the GORILLA GUIDE® to...

VMware Aria Operations for Networks

Optimize Applications End-to-End

JOEP PISCAER

vmware®

POWERED BY ActualTech MEDIA

THE GORILLA GUIDE TO...

VMware Aria Operations for Networks

By Joep Piscaer

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM VMWARE
Sehjung Hah
Matt Just
Martijn Smit
Abhijit Timble

ABOUT THE AUTHOR

Joep Piscaer is a seasoned IT professional, with 10-plus years experience as a CTO, head of IaaS and infrastructure, (enterprise) architect, and technical consultant. His specialization is in infrastructure, cloud, and way-of-work (DevOp, Infrastructure-as-Code). He has built Infrastructure-as-Code toolchains, IaaS platforms, transformed (infrastructure-focused) organizations to DevOps and Infrastructure-as-Code ways of work.

ENTERING THE JUNGLE

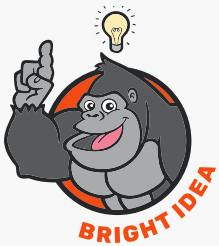
CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

The Gorilla is the professorial sort that enjoys helping people learn. In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.



BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Clouds Make It Harder To See

Welcome to The Gorilla Guide To®... Network Visibility with VMware Aria Operations for Networks! If you need to understand the necessity of knowing what your network is up to, this is the book for you.

The reality for IT teams these days is that there's more going on with your network than ever before: on-premises infrastructure has broken out, going to the cloud—or multiple clouds. That means data and applications are no longer confined to your walled garden, nor are the wires that they run across.

With all that "stuff" out there now, it can seem like an impossibly daunting task to properly track it all, and know what's happening where. But that's exactly what you need to do if you're going to properly manage your network. And that's where this Guide comes in.

It provides all the basics you need to know about network visibility. But it doesn't stop there—it also provides an overview of the means to obtain that visibility and use it to keep your network humming along smoothly.

VMware Aria Operations™ for Networks is the industry's leading way to manage this increasingly complex web of connections, and this book shows you what it can do. Once you've finished reading, you'll have a much greater understanding of what "network visibility" requires

in this modern age, and how VMware Aria Operations for Networks is designed to tackle the challenge.

VMware Aria Operations™ for Networks Universal can be deployed as a SaaS or deployed on-premises with the option to move to SaaS later during the subscription which makes the solution easy to use and operate and to run applications better.

If you're ready to get started, let's dive into Chapter 1, the jungle known as "hybrid cloud," and how it's changed the game, for both good and not-so-good when it comes to complexity.

CHAPTER 1

Hybrid Cloud Complexity

IN THIS CHAPTER:

- Hybrid cloud introduces additional complexity for networking admins
- Multiple networking vendors and public cloud services obscure visibility
- Security planning in heterogenous environments is hard

With the rise of public cloud, IT environments are becoming more difficult to manage. In addition to the on-premises data center, managing cloud estates and services requires additional knowledge, including different configurations and best practices. And the networks connecting private, hybrid, and public clouds are a significant part of managing that complexity.

Because networks go hand-in-hand with security and compliance, managing network configuration and security policies across these heterogenous environments is no trivial task.

This Gorilla Guide will focus on the network and security aspects of managing hybrid environments, and by extension the public cloud. In this chapter, we'll look at why public cloud and hybrid environments are harder to manage and operate.

Current Networking Challenges

Managing static, tightly controlled networks is a thing of the past. Networks are becoming highly dynamic and constantly changing and adapting. In addition, the cloud's ease of use leads to environments constantly being created and destroyed. How do you manage this high degree of variability while maintaining a tight security posture and essential visibility into changes?

Networking admins (and those in similar roles) face issues in these areas:

Time. A major benefit of using public cloud resources is the reduced time needed to start using a service, reducing the lead time for any project-dependent infrastructure and cloud resources. This helps speed up projects, as less time is spent on prerequisites and "plumbing," delivering value faster.

However, this also means there is less time to make sure configuration and policies used in these projects is compliant and secure. This can mean (potential) security issues need to be fixed later, or become hurdles to quick project completion.

Complexity. With breadth of possible services at your fingertips, it's easy to create heterogeneous environments across different vendors, products, and services—and the larger the variance of vendors in use, the harder it is to manage and operate the environment. This is especially true when it comes to applying security policies across the entire environment, as well as maintaining and proving security compliance.

