terms
vmw_nsx_firewall_ruleid	=	Use TAB or ENTER to separate multiple terms

timestamp	source	vmw_nsx_resource	vmw_nsx_operation	vmw_nsx_audit_username	vmw_nsx_audit_module
7/28/2020, 11:38:...	10.196.184.41	Global	Save configuration		ZONES_FIREWALL
7/28/2020, 11:38:...	10.196.184.41	Global	MODIFY		ZONES_FIREWALL
7/28/2020, 11:08:...	10.196.184.41	Global	Save configuration		ZONES_FIREWALL
7/28/2020, 11:08:...	10.196.184.41	Global	MODIFY		ZONES_FIREWALL
7/28/2020, 11:38:...	10.196.184.41	Global	Save configuration		ZONES_FIREWALL
7/28/2020, 11:38:...	10.196.184.41	Global	MODIFY		ZONES_FIREWALL

Figure 4.6 Distributed Firewall Event Summary in vRealize Log Insight

vRealize Log Insight also supports interactive analysis using logs in real time. In an example audit for access attempts shown in Figure 4.7, **172.16.60.22** (Web-03a) issued a ping to **172.16.60.12** (Web-04a) that was dropped due to firewall rule # **1009**



dfwpktlogs

Custom time range

vmw_nsx_firewall_action exists

vmw_nsx_firewall_action contains drop

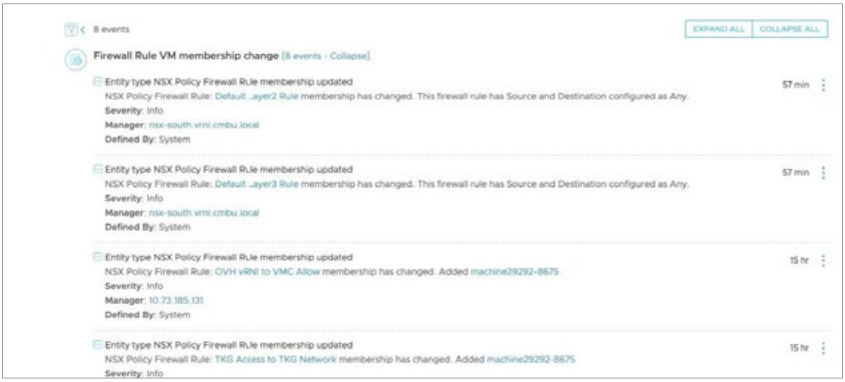
2016-06-13 17:00:00.000 to 2016-06-14 16:59:59.999

```
2016-06-14     2016-06-14T15:29:16.981Z esx-02a dfwpktlogs: INET match DROP domain-c26/1009 OUT 84 PROTO 1
08:29:06.451   172.16.60.22->172.16.60.12
               source  event_type  vmw_cluster  vmw_datacenter  vmw_object_id  vmw_vcenter  vmw_vcenter_id
               vmw_vr_ops_id  hostname  appname  vmw_nsx_firewall_action  vmw_nsx_firewall_rulename
               vmw_nsx_firewall_ruleid  vmw_nsx_firewall_traffic_direction  vmw_nsx_firewall_protocol  vmw_nsx_firewall_src
               vmw_nsx_firewall_dst

2016-06-14     2016-06-14T15:29:15.981Z esx-02a dfwpktlogs: INET match DROP domain-c26/1009 OUT 84 PROTO 1
08:29:05.374   172.16.60.22->172.16.60.12
               source  event_type  vmw_cluster  vmw_datacenter  vmw_object_id  vmw_vcenter  vmw_vcenter_id
```

Figure 4.7 Auditing for access attempts using vRealize Log Insight

vRealize Network Insight can simplify NSX configuration as well as micro-segmentation compliance auditing. NSX configuration compliance can be accomplished using vRealize Network Insight's best practice checklist monitoring capability to validate NSX compliance against hardening guidelines. Figure 4.8 highlights the use of vRealize Network Insight for NSX micro-segmentation compliance to audit changes made to firewall rule membership over a specified period. To view this data, search for "firewall rule membership" and specify the date range for the changes.



8 events

Firewall Rule VM membership change [8 events - Collapse]

Entity type NSX Policy Firewall RuIe membership updated — 57 min
NSX Policy Firewall Rule: Default Layer2 Rule membership has changed. This firewall rule has Source and Destination configured as Any.
Severity: Info
Manager: nsx-south.vrni.cmbu.local
Defined By: System

Entity type NSX Policy Firewall RuIe membership updated — 57 min
NSX Policy Firewall Rule: Default Layer3 Rule membership has changed. This firewall rule has Source and Destination configured as Any.
Severity: Info
Manager: nsx-south.vrni.cmbu.local
Defined By: System

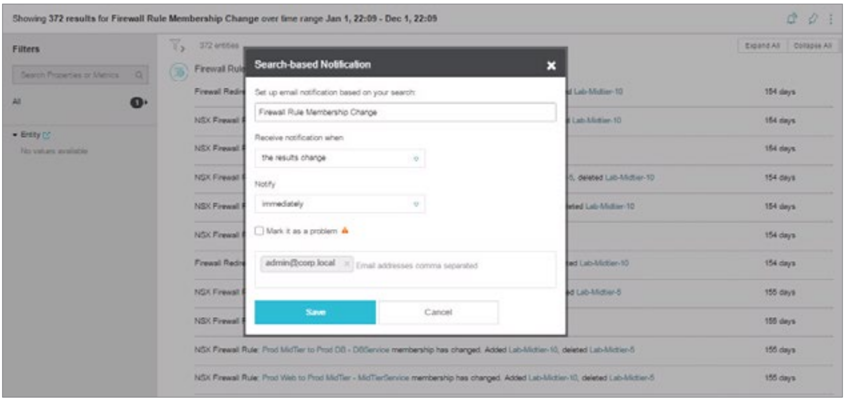
Entity type NSX Policy Firewall RuIe membership updated — 15 hr
NSX Policy Firewall Rule: OVH vRNI to VMC Allow membership has changed. Added machine29292-8675
Severity: Info
Manager: 10.73.185.131
Defined By: System

Entity type NSX Policy Firewall RuIe membership updated — 15 hr
NSX Policy Firewall Rule: TKG Access to TKG Network membership has changed. Added machine29292-8675
Severity: Info

Figure 4.8 Firewall rule membership changes over time in vRealize Network Insight

The information identifies any firewall rule changes made directly or indirectly because of VM membership changes. This is critical to the audit change tracking process as it identifies why, when, and how firewall rules changed. The changes can now be tracked, audited, and exported by following the live links.

This can be taken a step further by creating alerts to notify on changes, as shown in Figure 4.9, further augmenting the intelligent operations of the NSX environment.



Showing 372 results for Firewall Rule Membership Change over time range Jan 1, 22:09 - Dec 1, 22:09

Search-based Notification

Set up email notification based on your search:

Firewall Rule Membership Change

Receive notification when: the results change

Notify: immediately

☐ Mark it as a problem

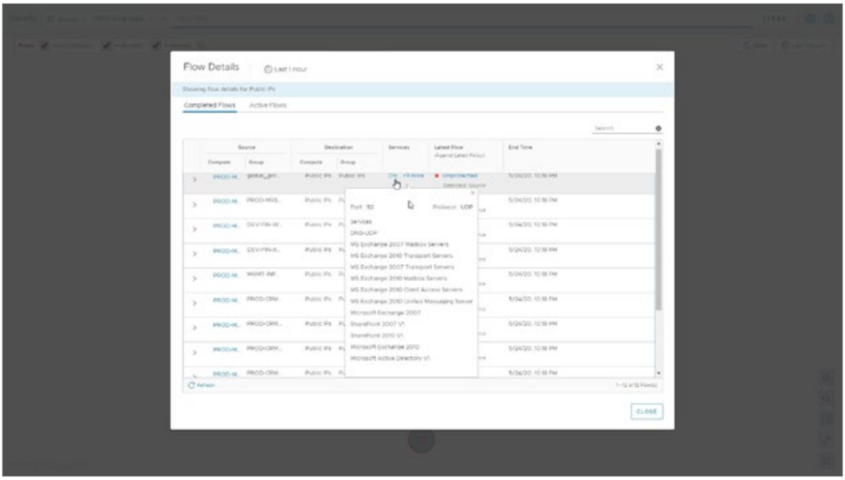
admin@corp.local ×

NSX Firewall Rule: Prod MidTier to Prod DB - DBService membership has changed. Added Lab-Midtier-10, deleted Lab-Midtier-5 — 155 days

NSX Firewall Rule: Prod Web to Prod MidTier - MidTierService membership has changed. Added Lab-Midtier-10, deleted Lab-Midtier-5 — 155 days

Figure 4.9 Creating change alerts for auditing in vRealize Network Insight

NSX Intelligence, introduced in NSX-T 2.5, can be used for demonstrating and maintaining security policies. This tool presents a complete historical record of each flow in and out of every workload along with detailed flow visualizations. This allows operators to compare security policy against actual flows, helping to identify exceptions and non-compliant flows at every point in time. An example of viewing the historical record of every flow is shown in Figure 4.10.



Flow Details ⏱ Last 1 hour

Showing flow details for Public IPs

Completed Flows | Active Flows

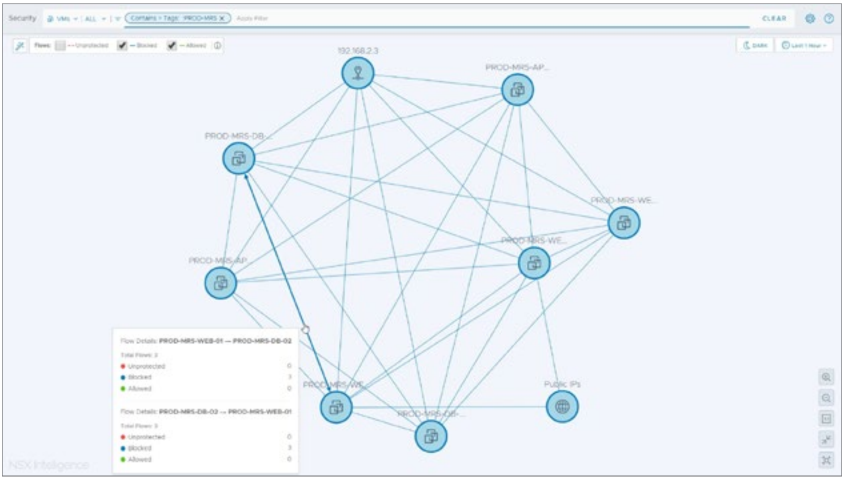
	Source		Destination		Services	Latest Flow (Against Latest Policy)	End Time
	Compute	Group	Compute	Group			
>	PROD-M...	global_gro...	Public IPs	Public IPs	DN... +8 More	● Unprotected Detected: Source	5/26/20, 10:18 PM
>	PROD-M...	PROD-MRS...	Public IPs	P...			5/24/20, 10:18 PM
>	PROD-M...	DEV-FIN-W...	Public IPs	P...			5/24/20, 10:18 PM
>	PROD-M...	DEV-FIN-A...	Public IPs	P...			5/26/20, 10:18 PM
>	PROD-M...	MGMT-INF...	Public IPs	P...			5/24/20, 10:18 PM
>	PROD-M...	PROD-CRM...	Public IPs	P...			5/24/20, 10:18 PM
>	PROD-M...	PROD-CRM...	Public IPs	P...			5/26/20, 10:18 PM
>	PROD-M...	PROD-CRM...	Public IPs	P...			5/26/20, 10:18 PM
>	PROD-M...	PROD-CRM...	Public IPs	P...			5/26/20, 10:18 PM

Port: 53 Protocol: UDP

Services
DNS-UDP
MS Exchange 2007 Mailbox Servers
MS Exchange 2010 Transport Servers
MS Exchange 2007 Transport Servers
MS Exchange 2010 Mailbox Servers
MS Exchange 2010 Client Access Servers
MS Exchange 2010 Unified Messaging Server
Microsoft Exchange 2007
SharePoint 2007 V1
SharePoint 2010 V1
Microsoft Exchange 2010
Microsoft Active Directory V1

Figure 4.10 Example of viewing historical flows

Examples of visualizations showing security policy impact are shown in Figure 4.11 and Figure 4.12.



Flow Details: PROD-MRS-WEB-01 → PROD-MRS-DB-02

Total Flows: 3

● Unprotected 0
● Blocked 3
● Allowed 0

Flow Details: PROD-MRS-DB-02 → PROD-MRS-WEB-01

Total Flows: 3

● Unprotected 0
● Blocked 3
● Allowed 0

Figure 4.11 Example of blocked flow visualization

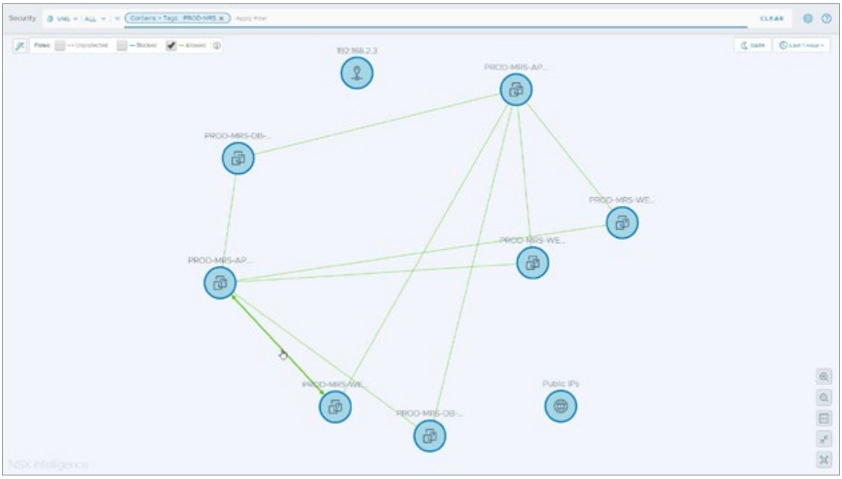


Figure 4.12 Example of allowed flow visualization

KPIs

Objective	KPI	Description
Zero instances of improper communication with or between applications in the NSX-based environment	• Average amount of time to detect and remediate improper communication with or between applications	This KPI provides a measure of the efficiency of identifying, validating, and remediating changes to application access or communication

Table 4.7 Sample compliance management impact KPI

Access management

Company insiders continue to be key threats to corporate security. Strong access management is critical to help mitigate the risk of suffering from an insider-enabled security breach. As of version 3.0, NSX-T Data Center addresses access management through its expanded authentication and authorization capabilities below and shown in Figure 4.13.

- Native Microsoft Active Directory (AD) authentication via the Lightweight Directory Access Protocol (LDAP)
- Integration with OpenLDAP
- VMware Workspace ONE® Access™ (formerly VMware Identity Manager™)
- Enhanced Role Based Access Control (RBAC)

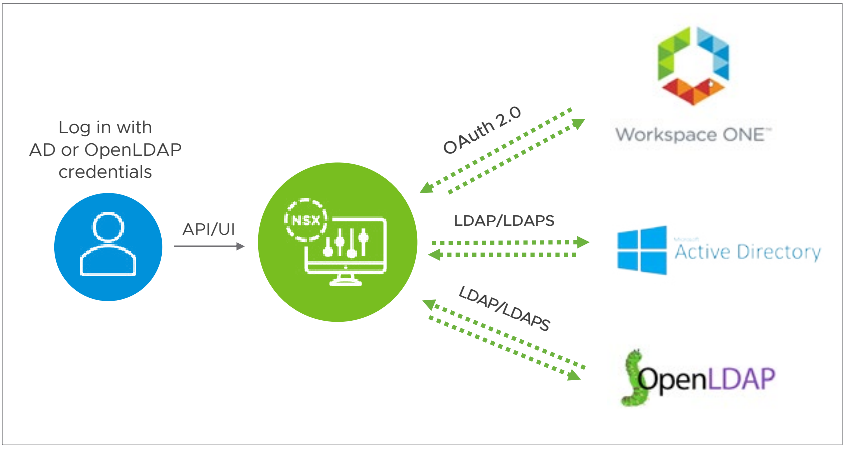


Figure 4.13 NSX-T Data Center authentication and authorization

NSX-T Data Center can leverage user credentials stored directly in AD using LDAP as an identity source. It can use LDAP as an identity source in its regular, unsecured configuration as well as a secure (LDAPS or startTLS) configuration. In addition, AD users or groups can be mapped directly to NSX-T Data Center RBAC-defined roles. Given that many enterprises are already using AD to store user and group credentials, using AD directly for authentication can simplify user onboarding without having to configure additional identity authentication systems.

In addition to supporting native AD integration, NSX-T Data Center can directly authenticate and onboard users who are using OpenLDAP. It support using OpenLDAP in either its unsecured configuration or in its secure configuration using LDAPS. As with AD using LDAP, users authenticating through OpenLDAP can be mapped to NSX-T Data Center RBAC-defined roles.

NSX-T Data Center can also authenticate using Workspace ONE Access. In this way, NSX-T Data Center can participate in a centralized, enterprise identity management and single sign-on authentication solution across its VMware-enabled environment. As with AD using LDAP or OpenLDAP, users authenticating through Workspace One Access can be mapped to NSX-T Data Center RBAC-defined roles.

The RBAC defined for NSX-T Data Center supports a fine-grained level of control of who has permission to execute actions. A summary level view of roles and permissions as of NSX-T Data Center version 3.0 is show in Table 4.8.[3]

[3] See https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/administration/GUID-26C44DE8-1854-4B06-B6DA-A2FD426CDF44.html for a more detailed explanation

RBAC Role	Permission
Enterprise Administrator	Super user; full access on all
Network Engineer	Full access on networking services, e.g. switching & routing
Network Operator	Read access on networking services, with the permission to run monitoring & trouble shooting tools
Security Engineer	Full access on security services, e.g. firewall and encryption
Security Operator	Read access on security services, with the permission to run monitoring & trouble shooting tools
Load Balancer Administrator	Full access to Load Balancer configuration
Load Balancer Auditor	Read access to Load Balancing Configuration
Auditor	Read access on all
Network Introspection Administrator	Network Introspection workflow and policy.
Guest Introspection Administrator	Guest Introspection workflow and policy.
VPN Admin	VPN workflow administration

Table 4.8 Summary level view of NSX-T Data Center RBAC

KPIs

Objective	KPI	Description
Zero instances of improper segregation of duties	• Number of NSX roles without an owner • Number of NSX roles assigned to the same individual	This KPI provides a measure of segregation of duties completeness by focusing on identifying, validating, and remediating NSX role ownership

Table 4.9 Sample access management impact KPI

Consuming NSX

The end goal for operationalizing NSX is to support its use. This section provides high-level considerations and guidance for consuming NSX capabilities. This is approached from two perspectives:

- Consumption of NSX capabilities by application and service developers
- Consumption of NSX capabilities by IT for IT

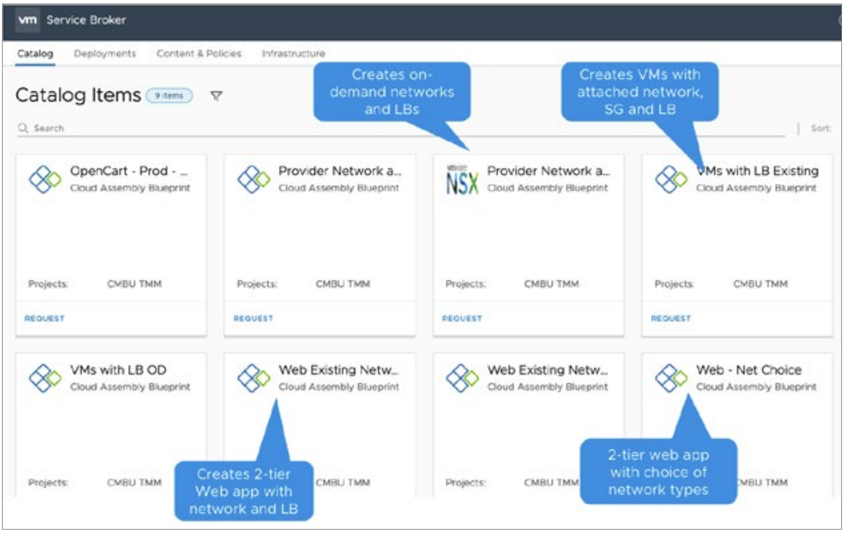
Developer consumption models

How do developers consume NSX capabilities when developing a new application? The recommended model is initial provisioning of virtual infrastructure from blueprints then packaging the virtual infrastructure blueprint—representing infrastructure-as-code—with its application blueprint for fully automated application plus virtual infrastructure deployment.

Provisioning from blueprints represents the lowest risk approach. One of the most powerful aspects of using capabilities of blueprints (or Puppet manifests, Chef recipes, Ansible playbooks, or, as of NSX-T Data Center version 3.0, Terraform) is the ability to provision the configuration defined in the blueprint repeatedly, guaranteeing the same result each time while reducing delays due to human error. This is ideal for application or service development; it builds on the base blueprint and ensures the exact same configuration is provisioned when moving through the stages of the development lifecycle. In this way, the same configuration is provisioned in integration testing, user acceptance testing, staging, and production. Any changes should be made to the blueprint rather than directly in the environment with new environments deployed from these modified blueprints.

Application development teams interact with blueprints in one of two ways: selecting an entry in a service catalog or integrating directly with the virtual infrastructure blueprint. Typically, the cloud infrastructure services team or platform services team develop the virtual infrastructure blueprints. From a software-defined networking and security perspective, these blueprints can include NSX objects such as segments, gateways, load balancers, distributed security policies, and security tags.

When consuming the virtual infrastructure blueprint, the member of the application development team responsible for deploying the virtual infrastructure—typically a person in a DevOps or Site Reliability Engineering role—is presented with a complete specification of the virtual infrastructure component. These infrastructure components could be VMs, containers, network objects, or some combination thereof as shown in Figure 5.1. This same approach can also enable on-demand delivery of complete application environments across clouds, with the configuration and management of networking and security included.



Creates on-demand networks and LBs

Creates VMs with attached network, SG and LB

Creates 2-tier Web app with network and LB

2-tier web app with choice of network types

Figure 5.1 Examples of blueprints in the service catalog

Application development teams are increasingly opting for the second approach; integrating with the virtual infrastructure blueprint directly using tools such as Terraform. Integrating with and using the virtual infrastructure blueprint directly has the added advantage of being able to integrate it directly into the CI/CD pipeline.

NSX-T Data Center version 3.0 includes a Terraform Provider. The NSX-T Terraform Provider presents a way to automate NSX to provide virtualized networking and security services using both ESXi and KVM based hypervisor hosts as well as container networking and security.

An example of deploying and destroying application-specific virtual infrastructure, including NSX network infrastructure, in a CI/CD pipeline using Jenkins is shown in Figure 5.2. This example assumes a simple application that is first deployed in a test environment. In this virtual infrastructure deployment, configurations (including networking and security components) are dynamically created based on the content of the development branch of the application GitHub repository. After the application is validated in the test environment, the development branch is merged into the production branch triggering the deployment in the production environment.

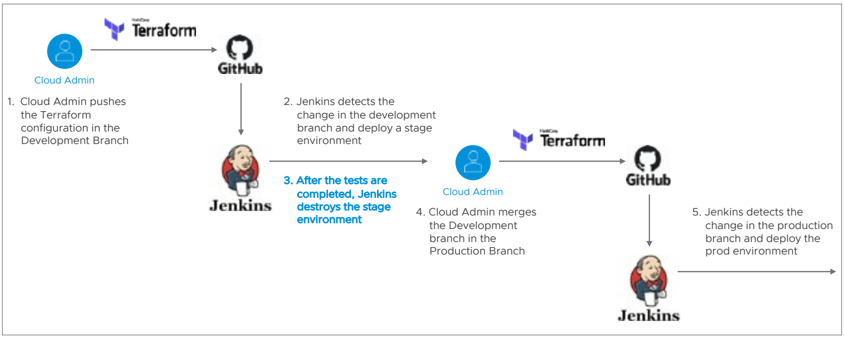

Terraform
Cloud Admin
GitHub
1. Cloud Admin pushes the Terraform configuration in the Development Branch
2. Jenkins detects the change in the development branch and deploy a stage environment
Jenkins
3. After the tests are completed, Jenkins destroys the stage environment
Terraform
Cloud Admin
GitHub
4. Cloud Admin merges the Development branch in the Production Branch
5. Jenkins detects the change in the production branch and deploy the prod environment
Jenkins

Figure 5.2 Integrating Terraform virtual infrastructure configuration to a multibranch CI/CD pipeline

IT for IT consumption models

As both a provider and consumer of corporate services, IT teams can access the NSX environment directly through the NSX Manager user interface or via API. Services can be made accessible through a self-service portal, vRealize automation, OpenStack, custom integration, third-party applications, or directly through the user interface.

The NSX-T user interface is HTML5-based. It contains several monitoring and troubleshooting dashboards, configuration wizards, and search filters. Consumption of NSX can be driven directly through the NSX Manager user interface, which can be accessed through the vSphere Web Client, if available.

NSX Manager provides a programmatic API to automate management activities. The API follows a resource-oriented REST architecture, using JSON object encoding. Clients interact with the API using RESTful web service calls over the HTTPS protocol. NSX has a rich API service that is used to configure NSX objects as well as install, configure, and build management of the NSX environment. NSX also provides a high degree of day-0 to day-2 operations automation.

> **Note:** As of NSX-T Data Center version 2.4, VMware introduced the Policy API, a new and modern, intent-based (declarative) API. Unlike the previous, imperative API (NSX-T Management Plane API), the new API provides a much easier and efficient way to push configurations to NSX. It simplifies network automation by allowing IT to specify what the connectivity and security needs of applications are as opposed to how networking and security should be configured step-by-step.
>
> Unlike the imperative-based model where detailed tasks need to be explicitly called out, this new way of provisioning infrastructure gives operators a one-shot, application-focused approach to automating configuration of the network.
>
> The declarative interface takes in simple, user-defined terms the connectivity and security requirements for the application environment specified in a JSON file. These policies are platform-agnostic and easily replicable, simplifying operations and improving efficiency.

IT can automate NSX-T deployment and configuration using DevOps tools such as Ansible and Terraform, a scripting tool such as VMware PowerCLI, or one of several programing languages, such as Python, Java, and Go. The ways in which NSX can be consumed using the REST API are shown in Figure 5.3.

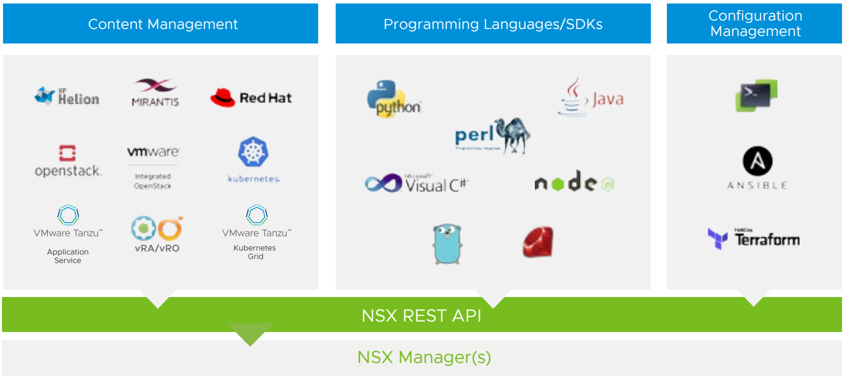


Figure 5.3 NSX Consumption using REST API

Some of the most popular automation mechanisms and tools for NSX are described below.

vRealize Automation

vRealize Automation can be used to build and manage a multi-vendor cloud infrastructure. In addition to end users, such as developers, using vRealize Automation to self-provision virtual machines and applications in private and public cloud environments, IT can use vRealize Automation to deploy physical machines (install OEM images) and IT services according to defined policies. The SaaS version, vRealize Automation Cloud, supports public clouds such as AWS, Azure, and Google Cloud Platform. Consumption is accomplished by selecting an item from a service catalog, for example Service Broker, as described in the *Developer Consumption Models* section.