Heterogenous configuration and potentially inconsistent security policies across the infrastructure compromise security compliance, muddying the otherwise clear waters of networking across the hybrid cloud environment.

Visibility. With a high volume of changes, maintaining a clear picture of the networking environment is crucial. Taking inventory of the

application landscape in the static networks of yore was one thing—doing the same in the ever-changing hybrid cloud environment is something else entirely. Taking inventory by discovering changes and doing dependency mapping to keep an up-to-date understanding of the application landscape has become more important as the number of changes in the environment increases.

Application Visibility

Many application architectures followed a similar architectural style of a database server, application logic servers, and web (or other front-end) servers, all running in virtual machines (VMs) on vSphere, plus a small number of VLANs that defined security characteristics.

But these days, applications are no longer "just a couple of VMs on VLANs." Applications run across networks, data centers, sites, and clouds. And they consist of more than just VMs: Involved systems can now include Software as a Service (SaaS), public cloud services, containers, third-party APIs and services, and more.

Microservices are a perfect example of the new challenges. Many applications are now broken down into a series of components—microservices—that can be scattered everywhere and re-used across different applications. How do you gain visibility into those complex beasts, including which services are dependent on others?

Security Planning

Then, after figuring out the grouping and dependencies, comes the necessary but difficult work of applying the right (granular) security settings.

Granular security solutions like micro-segmentation and distributed routing are great for tightening up the security posture. But how do you know what security rules to set? How do you even know which VMs make up an application, and what traffic flows between them?

Multi-Vendor Complexity

Networks grow and change organically. When public cloud is then brought in, new networking and security vendors enter the picture. How do you get visibility into traffic flows across different technology stacks?

Hybrid Cloud Migration Planning

Managing hybrid and multi-cloud can be a challenge for even the most experienced admin. That's why obtaining and maintaining visibility on these complex and dynamic environments across disparate technologies is essential.

There's also the problem of migrating an application to the cloud safely, which involves knowing which parts are safe to migrate. In similar vein, workloads are starting to move from VMs to containers, which creates problems around visibility, security, and compliance.

Network Health

In addition, staying in control of the networking infrastructure comes with its own special headaches. With all the moving parts, it's vital to be able to quickly see configuration changes and check up on the health of networking solutions like micro-segmentation. On top of that, admins must perform ongoing monitoring and troubleshooting of networking issues for security, performance, compliance, and more. What's an already-overworked IT staff to do?

VMware Aria Operations for Networks

VMware has an answer. VMware Aria Operations for Networks provides seamless visibility across the data center and hybrid cloud, including the edge, branch offices, and remote sites.

VMware Aria Operations for Networks supports four main use cases:

- Micro-segmentation security planning
- Holistic, vendor-agnostic networking configuration overviews for troubleshooting
- Networking configuration health and best-practices checks
- Cloud migrations

Let's go over some of its capabilities in more depth.

Security Planning

VMware Aria Operations for Networks began life as a tool to take the guesswork out of micro-segmentation security planning for NSX (VMware's software-defined networking technology) environments. Its traffic flow analytics automatically suggest firewall rules to micro-segment workloads.

Application Visibility

The VMware Aria Operations for Networks analytics engine analyses traffic flows for application discovery and dependency mapping, which help networking admins define security policies through an application lens, instead of looking at just the raw networking and security data. These insights help admins plan changes to the application landscape (like cloud migrations), as well as network changes, helping them determine the impact on application performance when moving all or part of an application to the cloud.

In later releases, VMware Aria Operations for Networks added features for network operations, including monitoring, troubleshooting, and optimization. It's at the heart of VMware's networking products across on-premises and cloud environments. It's tightly integrated into the various NSX editions for on-premises and cloud, as well as the underlying transport networks with physical and virtual networking devices.

This end-to-end (or really, top-to-bottom) visibility into the various network layers help admins troubleshoot misbehaving applications and drill down into the root cause of configuration and operational issues.

Traffic Flows

Traffic flows provide full visual overview across on-premises and public cloud workloads, which makes VMware Aria Operations for Networks useful for managing multi-cloud security, too. It captures flow data via the vSphere Distributed Switch, NSX distributed firewall and, other (physical) devices across the network.

Traffic Telemetry

VMware Aria Operations for Networks analyzes flows to provider traffic metrics, like throughput, dropped packets, and other telemetry.