The integration of vRealize Automation with NSX automates an application's network connectivity, security, performance, and availability. It can automate the deployment and configuration of NSX objects such as segments, gateways, distributed security policy, and security tags. This is shown in Figure 5.4.

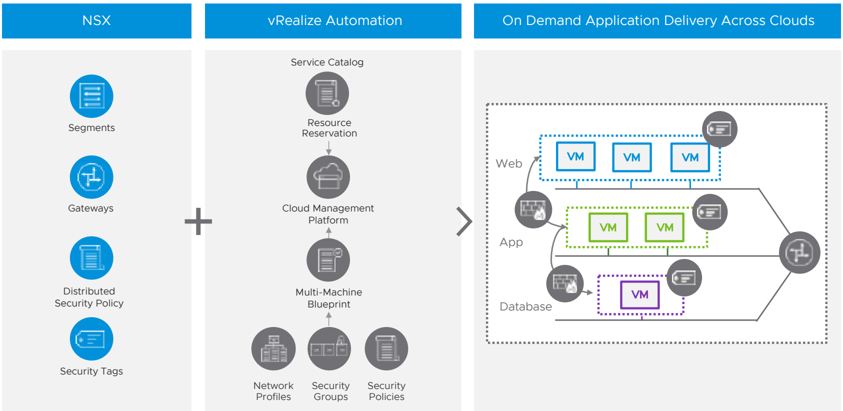
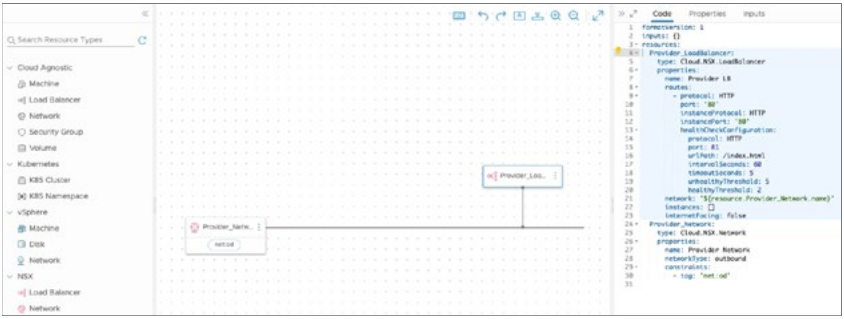


Figure 5.4 NSX integration with vRealize Automation

This NSX functionality can be consumed through a graphical layout canvas in Cloud Assembly blueprint designer, allowing the topology to be visualized as it is being created. Figure 5.5 shows a graphical example of a provider network object and a provider load balancer connection, with the corresponding YAML code on the right. These are added and configured by dragging and dropping the different objects from the menu on the left.



```
formatVersion: 1
inputs: {}
resources:
  Provider_LoadBalancer:
    type: Cloud.NSX.LoadBalancer
    properties:
      name: Provider LB
      routes:
        - protocol: HTTP
          port: '80'
          instanceProtocol: HTTP
          instancePort: '80'
          healthCheckConfiguration:
            protocol: HTTP
            port: 81
            urlPath: /index.html
            intervalSeconds: 60
            timeoutSeconds: 5
            unhealthyThreshold: 5
            healthyThreshold: 2
      network: '${resource.Provider_Network.name}'
      instances: []
      internetFacing: false
  Provider_Network:
    type: Cloud.NSX.Network
    properties:
      name: Provider Network
      networkType: outbound
      constraints:
        - tag: 'net:od'
```

Figure 5.5 Using Cloud Assembly blueprint designer to create NSX Infrastructure as Code

Automation and standardization using blueprints not only accelerate IT services delivery, but also provide repeatable processes that eliminate delays caused by manual errors.

Ansible

Red Hat Ansible delivers simple IT automation that ends repetitive tasks and frees up IT for more strategic work. Ansible modules interact with NSX-T Data Center using standard REST APIs and the only requirement is IP connectivity to NSX-T Data Center. Typically, Ansible is used for the initial environment creation/fabric preparation, then intent-based tools such as the Policy API or Terraform are leveraged to create network topologies and security policies. Ansible can trigger the Policy API or Terraform in order to have a single playbook perform the configuration end-to-end as shown in Figure 5.6.

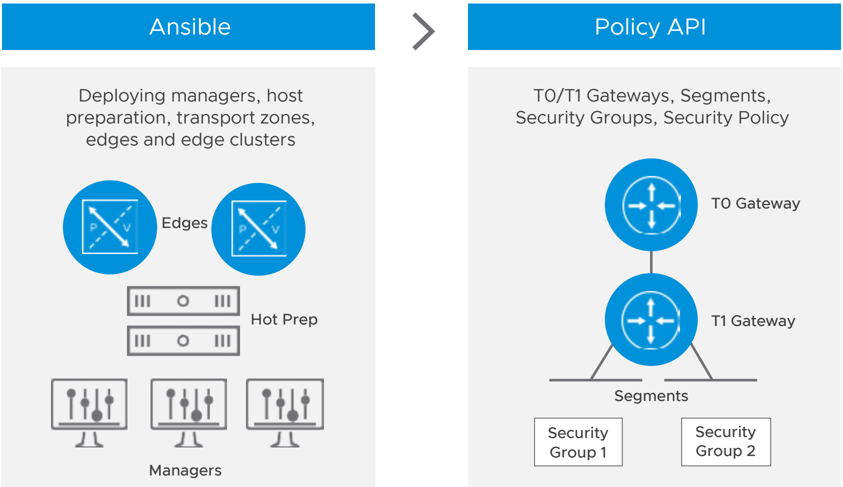

Ansible
Policy API
Deploying managers, host preparation, transport zones, edges and edge clusters
Edges
Hot Prep
Managers
T0/T1 Gateways, Segments, Security Groups, Security Policy
T0 Gateway
T1 Gateway
Segments
Security Group 1
Security Group 2

Figure 5.6 Example of Ansible directly triggering the Policy API

Terraform

Terraform is a widely deployed, open-source infrastructure as a code software by HashiCorp. It allows creation, modification, and deletion of an infrastructure using a high-level configuration files that can be shared between IT team members, treated as a code, edited, reviewed, and versioned. These configuration files are written in HCL (HashiCorp Configuration Language) which is JSON with some fine-tuning. Plain JSON can be also used.

As previously described in the *Developer Consumption Models* section, the NSX-T Terraform Provider presents a way to automate NSX to provide virtualized networking and security services using both ESXi and KVM based hypervisor hosts as well as container networking and security. IT can also use Terraform directly with a CI/CD pipeline, as previously described, to test, stage, and deploy NSX network infrastructure and security configurations. This also implies that the NSX network infrastructure and security configurations represented in infrastructure as code can be kept under integrated version control, which is highly encouraged as a best practice.

Scripting and Programming Languages

Finally, IT can consume NSX through scripting using VMware PowerCLI as well as other programming languages.

PowerCLI is a command-line and scripting tool built on Windows PowerShell. It provides more than 700 cmdlets for managing and automating VMware vSphere,® VMware vCloud,® vRealize Operations Manager, VMware vSAN,™ NSX-T Data Center, VMware Cloud on AWS, VMware HCX,® VMware Site Recovery Manager,™ and VMware Horizon® environments.

The NSX-T module is a low-level module (API access only) which contains a few cmdlets:

- **Connect-NsxtServer:** establishes a connection to an NSX-T server.
- **Disconnect-NsxtServer:** closes the connection to the NSX-T server
- **Get-NsxtPolicyService:** invokes the operations on the NSX-T Policy API service (create, read, update, delete)
- **Get-NsxtService:** invokes the operations on the NSX-T API service (create, read, update, delete)

These four cmdlets are powerful enough to create, remove or modify any object in the *NSX-T Manager*.

Regarding interacting with NSX using programming languages, VMware supports Python and Java Software Development Kits (SDKs) for NSX that can be downloaded from downloads.vmware.com or https://code.vmware.com/sdks. IT can use these SDKs to develop third-party software and automate NSX virtual network infrastructure. NSX's use of Open APIs enables use of standard tools like Swagger to generate language bindings for languages such as C, Go, Ruby, PHP, etc.

Tools for Monitoring, Operations, and Troubleshooting

Monitoring and troubleshooting are the most visible and frequently asked about aspects of operationalizing NSX, and effective monitoring and troubleshooting begins with the tools. The NSX environment offers a wide variety of tools that enable proactive monitoring and provide effective troubleshooting. Figure 6.1 offers a framework for organizing the NSX tool ecosystem.

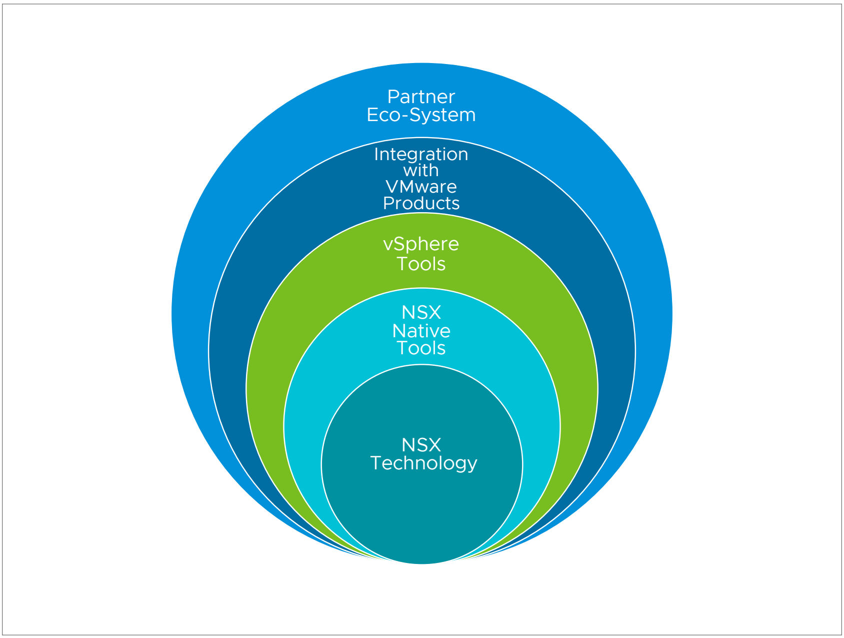


Figure 6.1 NSX tool ecosystem

These categories include:

- NSX-native tools: troubleshooting capabilities delivered within NSX
- vSphere tools: additional vSphere-based tools for NSX troubleshooting
- Tools provided by VMware products: NSX monitoring and troubleshooting capabilities provided by the vRealize Operations, vRealize Log Insight, and vRealize Network Insight
- Partner ecosystem: additional NSX troubleshooting tools provided by 3rd party VMware partners

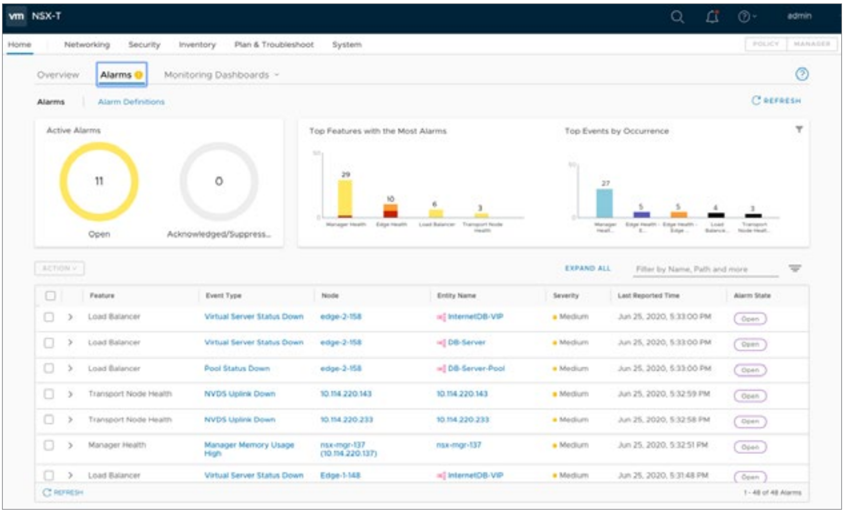
NSX Native Tools

NSX comes with tools that provide extensive native monitoring and troubleshooting capabilities. The primary built-in tools for monitoring and troubleshooting are accessed via the NSX Manager user interface and the command line interface (CLI) component. When coupled with component log files, these tools provide a standalone, comprehensive solution to monitor and troubleshoot an NSX-based infrastructure.

Dashboards: NSX-T includes an out-of-the-box dashboard that allows administrators to check the status of the primary NSX components in a single pane of glass. The dashboards as of NSX-T 3.0 include:

1. System—deployment and connectivity status of hosts and Edges, status information of transport nodes and transport zones
2. Clusters—health status of the NSX management cluster
3. Networking—information about tier-0 & tier-1 gateways, segments, VPNs, and load balancers
4. Security—information about distributed firewall, network introspection, and endpoint protection
5. Custom—define custom dashboards which enable ease of monitoring of specific use-cases

Alarm Dashboard: With NSX-T 3.0 and newer, NSX can alert users of noteworthy conditions by using the Alarms/Events framework.



Feature	Event Type	Node	Entity Name	Severity	Last Reported Time	Alarm State
Load Balancer	Virtual Server Status Down	edge-2-158	InternetDB-VIP	Medium	Jun 25, 2020, 5:33:00 PM	Open
Load Balancer	Virtual Server Status Down	edge-2-158	DB-Server	Medium	Jun 25, 2020, 5:33:00 PM	Open
Load Balancer	Pool Status Down	edge-2-158	DB-Server-Pool	Medium	Jun 25, 2020, 5:33:00 PM	Open
Transport Node Health	NVDS Uplink Down	10.114.220.143	10.114.220.143	Medium	Jun 25, 2020, 5:32:59 PM	Open
Transport Node Health	NVDS Uplink Down	10.114.220.233	10.114.220.233	Medium	Jun 25, 2020, 5:32:58 PM	Open
Manager Health	Manager Memory Usage High	nsx-mgr-137 (10.114.220.137)	nsx-mgr-137	Medium	Jun 25, 2020, 5:32:51 PM	Open
Load Balancer	Virtual Server Status Down	Edge-1-148	InternetDB-VIP	Medium	Jun 25, 2020, 5:31:48 PM	Open

Figure 6.2 NSX-T 3.0 Alarm Dashboard

Counters, Statistics, Tables: NSX provides visibility on different aspects of the traffic that goes through the NSX fabric. The following are exposed through the NSX Manager:

- Node statistics—including CPU, memory, disk, or interface-related information—are exposed by the NSX Manager nodes and transport nodes (i.e., ESXi, KVM and NSX Edge nodes).
- In addition, each function running on the transport nodes (e.g., logical switching, logical routing, NAT, and DFW) exposes operational data relevant to that function.
- On-demand statistics such as interface statistics, MAC address tables, or TEP tables are queried in real time while bulk statistics (typically aggregation of distributed stats) are collected by periodic polling.

Besides counters, statistics, and tables for the traffic through the NSX fabric, it is also possible to monitor the status other important aspects of a typical NSX deployment: logical switch port, BGP neighbor status, and Geneve tunnel status.

NSX also provides a VM inventory which it reads directly from all supported hypervisors—vSphere, RHEL KVM, and Ubuntu KVM—as well as a criteria-based search utility for inventory objects.

NSX API: NSX Manager provides a programmatic API to automate management activities. The API follows a resource-oriented REST architecture, using JSON object encoding. Clients interact with the API using RESTful web service calls over the HTTPS protocol. The NSX API documentation is available in the Resources section and is also embedded in the NSX Manager for easy access.

Additionally, there are Python and Java Software Development Kits (SDKs) available for NSX. These can be downloaded from the Drivers & Tools section under the NSX Downloads page.

NSX CLI: An NSX-specific CLI is available on NSX appliances (NSX Managers, NSX Controllers, NSX Edge Nodes) and on hypervisors that are transport nodes.

NSX Central CLI: NSX includes a feature called Central CLI, which allows an administrator to run a command on any NSX appliance or transport node directly from the NSX Manager CLI. This is useful to prevent changing interfaces and for instances where NSX administrators/operators may not have access to the hypervisor's CLI. Furthermore, Central CLI permits the administrator to run the same command on multiple nodes simultaneously, including nodes of multiple types (e.g., an NSX Controller, an ESXi hypervisor, and a KVM hypervisor).

Local and Remote Logging:

NSX components such as NSX Manager, NSX Controller, ESXi host, and KVM host retain their logs locally. These components can also send syslog messages to a remote logging server. Logs can be sent to different types of syslog collectors such as SIEM tools, vRealize Log Insight, Splunk, and other open source or 3rd party products. Remote logging is supported on NSX Manager/Controller cluster, NSX Edge, and the supported hypervisors.

Logging can also be configured for the NSX-T Container plug-in (NCP) for Kubernetes as well as the NSX Container Network Interface (CNI) plug-in. In addition, the NSX distributed firewall and Edge firewall provide logging capabilities for firewall rulesets. Enabling logging for the NSX DFW and Edge firewall can be done per section and per firewall rule. Firewall sections are used to group a set of firewall rules as well as for multi-tenancy (e.g., specific rules for sales and engineering departments).

Traceflow

Traceflow can inspect the path of a packet as it travels from one logical port on the logical network to another logical port on the same network. NSX Traceflow traces the transport node-level path of a packet injected at a logical port. It observes a marked packet as it traverses the overlay network, monitoring as it crosses the overlay network until it reaches a destination guest VM or an Edge uplink.

This flow allows identification of issues such as bottlenecks or disruptions. Each network component reports the packet handling on input and output, helping determine whether issues occur when receiving a packet or when forwarding the packet. The injected marked packet is never actually delivered to the destination guest VM, which enables Traceflow to be successful even when the guest VM is powered down.

Traceflow can be used on transport nodes and supports both IPv4 and IPv6 protocols including: ICMP, TCP, UDP, DHCP, and DNS. Traceflow supports both unicast and broadcast traffic at layers 2 & 3.

IPFIX:

IPFIX is a standard protocol for transmitting traffic flow information over the network. Traffic flows can be forwarded to external IPFIX collectors for centralized flow collection, longer data retention, data analysis, and troubleshooting. When configured to export switching and firewall flows:

- For firewalls, the network flow managed by the distributed firewall component is exported.
- For switches, the network flow at virtual interfaces and physical NICs is exported.

Port Mirroring:

Port mirroring is used on a switch to send a copy of packets seen on one switch port (or an entire VLAN) to a monitoring connection on another switch port. Port mirroring is used to analyze and debug data or diagnose errors on a network. In NSX-T, port mirroring supports the following session types: local SPAN, logical SPAN, remote SPAN, and remote L3 SPAN.

NSX Intelligence

VMware NSX® Intelligence™ is a distributed analytics engine built into NSX-T Data Center. It leverages a granular workload and network context unique to NSX to deliver converged security policy management, analytics, and compliance with data center–wide visibility.

NSX Intelligence provides a user interface via a single management pane within NSX Manager and provides the following features for real-time flow visualizations and firewall rule planning:

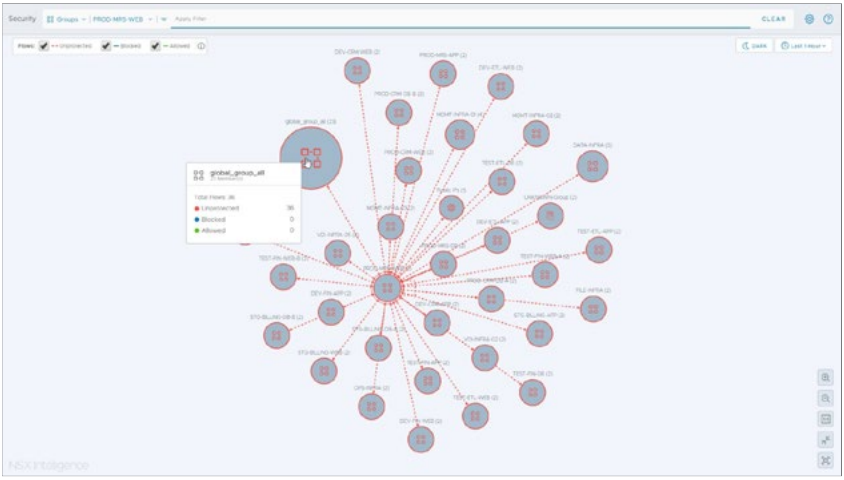
- **Data flow view:** NSX Intelligence provides almost real-time flow information on data between workloads in the environment. Information—including VMs, external IPs and public IPs—is displayed both within and outside the NSX domain. NSX Intelligence correlates live or historic flows, user configurations, and workload inventory.

- **Filtering Views:** Administrators can filter the communication map to the VM level, view correlated VM and network context, and show flow details and related groups.

- **Automated Micro-segmentation Planning:** NSX Intelligence generates distributed firewall policy sections, groups, and services, which admins can either accept or modify for micro-segmentation planning. The software also generates new inventory groups or services. The recommendations assist with the implementation of micro-segmentation at the application level. They enable enforcement of a more dynamic security policy by correlating traffic patterns of communication that is occurring between the VMs in the NSX-T Data Center environment.

- **Continuous Recommendations:** NSX Intelligence provides a choice of on-demand or continuous monitoring for recommendation sessions. When continuous monitoring is enabled on a group, NSX Intelligence will generate new recommendations upon detecting VM membership changes in the group.

Figure 6.3 shows the inter-group communication for the VM group tagged with ‘PROD-MRS-WEB.’ The 36 traffic flows are all ‘Unprotected,’ which means there are no firewall rules associated with these flows.



global_group_all

Total Flows: 36

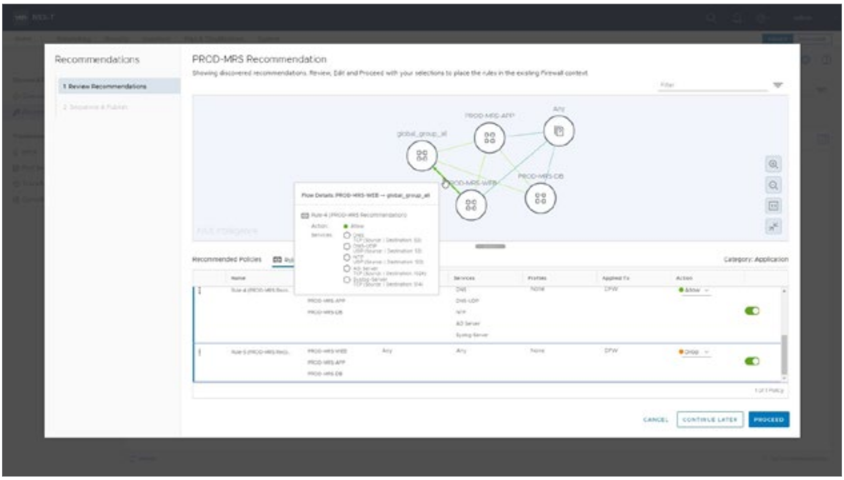
● Unprotected 36

● Blocked 0

● Allowed 0

Figure 6.3 Unprotected traffic flows example

As seen in Figure 6.4, based on the discovery, the recommended DFW rules for the ‘PROD-MRS’ 3-tier app are listed which the administrator can review, edit, and place into the existing firewall context.



PROD-MRS Recommendation

Showing discovered recommendations. Review, Edit and Proceed with your selections to place the rules in the existing Firewall context.

Flow Details: PROD-MRS-WEB → global_group_all

Rule-4 (PROD-MRS Recommendation)

Action: ● Allow

Services: ○ DNS TCP (Source: | Destination: 53) ○ DNS-UDP UDP (Source: | Destination: 53) ○ NTP UDP (Source: | Destination: 123) ○ AD Server TCP (Source: | Destination: 1024) ○ Syslog-Server TCP (Source: | Destination: 514)

Recommended Policies

Category: Application

Name			Services	Profiles	Applied To	Action
Rule-4 (PROD-MRS Reco...	PROD-MRS-APP PROD-MRS-DB		DNS DNS-UDP NTP AD Server Syslog-Server	None	DFW	● Allow
Rule-5 (PROD-MRS Reco...	PROD-MRS-WEB PROD-MRS-APP PROD-MRS-DB	Any	Any	None	DFW	● Drop

1 of 1 Policy

Figure 6.4 Example of firewall rules recommendations based on discovery

vSphere Tools

The next layer up is the NSX monitoring and troubleshooting toolset provided by vSphere. The table below highlights a couple of frequently used operations. For NSX-T, the troubleshooting and monitoring capabilities are available from the NSX Manager UI. In the older variant of the platform (i.e., NSX for vSphere), they are available in the vSphere Web Client **Networking & Security** menu. The NSX Manager to vCenter initial connection process installs a web client plug-in for NSX on the vSphere Web Client server. Some of the tools are best accessed from the vSphere CLI.

Operation	Tool
Detailed health of logical network	vSphere CLI (e.g., esxcli)
Performance issues	vSphere CLI (e.g., esxtop)
Packet capture	vSphere CLI (e.g., pktcap)

Table 6.1 Sample vSphere-based troubleshooting capabilities

VMware vRealize Intelligent Operations Tools

The next level of the NSX monitoring and troubleshooting stack is VMware product tools. There are three VMware products for NSX monitoring and troubleshooting:

- vRealize Network Insight
- vRealize Operations
- vRealize Log Insight

VMware vRealize Network Insight

vRealize Network Insight was purpose-built for holistic network and security monitoring and troubleshooting. Along with NSX Intelligence, it is the primary NSX monitoring and troubleshooting product for intelligent operations on NSX and beyond. The SaaS version is called vRealize Network Insight Cloud and includes the same features and interface as the on-premises version. vRealize Network Insight supports VMs, Kubernetes containers, physical servers, physical networking equipment (e.g., switches, routers, firewalls, load balancers), VMware SD-WAN, as well as public cloud instances in Amazon AWS, Microsoft Azure, and VMware Cloud.

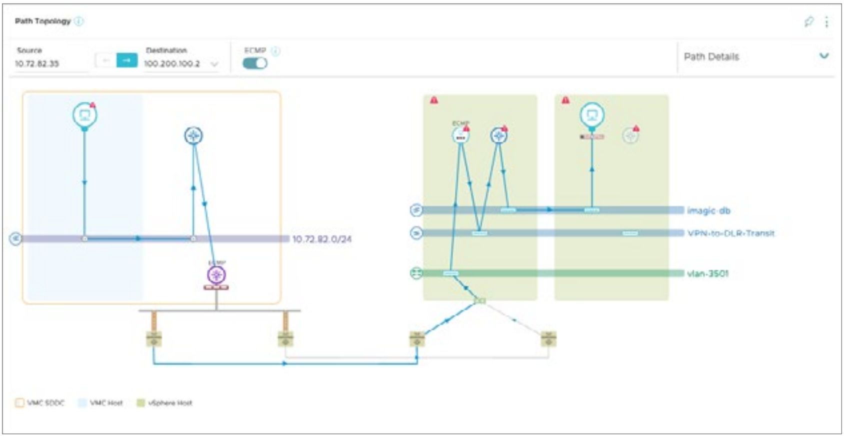
vRealize Network Insight provides seamless visibility and converged network operations across the data center (virtual and physical) and hybrid cloud as well as branch offices and remotes sites via VMware SD-WAN integration.