Networking Configuration

In addition to operational telemetry, VMware Aria Operations for Networks also stores configuration data from networking devices across the environment. This includes devices like switches, routers, load balancers, and firewalls. VMware Aria Operations for Networks queries and stores the current, *running* configuration of a networking device, as well as that of vCenter, NSX, and AWS VPCs.

Also stored are the configuration of physical and VMs and containers, taken from networking devices, vCenter, and NSX.

Vendor-Agnostic

VMware Aria Operations for Networks is vendor-agnostic, meaning it works with many third-party networking and security vendors to get visibility into hybrid cloud networking.

Agentless

VMware Aria Operations for Networks does not require agents, but instead relies on NetFlow, IPFIX, and sFlow to gather traffic telemetry from networking and security devices. Virtually every networking and security vendor, including those building virtualized network functions, support these protocols. All other data retrieval, such as configurations and metrics, also use industry-standard agentless protocols like API, SSH, and SNMP.

Internet Protocol Flow Information Export (IPFIX) is a standard for the format and export of network flow information. You can configure IPFIX for switches and firewalls. For switches, network flow at virtual interfaces (VIFs) and physical NICs (pNICs) is exported. For firewalls, network flow that is managed by the distributed firewall component is exported.

Enabling NetFlow on vCenter and IPFIX on NSX (both NSX-T and NSX-V) are the only "write" actions VMware Aria Operations for Networks does. For the rest, it only consumes data sent to its Collectors.

Built for Multi-Cloud

VMware Aria Operations for Networks gathers data from many different source environments and device types, ranging from VMware vSphere hosts, NSX network virtualization, and physical devices, as well as public cloud networking constructs.

Search Engine

A unique aspect of VMware Aria Operations for Networks is how open the product is: the search capabilities of VMware Aria Operations for Networks are very extensive, so networking admins are not limited to what the UI prescribes—customized search queries allow admins to build their own filtering and grouping. This is immensely powerful, even though using the search engine takes a little getting used to. We'll dive into that topic later.

Architecture

VMware Aria Operations for Networks is available as an on-premises installable product, as well as a SaaS offering to simplify deployment and operations. In the SaaS version, VMware takes care of installation, upgrades, platform security, availability and performance, and the underlying infrastructure.

Functionally, the two VMware Aria Operations for Networks editions are (mostly) identical, albeit deployed differently, as seen in **Figure 1**. In the on-premises version, you can deploy the platform and collector nodes as you see fit.

In the SaaS version, VMware hosts and controls the platform nodes (which run the analytics engine and UI, and contain the central data repository). The collectors are deployed inside the cloud tenants or on-premises to collect flow and configuration data and send it to the SaaS-hosted platform nodes.

Collectors collect configuration (like firewall rules and switch configs), inventory (e.g., vCenter and AWS inventory, VM and container metadata like operating systems, and network settings) and traffic flow information (like source, destination, and protocol/port). Collectors only collect metadata, not the contents of traffic flows or any other "actual" data. Collectors are usually placed as close as possible to the environment they're monitoring.