It is an analytics tool focused on proactively enabling:

- 360˚ visibility and analytics
- Security planning and operations
- Application discovery and operations
- Network health, troubleshooting, and performance monitoring

360 Visibility and Analytics

The 360˚ visibility capabilities function across both the underlay (i.e., physical) and overlay (i.e., virtual) network fabric to glue both the virtual and physical world together, to make troubleshooting and optimizing network performance easy. This is based on selecting a source and destination object between which it provides visibility across both the virtual and physical layers. Figure 6.5 gives an example of an object’s layer 3 and layer 4 path.



Path Topology

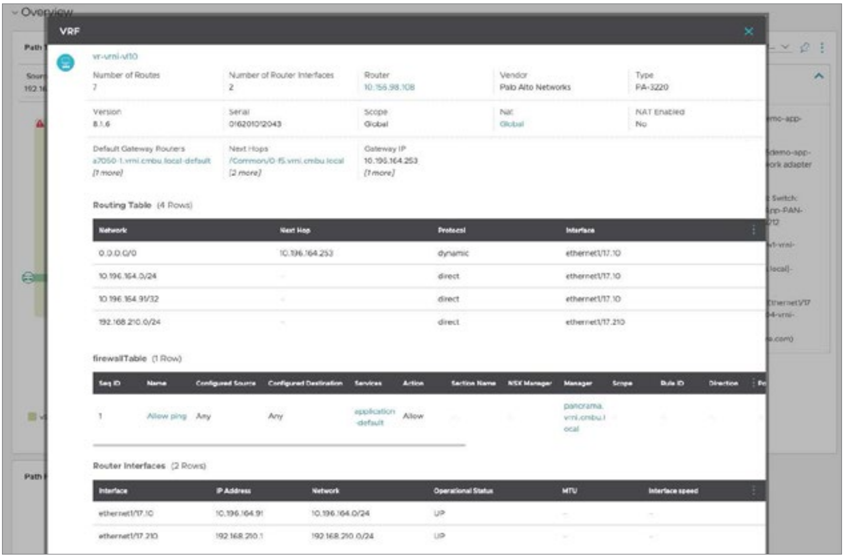
Source: 10.72.82.35

Destination: 100.200.100.2

ECMP

Figure 6.5 360° topology view

This provides a contextual view of the network covering each hop across VLANs and VXLANs or logical segments. Key configuration information for each object is available through hover text., even for objects not managed by NSX. This configuration information is provided for everything in the path, both virtual (e.g., VM and host, VLAN and port group, VNIC), physical objects (e.g., Cisco switches, Palo Alto Networks firewalls), VMware SD-WAN, public cloud Microsoft Azure, Amazon AWS, and VMware Cloud on AWS. Figure 6.6 shows a sample configuration for a Palo Alto Networks VRF.



VRF

vr-vrni-vl10

Number of Routes	Number of Router Interfaces	Router	Vendor	Type
7	2	10.156.98.108	Palo Alto Networks	PA-3220
Version	**Serial**	**Scope**	**Nat**	**NAT Enabled**
8.1.6	016201012043	Global	Global	No
Default Gateway Routers	**Next Hops**	**Gateway IP**		
a7050-1.vrni.cmbu.local-default [1 more]	/Common/0-f5.vrni.cmbu.local [2 more]	10.196.164.253 [1 more]		

Routing Table (4 Rows)

Network	Next Hop	Protocol	Interface
0.0.0.0/0	10.196.164.253	dynamic	ethernet1/17.10
10.196.164.0/24	-	direct	ethernet1/17.10
10.196.164.91/32	-	direct	ethernet1/17.10
192.168.210.0/24	-	direct	ethernet1/17.210

firewallTable (1 Row)

Seq ID	Name	Configured Source	Configured Destination	Services	Action	Section Name	NSX Manager	Manager	Scope	Rule ID	Direction
1	Allow ping	Any	Any	application-default	Allow	-	-	panorama.vrni.cmbu.local	-	-	-

Router Interfaces (2 Rows)

Interface	IP Address	Network	Operational Status	MTU	Interface speed
ethernet1/17.10	10.196.164.91	10.196.164.0/24	UP	-	-
ethernet1/17.210	192.168.210.1	192.168.210.0/24	UP	-	-

Figure 6.6 Example Palo Alto Networks VRF configuration

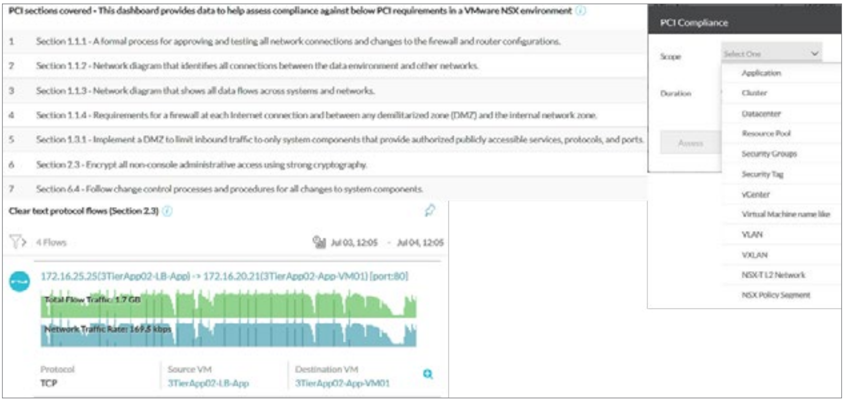
In this example, traffic flows between objects as well as physical and virtual port path performance metrics. There is also a time machine feature to look at the state of the path between the selected objects at a given point in time. Objects allow drill down to view specific information about problems, changes, firewall rules, applicable flow paths, and localized topology.

vRealize Network Insight also provides purpose-built proactive health and availability monitoring, capabilities to understand problems and changes across all objects in the NSX environment, and custom event definition for proactive problem detection. This functionality is available for anything relevant to NSX, including VMs, ESX hosts, virtual networks, and firewalls. vRealize Network Insight can also correlate problems on physical components with their virtual counterparts (e.g., mismatched MTU settings).

Security Planning and Operations

PCI Compliance Dashboard

The PCI compliance dashboard helps in assessing compliance against the PCI requirements in the NSX environment. It takes the PCI sections that are relatable to infrastructure and shows their data in a single dashboard. Along with the snapshots of the micro-segmentation planner donut graph to prove network traffic flows, the PCI compliance dashboard can be exported as a PDF and presented to an auditor for review.



PCI sections covered - This dashboard provides data to help assess compliance against below PCI requirements in a VMware NSX environment

1	Section 1.1.1 - A formal process for approving and testing all network connections and changes to the firewall and router configurations.
2	Section 1.1.2 - Network diagram that identifies all connections between the data environment and other networks.
3	Section 1.1.3 - Network diagram that shows all data flows across systems and networks.
4	Section 1.1.4 - Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
5	Section 1.3.1 - Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
6	Section 2.3 - Encrypt all non-console administrative access using strong cryptography.
7	Section 6.4 - Follow change control processes and procedures for all changes to system components.

Clear text protocol flows (Section 2.3)

4 Flows   Jul 03, 12:05 - Jul 04, 12:05

172.16.25.25(3TierApp02-LB-App) -> 172.16.20.21(3TierApp02-App-VM01) [port:80]

Total Flow Traffic: 1.7 GB

Network Traffic Rate: 169.5 kbps

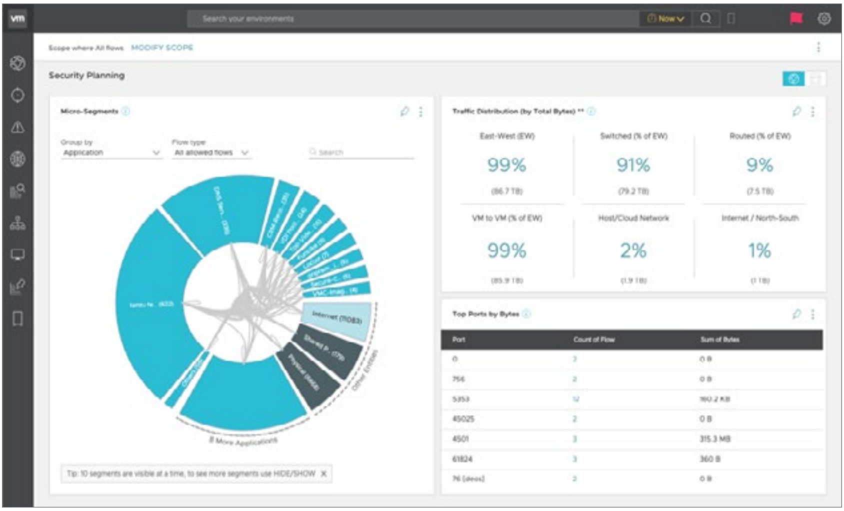
Protocol	Source VM	Destination VM
TCP	3TierApp02-LB-App	3TierApp02-App-VM01

Figure 6.7 PCI compliance dashboard example

Audit Over Time

vRealize Network Insight also has a time machine built in. On any object that it monitors (i.e., a VM, firewall rule, switch port, NSX configuration, etc.), you have the ability to see changes mapped out on a timeline (going back months or years). This timeline can be used to audit changes inside the environment, and even roll back changes to a previous state that vRealize Network Insight has recorded.

It is also possible to audit the working of the security policies on a VM. The Security Planner can show all connectivity happening on a per-VM basis, and you can have Allowed and Denied Flows auditing from a VM level, as seen in Figure 6.8.



Scope where All flows MODIFY SCOPE

Security Planning

Tip: 10 segments are visible at a time, to see more segments use HIDE/SHOW

Traffic Distribution (by Total Bytes) **

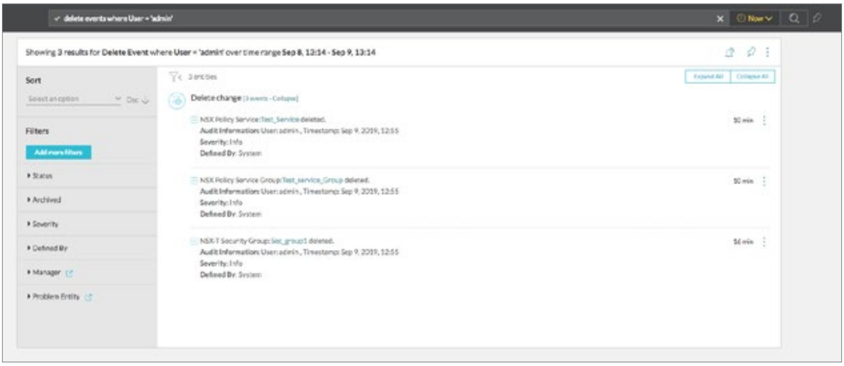
East-West (EW) 99% (86.7 TB)
Switched (% of EW) 91% (79.2 TB)
Routed (% of EW) 9% (7.5 TB)
VM to VM (% of EW) 99% (85.9 TB)
Host/Cloud Network 2% (1.9 TB)
Internet / North-South 1% (1 TB)

Top Ports by Bytes

Port	Count of Flow	Sum of Bytes
0	2	0 B
756	2	0 B
5353	12	160.2 KB
45025	2	0 B
4501	3	315.3 MB
61824	3	360 B
76 [devs]	2	0 B

Figure 6.8 Traffic flows overview dashboard example

vRealize Network Insight can capture and audit information of NSX objects quickly from the NSX Manager. The information includes the username who created or modified the NSX object, when the operation happened and the operation details on the object as shown in Figure 6.9.



delete events where User = 'admin'

Showing 3 results for Delete Event where User = 'admin' over time range Sep 8, 13:14 - Sep 9, 13:14

Delete change [3 events - Collapse]

NSX Policy Service:Test_Service deleted. 50 min
Audit Information: User: admin., Timestamp: Sep 9, 2019, 12:55
Severity: Info
Defined By: System

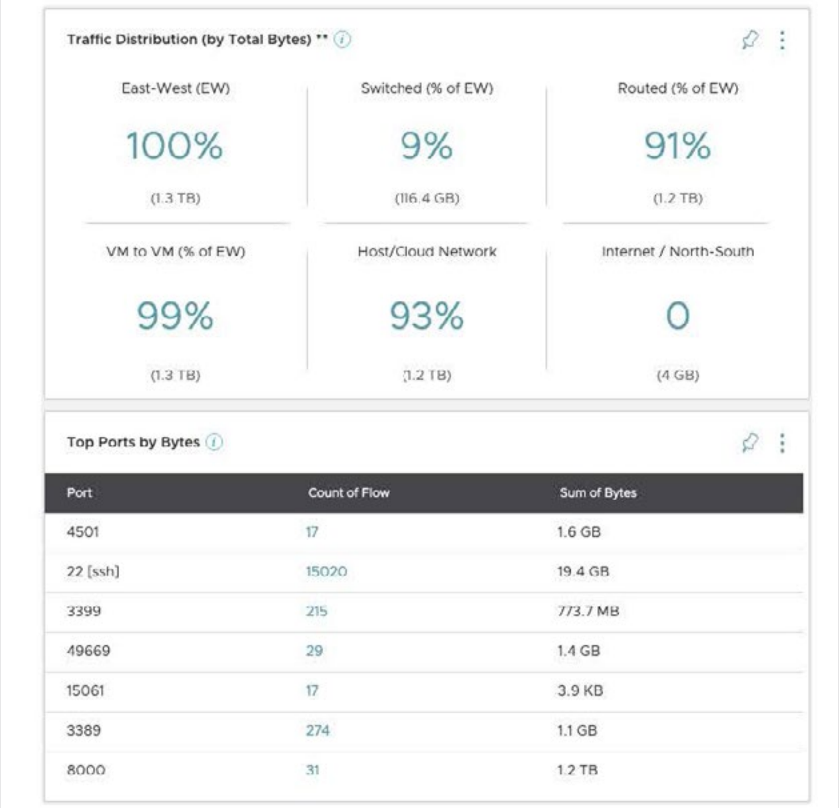
NSX Policy Service Group:Test_service_Group deleted. 50 min
Audit Information: User: admin., Timestamp: Sep 9, 2019, 12:55
Severity: Info
Defined By: System

NSX-T Security Group: Sec_group1 deleted. 56 min
Audit Information: User: admin., Timestamp: Sep 9, 2019, 12:55
Severity: Info
Defined By: System

Figure 6.9 Event audit example

Viewing Micro-segmentation and Flow Data

The network traffic flow data can be presented at a high level (e.g., showing the entire infrastructure), a per-object level (e.g., per network, application, or resource pool), and down to a granular per-flow record level. Starting from a high level, this is an excellent view to see what kind of behavior is happening inside infrastructure, as depicted in Figure 6.10. It shows how much traffic is north-south, east-west, VM-to-VM, and routed versus switched. It also gives a quick view of which network ports are used the most.



Traffic Distribution (by Total Bytes) **

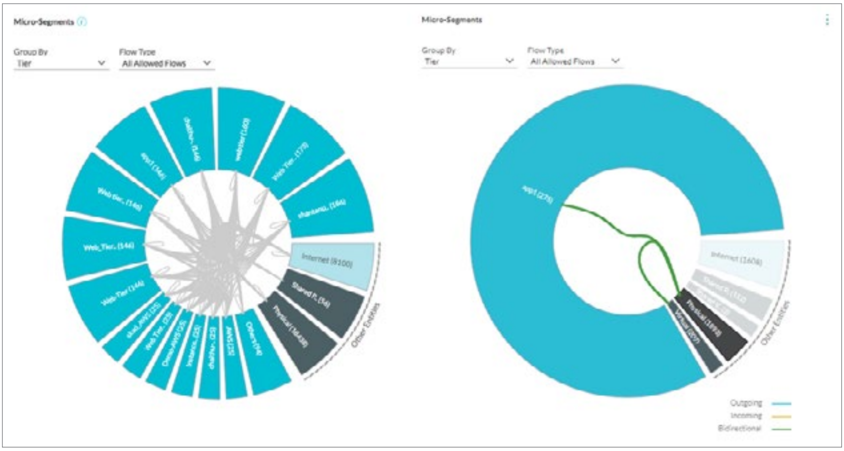
East-West (EW)	Switched (% of EW)	Routed (% of EW)
100%	9%	91%
(1.3 TB)	(116.4 GB)	(1.2 TB)
VM to VM (% of EW)	**Host/Cloud Network**	**Internet / North-South**
99%	93%	0
(1.3 TB)	(1.2 TB)	(4 GB)

Top Ports by Bytes

Port	Count of Flow	Sum of Bytes
4501	17	1.6 GB
22 [ssh]	15020	19.4 GB
3399	215	773.7 MB
49669	29	1.4 GB
15061	17	3.9 KB
3389	274	1.1 GB
8000	31	1.2 TB

Figure 6.10 Network flow data example

In the donut view, shown in Figure 6.11, the blue lines denote the outgoing flows, the green lines denote the incoming flows, and the yellow lines denote the flows that are bidirectional. Individual segments can be selected to view specific details.



Micro-Segments

Group By: Tier

Flow Type: All Allowed Flows

Micro-Segments

Group By: Tier

Flow Type: All Allowed Flows

Figure 6.11 Donut view data flow example

Recommended Firewall Rules

vRealize Network Insight also excels at proactive micro-segmentation operations; to learn more about NSX micro-segmentation, view the vRealize Network Insight Cookbook or download the **VMware NSX Micro-segmentation: Day 1** white paper referenced in Table 8.1 in the “Where to go for More Information” section. vRealize Network Insight provides a NetFlow-based assessment to model security groups and firewall rules. It also generates actionable recommendations for implementing micro-segmentation. The NetFlow-based assessment capability uses real time analytics and flow data correlation to provide insights into the data traffic flow profile. For example, it can identify the percentage of traffic that flowed east-west within the data center, what percent flowed to the Internet, and what percent was routed through physical networks. It offers a breakdown of individual services and ports used over that 24-hour period, and can then make recommendations for firewall rule development based on real time communications. These recommended rules can be imported directly into NSX for refinement and implementation.

Application Discovery and Operations

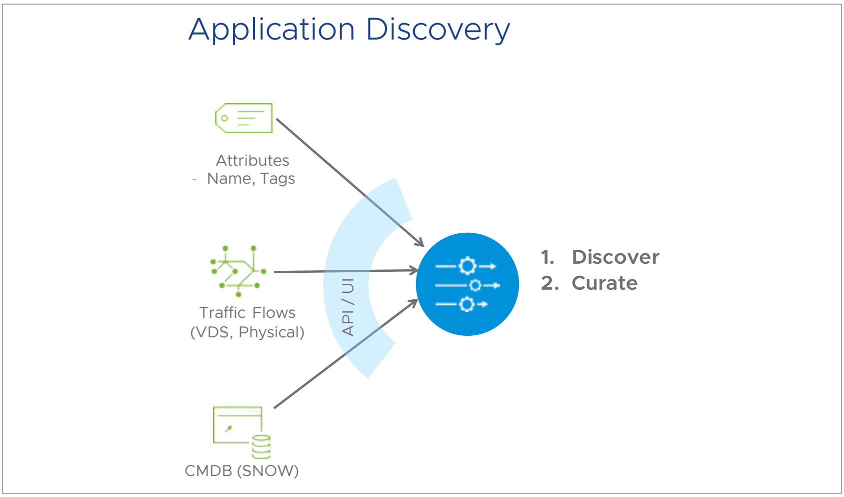
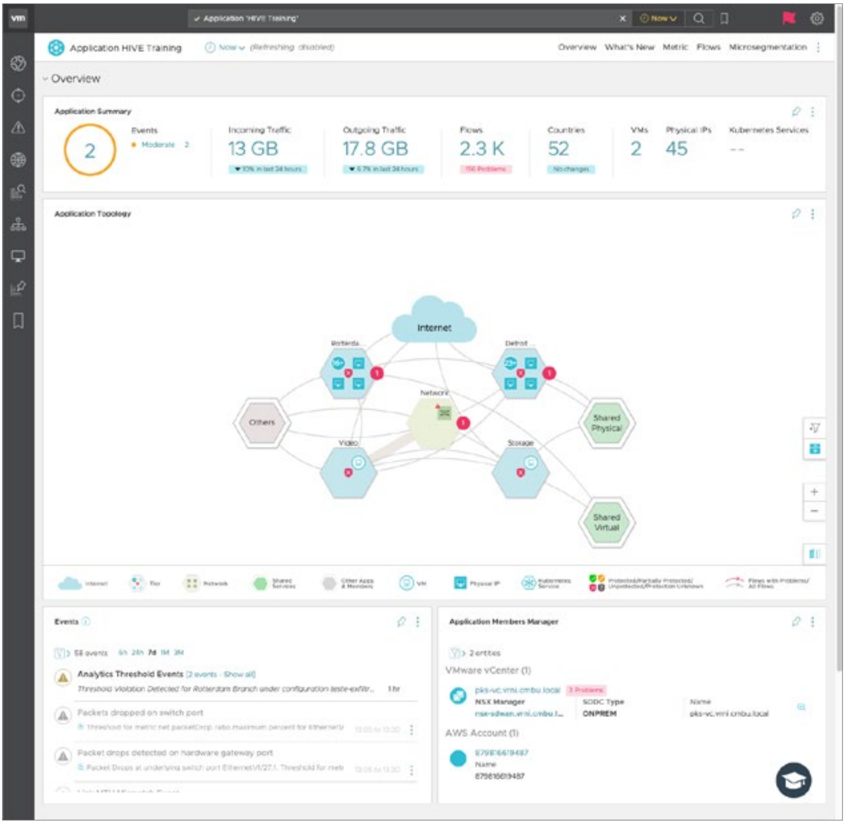


Figure 6.12 Application discovery overview

vRealize Network Insight focuses troubleshooting and monitoring on the application, as that's what is important in the end. Every single application gets its own dashboard, as seen in Figure 6.13. Networking admins and application owners can talk about the same concept, when they are sharing the terminology. The application dashboard includes the topology of the application itself, real-time network flows that flow between the tiers and the outside of the application, all infrastructure events, all workload metrics; everything the admin needs to troubleshoot the application. By zooming in, the tiers get expanded to include all workloads (VMs, containers) and the flow connections for each of those workloads.



Events	Incoming Traffic	Outgoing Traffic	Flows	Countries	VMs	Physical IPs	Kubernetes Services
2 ● Moderate 2	13 GB ▼10% in last 24 hours	17.8 GB ▼6.7% in last 24 hours	2.3 K 156 Problems	52 No changes	2	45	--

58 events 6h 24h 7d 1M 3M

Analytics Threshold Events [2 events · Show all]
Threshold Violation Detected for Rotterdam Branch under configuration teste-exfiltr... 1 hr

Packets dropped on switch port
Threshold for metric net.packetDrop.ratio.maximum percent for Ethernet1/

Packet drops detected on hardware gateway port
Packet Drops at underlying switch port Ethernet1/1/27.1. Threshold for metr

2 entities
VMware vCenter (1)
pks-vc.vrni.cmbu.local 3 Problems
NSX Manager: nsx-sdwan.vrni.cmbu.l...
SDDC Type: ONPREM
Name: pks-vc.vrni.cmbu.local

AWS Account (1)
879816619487
Name: 879816619487

Figure 6.13 vRNI application dashboard example

When working with several applications and across multiple tiers, creating applications using the public APIs or the user interface becomes along process. vRealize Network Insight automates their discovery and addition into vRealize Network Insight, significantly reducing much of the manual effort.

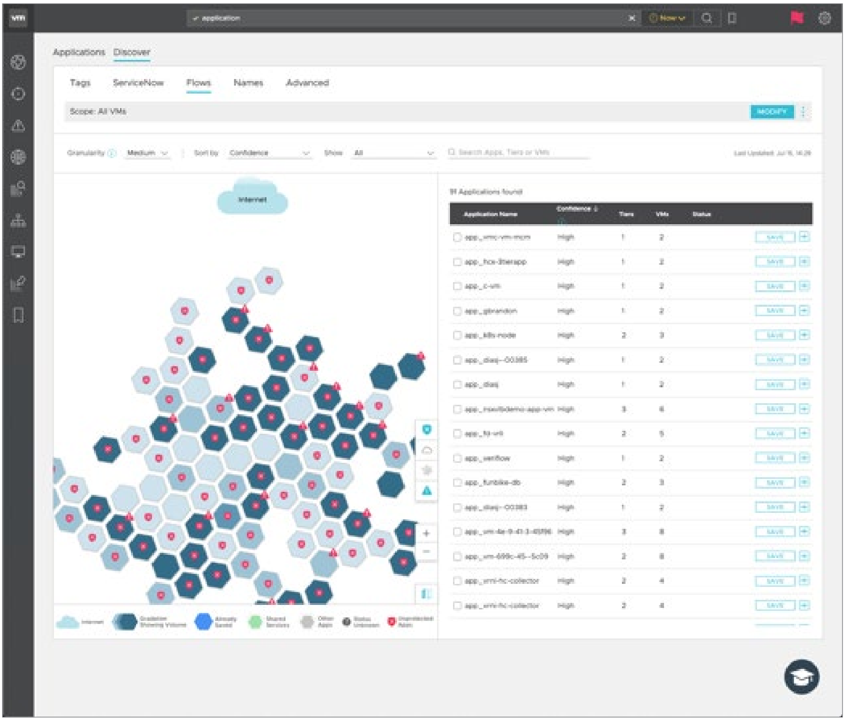
vRealize Network Insight can perform application discovery based on:

- Tags (vCenter, AWS, Azure, or NSX Security tags)
- Security groups
- VM names
- ServiceNow CMDB attributes
- Network traffic flows

The last option (traffic flows) is the most interesting one, using a Machine Learning algorithm to learn about the application and tier boundaries by simply looking at the traffic flowing through the network.

vRealize Network Insight provides planning and recommendations for implementing the micro-segmentation security. It helps the user to manage and scale the VMware NSX deployments quickly and confidently.

As seen in Figure 6.14 below, the discovered applications are easy to filter and review. There are filters available to show only the applications that are talking to the Internet or only show the top 10/20/50/100 applications based on the amount of member VMs. It can also focus on the unprotected VMs (i.e., the ones that do not have NSX firewall rules attached to them) or filter out the applications that offer shared services (e.g., DNS, NTP, AD), or are commonly used by other applications and save them for troubleshooting, monitoring, or security planning.