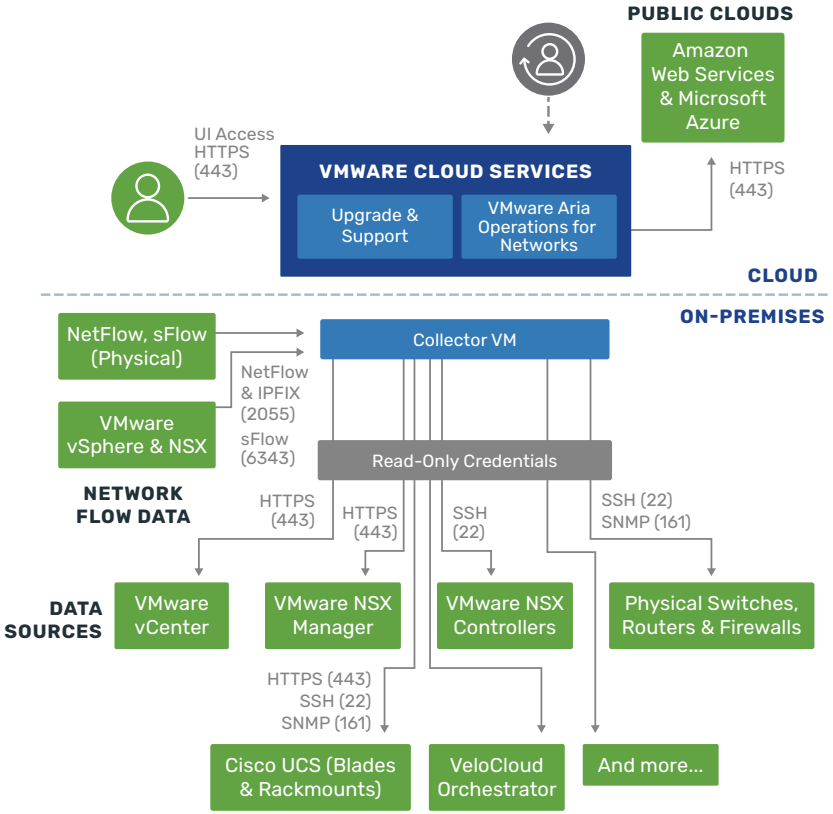


Figure 1: VMware Aria Operations for Networks platform architecture

The platform nodes ingest data and correlate this data, so that a destination IP address captured in a flow segment is correlated to the VM that has that IP address associated to it in its metadata. The platform nodes can scale vertically (using *t-shirt sizes* to denote different sizes of each appliance), as well as horizontally using multiple nodes in a deployment.

Up Next

Now that you have an overview of VMware Aria Operations for Networks, it's time to talk about gaining visibility into your applications. That's the focus of Chapter 2.

CHAPTER 2

Gaining Application Visibility

IN THIS CHAPTER:

- Taking application inventory and discovery
- Application dependency mapping
- Security planning

Application Discovery and Visibility

A key ability of VMware Aria Operations for Networks is putting the data it gathers to good use in gaining visibility into applications. It takes that networking data and, with the help of machine learning (ML), constructs meaningful insights into what networking components make up applications, how components are dependent on each other, which are shared, and where the different components run.

The process starts with VMware Aria Operations for Networks collectors taking inventory of the various physical components—switches, routers, firewalls, load balancers, and so on—as well as virtual components, including vCenter, NSX, and AWS inventories.

By turning on network flow collection, VMware Aria Operations for Networks helps admins understand the movement between application components, allowing network engineers to look at traffic data with an application perspective.

As mentioned, this method uses ML to discover application boundaries automatically. First, traffic flows are analyzed to figure out application boundaries, grouping VMs that mostly talk more among themselves, and determining tiers within the application based on similar same traffic patterns (like VMs with the same network ports opened). The ML algorithms also detect shared services, identifying services like Active Directory or DNS.

The honeycomb widget (**Figure 2**) shows these discovered applications in a way that lets admins filter and sort components visually, and group them into user-defined applications.

It's important to note that these groupings do not consist solely of the application components themselves—VMware Aria Operations for Networks is a networking-focused product. Application groupings in VMware Aria Operations for Networks include any and all of the networking components that support the application components, including physical switches, virtual networking, distributed firewalls, load balancers, and interconnects between cloud and on-premises, and more.

Analyzing its traffic flows, VMware Aria Operations for Networks can help determine which workloads on the network communicate and over which protocols. Admins then group these components into applications, and optionally mark components as shared between applications.

The honeycomb widget is an ideal starting place to define and group discovered applications. Each hexagon in the widget is a collection of different infrastructure components that VMware Aria Operations for Networks has identified as part of an application definition.