Scope: All VMs

Granularity: Medium · Sort by: Confidence · Show: All · Search Apps, Tiers or VMs · Last Updated: Jul 16, 14:29

11 Applications found

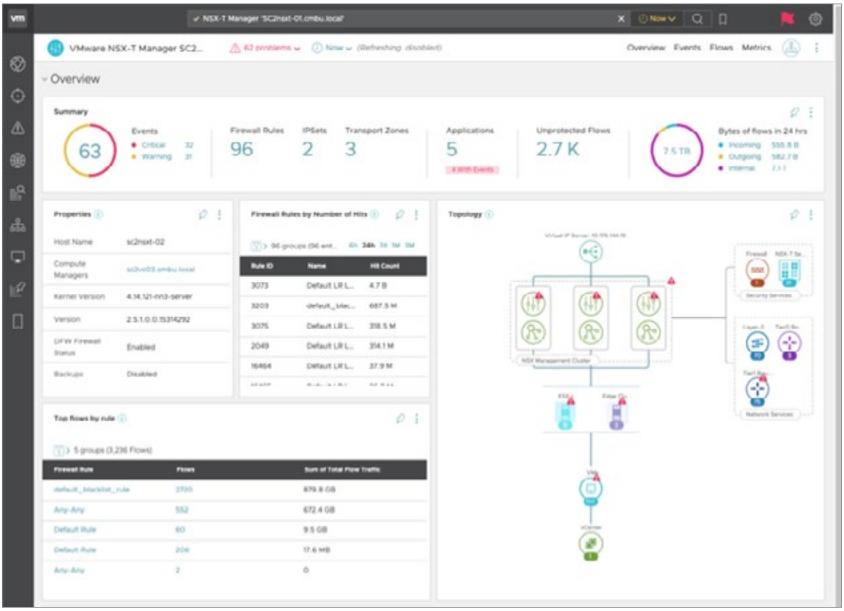
Application Name	Confidence	Tiers	VMs	Status
□ app_vmc-vm-mcm	High	1	2	SAVE
□ app_hcx-3tierapp	High	1	2	SAVE
□ app_c-vm	High	1	2	SAVE
□ app_gbrandon	High	1	2	SAVE
□ app_k8s-node	High	2	3	SAVE
□ app_diasj--00385	High	1	2	SAVE
□ app_diasj	High	1	2	SAVE
□ app_nsxv9demo-app-vm	High	3	6	SAVE
□ app_fd-vm	High	2	5	SAVE
□ app_vertflow	High	1	2	SAVE
□ app_funbike-db	High	2	3	SAVE
□ app_diasj--00383	High	1	2	SAVE
□ app_vm-4e-9-41-3-45f96	High	3	8	SAVE
□ app_vm-699c-45--5c09	High	2	8	SAVE
□ app_vrni-hc-collector	High	2	4	SAVE
□ app_vrni-hc-collector	High	2	4	SAVE

Figure 6.14 Discovered applications example

NSX Operations Dashboard

When IPFIX is enabled on the NSX data source, the NSX distributed firewall will starts sending IPFIX to vRealize Network Insight. The added value of doing so is that NSX also sends flows that are blocked from going on the network by the distributed firewall. It also flags allowed flows with a matching firewall rule ID, if any, allowing Network Insight to correlate flows to existing firewall rules.

This integration enables quick identification of any flows not protected by any firewall rules and creation of a 'to-do' diagram of network flows still requiring micro-segmentation.


✓ NSX-T Manager 'SC2nsxt-01.cmbu.local'

VMware NSX-T Manager SC2... ⚠ 63 problems ⌄ Now ⌄ (Refreshing disabled)

Overview Events Flows Metrics

Overview

Summary

63 Events ● Critical 32 ● Warning 31

Firewall Rules 96 IPSets 2 Transport Zones 3 Applications 5 (4 With Events) Unprotected Flows 2.7 K

7.5 TB Bytes of flows in 24 hrs ● Incoming 555.8 B ● Outgoing 582.7 B ● Internal 7.1 T

Properties

Host Name	sc2nsxt-02
Compute Managers	sc2vc03.cmbu.local
Kernel Version	4.14.121-nn3-server
Version	2.5.1.0.0.15314292
DFW Firewall Status	Enabled
Backups	Disabled

Firewall Rules by Number of Hits

96 groups (96 ent... 6h 24h 7d 1M 3M

Rule ID	Name	Hit Count
3073	Default LR L...	4.7 B
3203	default_blac...	687.5 M
3075	Default LR L...	318.5 M
2049	Default LR L...	314.1 M
16464	Default LR L...	37.9 M

Top flows by rule

5 groups (3,236 Flows)

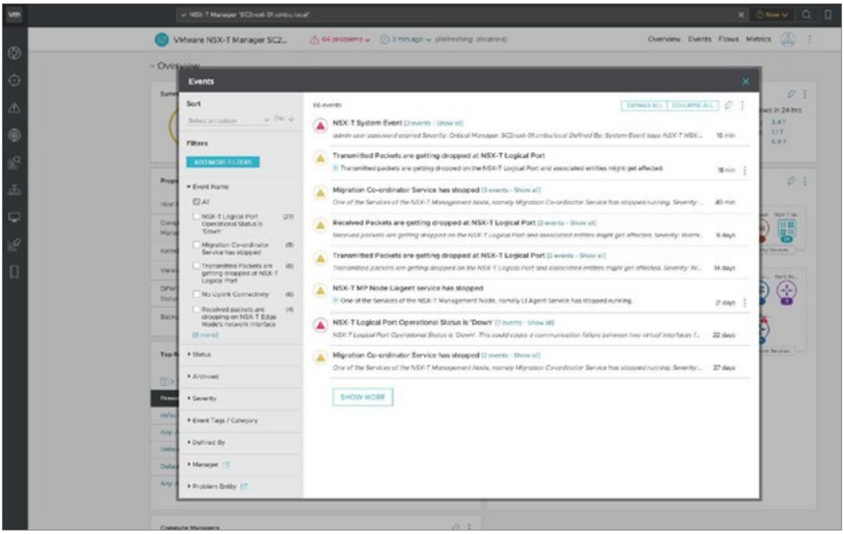
Firewall Rule	Flows	Sum of Total Flow Traffic
default_blacklist_rule	2720	879.8 GB
Any-Any	552	672.4 GB
Default Rule	60	9.5 GB
Default Rule	206	17.6 MB
Any-Any	2	0

Topology

Figure 6.15 Distributed firewall rules dashboard example

Best Practices Checklist Monitoring

Another useful feature of vRealize Network Insight is the best practices checklist monitoring. The best practices checklist is a collection of NSX rules based on real-life deployments. These were developed from an operations' perspective related to the critical parameters and thresholds of the NSX management, control, and data planes. vRealize Network Insight proactively monitors the NSX environment for violations of the best practice checklist rules and allows quick identification the offending components for remediation. A sample checklist failure screen is shown in Figure 6.16.


VMware NSX-T Manager SC2...
64 problems
3 min ago
(Refreshing disabled)
Overview
Events
Flows
Metrics
Events
Sort
Select an option
Dsc
Filters
ADD MORE FILTERS
Event Name
All
NSX-T Logical Port Operational Status is 'Down' (27)
Migration Co-ordinator Service has stopped (8)
Transmitted Packets are getting dropped at NSX-T Logical Port (8)
No Uplink Connectivity (6)
Received packets are dropping on NSX-T Edge Node's network interface (4)
[8 more]
Status
Archived
Severity
Event Tags / Category
Defined By
Manager
Problem Entity
64 events
EXPAND ALL
COLLAPSE ALL
SHOW MORE

NSX-T System Event [2 events - Show all]
admin user password expired Severity: Critical Manager: SC2nsxt-01.cmbu.local Defined By: System Event tags: NSX-T NSX-... 16 min

Transmitted Packets are getting dropped at NSX-T Logical Port
Transmitted packets are getting dropped on the NSX-T Logical Port and associated entities might get affected. 18 min

Migration Co-ordinator Service has stopped [3 events - Show all]
One of the Services of the NSX-T Management Node, namely Migration Co-ordinator Service has stopped running. Severity: ... 49 min

Received Packets are getting dropped at NSX-T Logical Port [2 events - Show all]
Received packets are getting dropped on the NSX-T Logical Port and associated entities might get affected. Severity: Warn... 8 days

Transmitted Packets are getting dropped at NSX-T Logical Port [2 events - Show all]
Transmitted packets are getting dropped on the NSX-T Logical Port and associated entities might get affected. Severity: W... 14 days

NSX-T MP Node Liagent service has stopped
One of the Services of the NSX-T Management Node, namely LI Agent Service has stopped running. 21 days

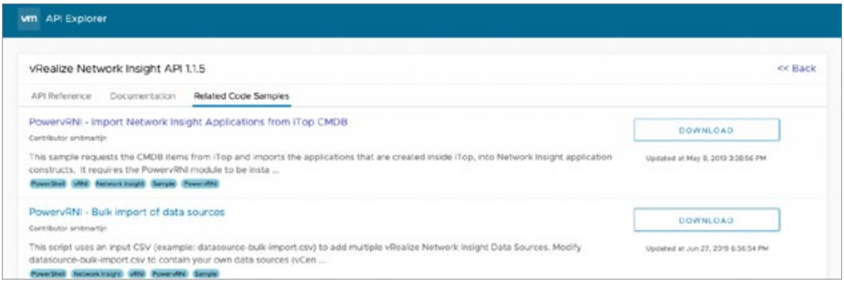
NSX-T Logical Port Operational Status is 'Down' [7 events - Show all]
NSX-T Logical Port Operational Status is 'Down'. This could cause a communication failure between two virtual interfaces f... 22 days

Migration Co-ordinator Service has stopped [2 events - Show all]
One of the Services of the NSX-T Management Node, namely Migration Co-ordinator Service has stopped running. Severity: ... 27 days

Figure 6.16 Example best practice checklist failure listing

Built-in API Explorer

Network operators can use APIs to automate workflows in vRealize Network Insight. The APIs follow the REST style similar to the NSX API. The API documentation for the vRealize Network Insight public API is available from inside the interface. The API Explorer contains information on all API endpoints.



vRealize Network Insight API 1.1.5

PowervRNI - Import Network Insight Applications from iTop CMDB
Contributor smitmartijn
This sample requests the CMDB items from iTop and imports the applications that are created inside iTop, into Network Insight application constructs. It requires the PowervRNI module to be insta ...
PowerShell vRNI Network Insight Sample PowervRNI
Updated at May 9, 2019 3:28:56 PM

PowervRNI - Bulk import of data sources
Contributor smitmartijn
This script uses an input CSV (example: datasource-bulk-import.csv) to add multiple vRealize Network Insight Data Sources. Modify datasource-bulk-import.csv to contain your own data sources (vCen ...
PowerShell Network Insight vRNI PowervRNI Sample
Updated at Jun 27, 2019 6:56:54 PM

Figure 6.17 API endpoint information access from the built-in API explorer

To make automating against vRealize Network Insight easier, there are SDKs for both PowerShell and Python available. These include a list of examples around adding applications, data sources, retrieving data such as flows, and many more.

- The PowerShell module called PowervRNI: https://powervrni.github.io/
- Python SDK: https://github.com/vmware/network-insight-sdk-python

vRealize Operations

vRealize Operations and the subscription-based vRealize Operations Cloud provide self-driving operations management from infrastructure to applications across physical, virtual, and multi-cloud environments. For NSX it provides inventory monitoring and troubleshooting, as well as capacity and performance management of NSX resources like management clusters and services, edge clusters, logical switches and routers, transport zones and nodes, load balancers, and firewalls. In addition to monitoring these resources, it provides file system usage for individual nodes in the controller cluster, transmitted/received bytes, and packet drop metrics for the Ethernet interfaces. There are more than 25 out-of-the-box alerts related to these monitored resources.

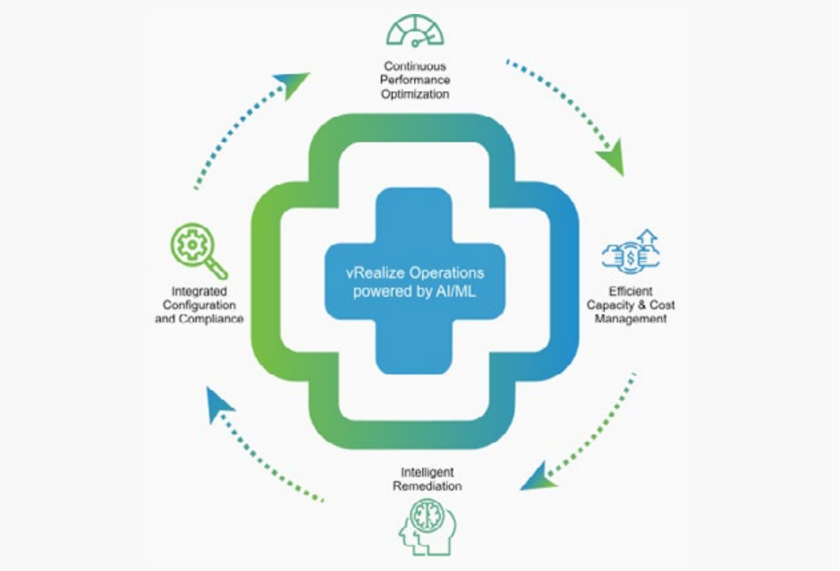
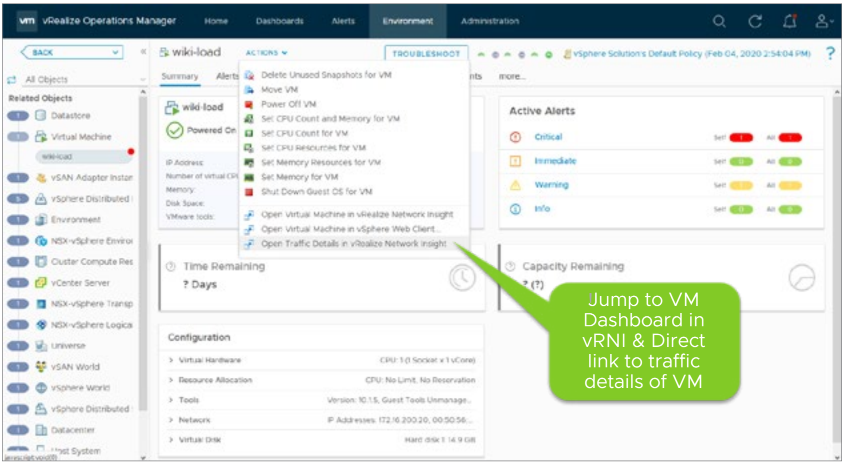

Continuous Performance Optimization
Efficient Capacity & Cost Management
Intelligent Remediation
Integrated Configuration and Compliance
vRealize Operations powered by AI/ML

Figure 6.18 vRealize Operations areas of focus

vRealize Network Insight can also be integrated with vRealize Operations, to provide more network and security context within vRealize Operations. The integration provides access to alerts and potential issues identified by vRealize Network Insight that are associated with the relevant NSX-T objects in vRealize Operations. Shared objects such as NSX Edge, Virtual Machine, and vSphere Host have a 'launch in context' option in the Actions menu and the ability to jump directly to the appropriate screen in vRealize Network Insight as seen in Figure 6.19.