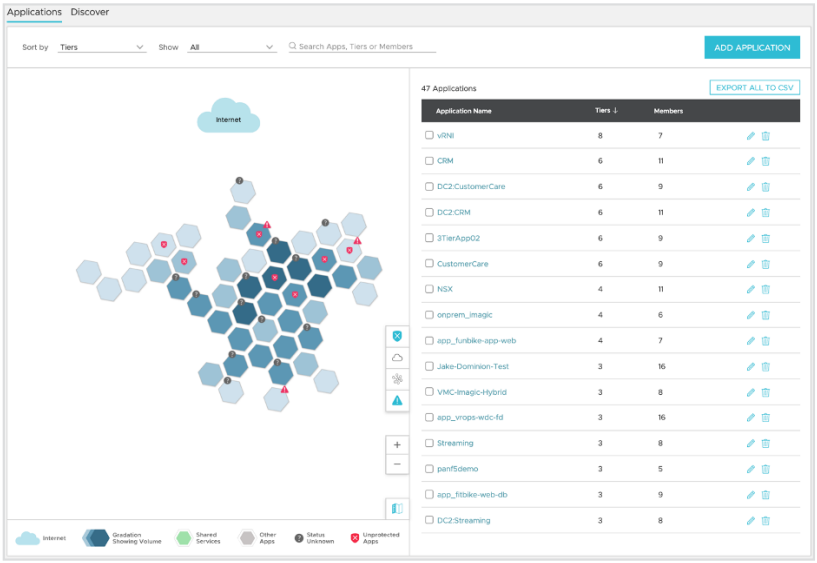


Figure 2: The honeycomb widget visually represents discovered applications

Filters can be applied to show different characteristics, like unprotected flows, talking to the internet, shared application services, or applications with issues. These filters will change the honeycomb visualization.

A traffic flow is defined as a stream of packets, aggregated across individual sessions, with unique source IP address, destination IP address, IP protocol, and destination UDP/TCP port. A flow can represent unidirectional or bidirectional communication.

A flow allows traffic to be summarized for the purposes of security planning. VMware Aria Operations for Networks allows admins to dive into individual traffic sessions for more detailed information.

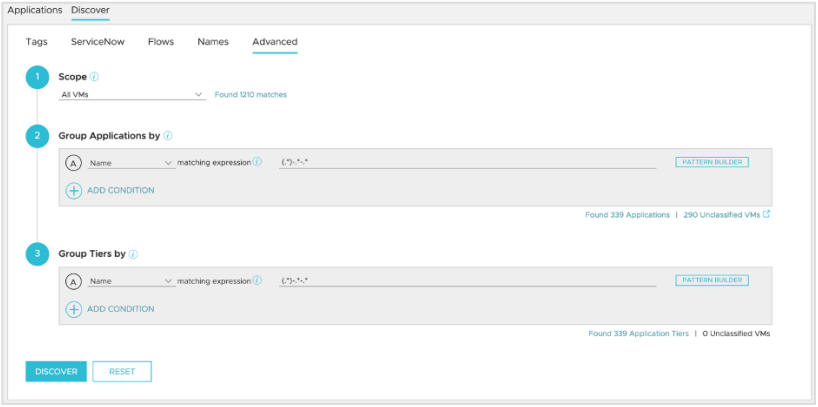


Figure 3: Group applications using metadata

In addition to traffic flows, VMware Aria Operations for Networks has other ways of discovering the relationship between workloads on the network. vCenter tags and custom attributes; AWS tags; workload instance naming conventions; and pre-filled data from a CMDB are other often-used discovery methods. **Figure 3** shows grouping VMs using a regular expression.

Discovered application sets can be saved. This saves the grouping criteria like the regular expression, the definition and grouping of application tiers, and more. A saved application, like the one shown in **Figure 4**, allows admins to interact with all application components as a whole, show traffic flows between tiers, and see all networking components involved in traffic flows between application components.

Saved Applications can be viewed using the Application Dashboard, a per-application topology view with all of its VMs and networking devices. This scoping down helps admins to troubleshoot their environments, as it automatically limits where they should look to identify issues.

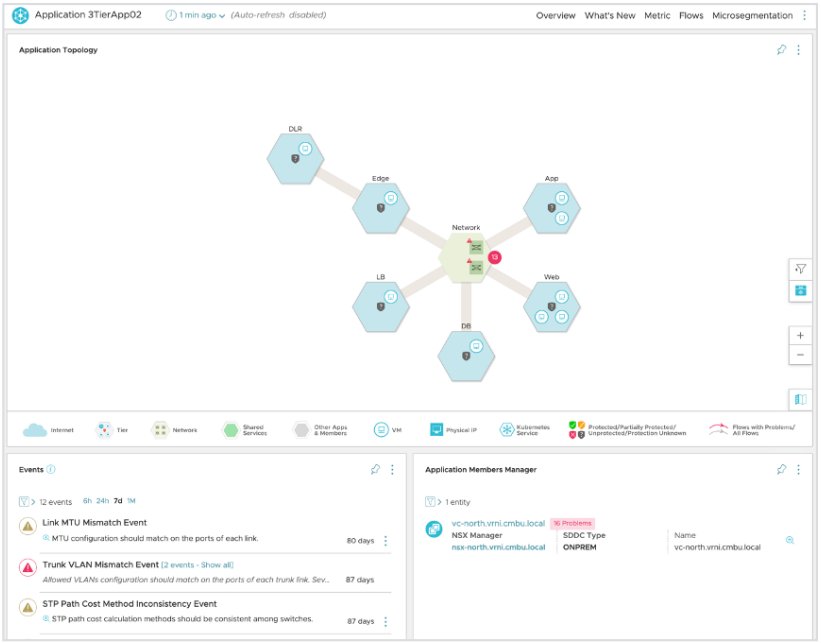


Figure 4: An illustration of an application's topology

While this is a relatively new addition to VMware Aria Operations for Networks, it is one of the most helpful ways of structuring the networking data into a more logical, higher-level view of what's going on over the network, allowing networking flow and configuration data to be contextualized in more human-readable formats.

In an application topology, admins can dive into physical network devices and interfaces. **Figure 5** shows two physical switches as part of an application definition. In addition, this network overview allows a more detailed look at the relevant switch ports.

Naturally, the application landscape changes continuously. Running VMware Aria Operations for Networks's application discovery process periodically will detail any changes to the landscape, as well as surface up new applications.

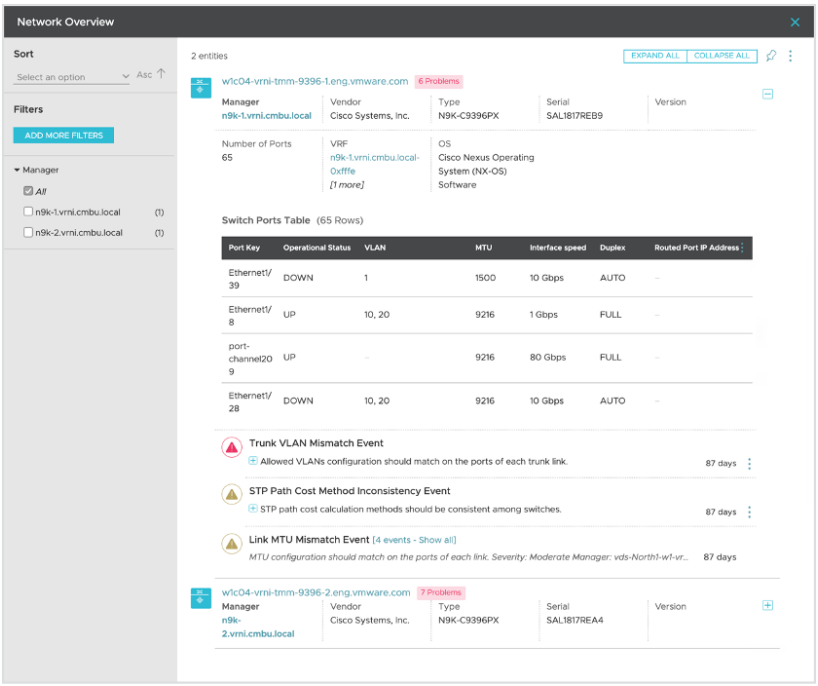


Figure 5: The Network Overview tab

Dependency Mapping

Relationships between different workloads are hard to keep track of. By analyzing traffic flows, however, these dependencies can be made visible automatically, as long as traffic is flowing between them.

The VMware Aria Operations for Networks analytics engine analyzes these traffic flows to understand how components interact. An example of a dependency mapping is shown in **Figure 6**, which shows the relationship between application components based on traffic flow. This helps admins understand the logical relationship between application components.

Different colored lines indicate the direction of flow: outgoing, incoming, or bidirectional. Each of the slices in this "donut" can be clicked