Jump to VM Dashboard in vRNI & Direct link to traffic details of VM

Figure 6.19 Example of vRealize Operation's launch in context

Apart from health monitoring, another use-case that vRealize Operations supports in the context of NSX is the ability to monitor utilization of NSX and set alerts in comparison to the configuration maximums (e.g. Edge Node count, ARP Entries, Tag count) either on-premises or in VMware Cloud on AWS SDDCs.

vRealize Log Insight

vRealize Log Insight provides heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility. This enables deep operational visibility and faster troubleshooting. The Log Insight Content Pack for NSX provides operational reporting, trending, and alerting visibility for all sources of log data within NSX. Each major NSX function—logical switching, routing, distributed firewalls, gateways, and edge services—is represented via custom dashboards, filters, and alerts.

It is structured in a hierarchical manner, starting at an overview level showing problems based on a rollup of underlying NSX components. Each level provides specific, actionable information associated with the problem. This guides the troubleshooting effort to the appropriate next level of NSX component dashboard that shows specific alerts. These alerts display specific problems and recommended remediation actions.

Figure 6.20 shows the out-of-the-box top dashboard for NSX-T within vRealize Log Insight.

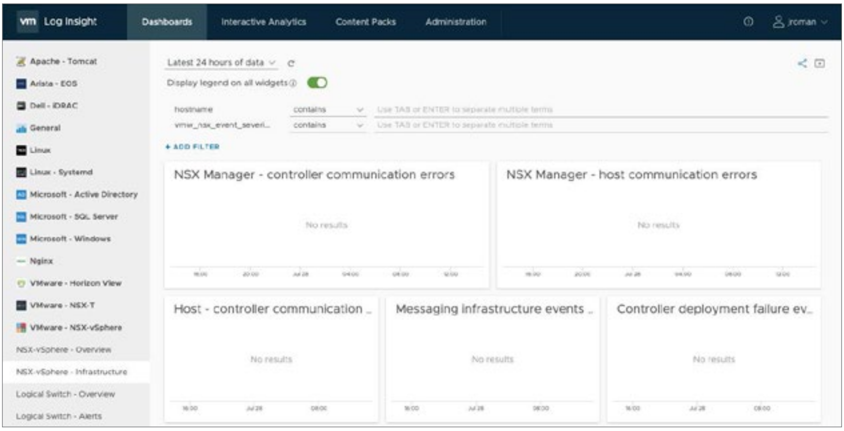


Figure 6.20 vRealize Log Insight top level dashboard for NSX-T

The NSX-T Log Insight Content Pack provides for additional collection, consolidation, and correlation of NSX log data. This graphically rich content pack contains 7 dashboards and 52 widgets used to represent the NSX-T logs graphically and make them more intuitive and actionable. The content pack covers NSX-T functions such as audit information, logical switch, logical router, firewall traffic, DHCP. NSX-T administrators can view issues related to communication between different NSX components. The logs include audit information, errors, configuration and traffic patterns. This content pack provides last mile troubleshooting to complement the monitoring and troubleshooting capabilities of vRealize Network Insight and vRealize Operations.

When debugging issues, distributed firewall traffic logging is very useful for working with network traffic in real-time. Selecting **Distributed Firewall – Overview** results in Figure 6.21.

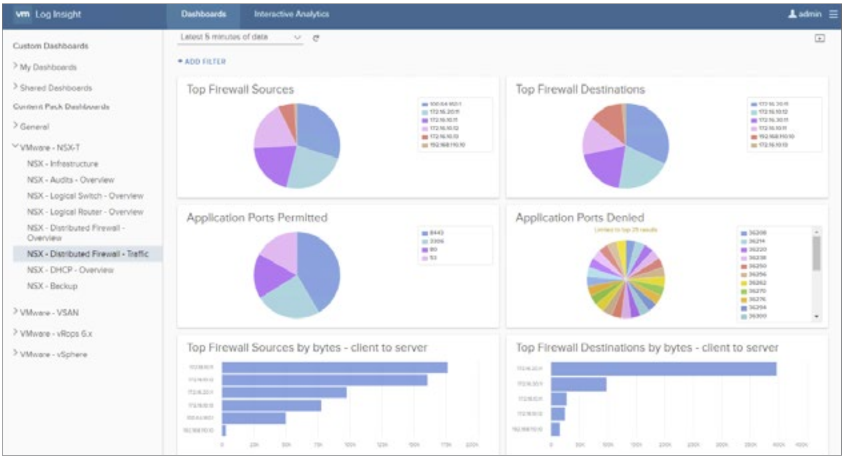
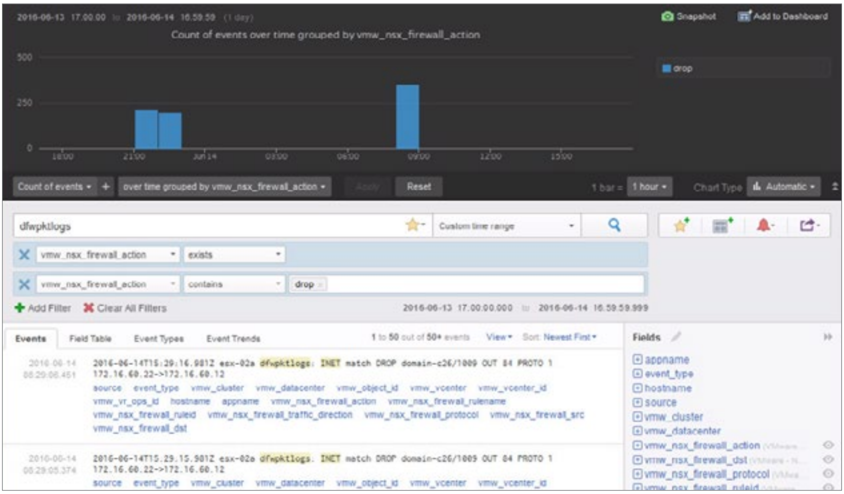


Figure 6.21 Distributed Firewall Overview dashboard in vRealize Log Insight

To further explore the **Firewall Actions** resulting in drops, hover over the line depicting drops in the **Firewall Action** pane and access the details shown in Figure 6.22.



dfwpktlogs

vmw_nsx_firewall_action exists

vmw_nsx_firewall_action contains drop

2016-06-13 17:00:00.000 to 2016-06-14 16:59:59.999

1 to 50 out of 50+ events

```
2016-06-14    2016-06-14T15:29:16.981Z esx-02a dfwpktlogs: INET match DROP domain-c26/1009 OUT 84 PROTO 1
08:29:06.451  172.16.60.22->172.16.60.12
              source event_type vmw_cluster vmw_datacenter vmw_object_id vmw_vcenter vmw_vcenter_id
              vmw_vr_ops_id hostname appname vmw_nsx_firewall_action vmw_nsx_firewall_rulename
              vmw_nsx_firewall_ruleid vmw_nsx_firewall_traffic_direction vmw_nsx_firewall_protocol vmw_nsx_firewall_src
              vmw_nsx_firewall_dst

2016-06-14    2016-06-14T15:29:15.981Z esx-02a dfwpktlogs: INET match DROP domain-c26/1009 OUT 84 PROTO 1
08:29:05.374  172.16.60.22->172.16.60.12
              source event_type vmw_cluster vmw_datacenter vmw_object_id vmw_vcenter vmw_vcenter_id
```

Figure 6.22 Firewall Actions log details in vRealize Log Insight

The log entry shows **172.16.60.22** (Web-03a) issued a ping to **172.16.60.12** (Web-04a). It was dropped due to firewall rule # **1009**, which is the expected behavior.

Figure 6.22 also demonstrates vRealize Log Insight's filtering power. The **Filter** option allows a user to dynamically extract any field from the data using regular expression. The extracted fields can be used for selection, projection, and aggregation. The **Fields** pane on the right side of the screen allows for customization in search and display of data classifications and keywords.

vRealize Log Insight is also available as a VMware cloud service called vRealize Log Insight Cloud and was formerly known as VMware Log Intelligence. The service provides fully managed and integrated log analytics and troubleshooting service. It works across VMware-based private clouds, VMware Cloud on AWS, and native public clouds such as AWS.

NSX-T Splunk App

VMware also provides a VMware-supported Splunk application for NSX-T. It is available at https://my.vmware.com/. It includes the same widgets and dashboards than the NSX-T Log Insight Content Pack and provides:

- Centralized log collector for different NSX-T virtual networking services
- Several dashboards and widgets representing graphical view of logging data for NSX-T components
- Information on audit, configuration, traffic, and error logs for NSX-T

Partner Ecosystem Tools

NSX has a growing ecosystem of technology partners that have integrated monitoring, troubleshooting, logging, and auditing functionality. Examples include the NetScout vSTREAM virtual appliance and Gigamon GigaVUE-VM.

In addition to traffic redirection through a service, NSX-T also supports the network monitoring use case as of version 2.5. In this use case, copies of packets are forwarded to a partner service virtual machine (SVM), allowing inspection, monitoring, or collection of statistics while the original packets do not pass through the network monitoring service.

For a complete list of partner ecosystem tools, the latest updates as well as version compatibility, check the online VMware Compatibility Guide.

Conclusion

As part of VMware's SDDC, NSX delivers a previously unheard of level of flexibility and agility with its software-defined networking and security capabilities. To fully leverage these capabilities in a sustained manner, VMware highly recommends optimizing operations for a software-defined infrastructure. To be truly effective, optimize the deployment of the most valuable resources—people—in blended teams. Ensure they have the right skills to not only make the NSX operations successful, but to make them successful as both individuals and as a team. Optimize critical operational processes to take advantage of the opportunities software-defined networking and security provide. Leverage the new breed of tools providing intelligent operations to enhance monitoring and troubleshooting capabilities for NSX and the software-defined datacenter. Making these changes enables an operating model that allows a shift to an intelligent operations mindset. Adopting NSX technology and adapting operating models in these ways will best leverage the investments in and realize the benefits of software-defined networking and security.

Where to go for more information

Description	Reference
Organizing for the Cloud	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutionoverview/vmware-oganizing-for-the-cloud-feb2017.pdf
NSX Troubleshooting Guide	http://pubs.vmware.com/nsx-63/topic/com.vmware.ICbase/PDF/nsx_63_troubleshooting.pdf
Troubleshooting VMware NSX for vSphere 6.x (KB2122691)	https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2122691
NSX-T Data Center Documentation	https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html
NSX-T API Documentation	https://code.vmware.com/apis/976/nsx-t
NSX-T CLI Documentation	https://vdc-download.vmware.com/vmwb-repository/dcr-public/cc42e3c1-eb34-4567-a916-147e79798957/8fff776d-fabd-4157-9c79-fdec07a5599f/nsxt_30_cli.htm
NSX-T Reference Guide	https://communities.vmware.com/docs/DOC-37591
NSX Intelligence Product Documentation	https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html
vRealize Network Insight Cookbook	https://lostdomain.org/vrealize-network-insight-cookbook/
VMware Compatibility Guide	https://www.vmware.com/resources/compatibility/search.php
Ansible Documentation	https://docs.ansible.com/
NSX-T Terraform Provider	https://www.terraform.io/docs/providers/nsxt/index.html
VMware PowerCLI	https://code.vmware.com/web/tool/12.0.0/vmware-powercli
NSX CLI	http://pubs.vmware.com/nsx-63/topic/com.vmware.ICbase/PDF/nsx_63_cli.pdf
Python SDK	https://code.vmware.com/web/sdk/2.5.1/nsx-t-python
Java SDK	https://code.vmware.com/web/sdk/2.5.1/nsx-t-java
NSX for vSphere API	http://pubs.vmware.com/nsx-63/topic/com.vmware.ICbase/PDF/nsx_63_api.pdf
Automation Leveraging NSX REST API	https://communities.vmware.com/docs/DOC-31921
NSX Logging and System Events	http://pubs.vmware.com/nsx-63/topic/com.vmware.ICbase/PDF/nsx_63_logging_and_system_events.pdf
NSX documentation	https://www.vmware.com/support/pubs/nsx_pubs.html

Description	Reference
VMware NSX Mirco-segmentation: Day 1	http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf
Organizing for the Cloud	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/services/vmware-organizing-for-the-cloud-white-paper.pdf
High performance organizations	"Lean Enterprises", by Jez Humble, Joanne Molesky, and Barry O'Reilly

As part of VMware's Software Defined Data Center, NSX provides software defined networking and security capabilities that deliver previously unheard of levels of flexibility and agility. To fully leverage these capabilities in a sustained manner, certain operational optimizations should be considered.

Operationalizing VMware NSX brings together knowledge and guidance for optimizing the ongoing operations of the VMware NSX component of a software defined data center. It addresses both tactical optimizations —such as tooling for monitoring and troubleshooting—and strategic organization – including team structure, culture, roles, responsibilities, and skillsets – all while supporting ITSM process considerations. This revision of *Operationalizing VMware NSX* is being published to include the many advances, represented by VMware NSX for Data Center, made since the original version published in 2017.

NSX has already helped over a thousand organizations improve the network and security posture of their software defined data center by fundamentally changing the way they approach network and security.

Operationalizing NSX is your roadmap to fully realizing the benefits provided by a software defined data center running NSX. You will find proven insights and recommendations for optimizing the way you organize and operate the environment, unlocking its full potential to provide the flexibility and agility your business stakeholders require.

ISBN-10: 0-9986104-3-7
ISBN-13: 978-0-9986104-36

ISBN 9780998610436
51299 >
9 780998 610436

vmware®

www.vmware.com/go/nsx
www.cloud.vmware.com/vmc-aws