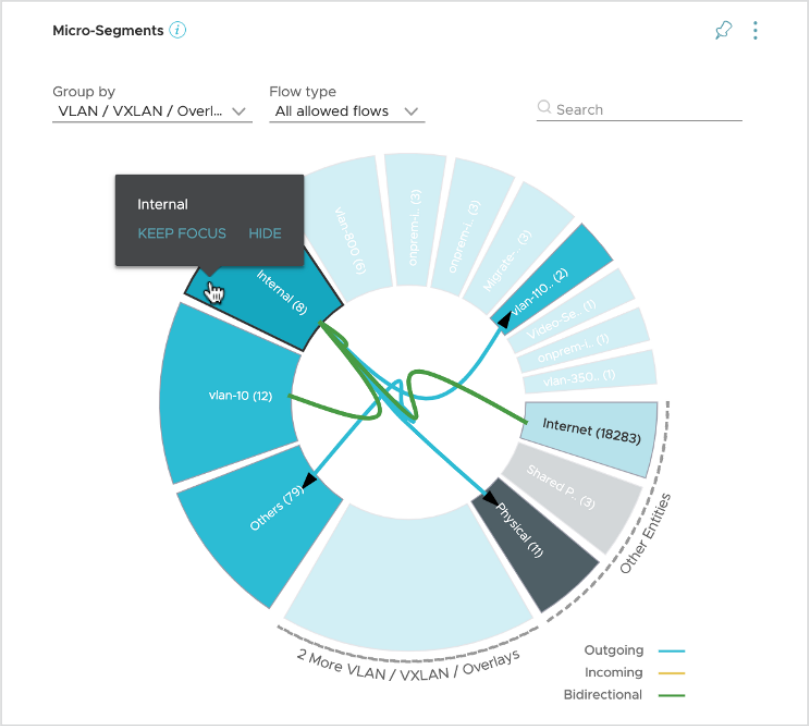


Figure 6: Dependency Mapping

on to view dependencies between them, and each line (traffic) can be clicked on to show more details about the traffic flowing between the slices.

Plan for Micro-Segmentation

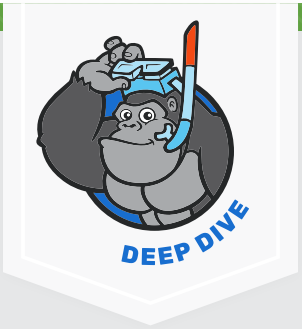
Even with visibility into applications and mutual dependencies, it's not easy to plan for micro- segmentation, which is often the main use case customers start out with when using VMware Aria Operations for Networks.

Because of the high level of cardinality of security rules in a micro-segmentation environment, defining security rules is a daunting task—it's

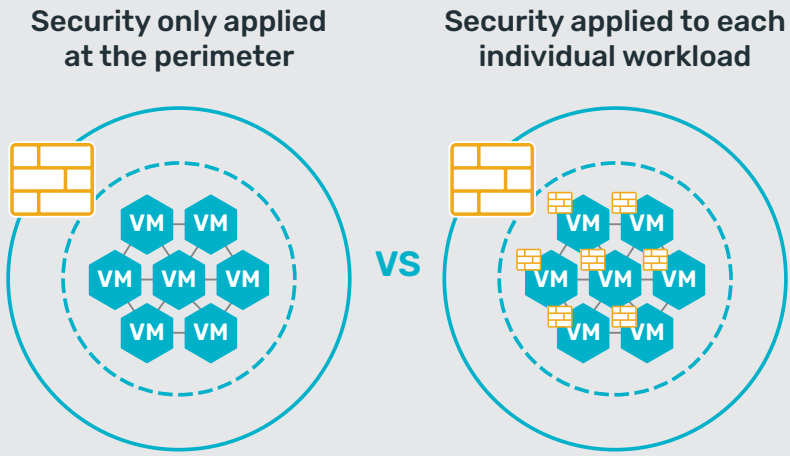
not as easy as just turning micro-segmentation on. The effect of micro-segmentation with no firewall rules would be no traffic flows. This is because micro-segmentation equals zero trust, and zero trust means to deny all traffic unless explicitly allowed.

With this level of granularity, getting started is difficult. Imagine going through troves of documentation to find out the communication paths between application components with the correct protocols and ports, translating the different application components and roles to workloads installed in your environment, and manually creating the required firewall rules. Doing that without making errors would be nearly impossible, and errors like these tend to lead to application downtime.

Zero Trust and Micro-Segmentation



Micro-segmentation is a *zero trust* networking model, where each workload (container, virtual machine, or cloud workload) is protected by granular, per-workload security policies.



Zero trust networking is a relatively new paradigm and inverts the "edge" security paradigm.

In the edge (or DMZ) security paradigm, traffic within the security boundary is inherently trusted. Only traffic going outside this security perimeter (called "north-south traffic") is subject to security policies. Traffic that stays within the perimeter (called "east-west traffic") is not secured by security policies or firewalls. While some form of in-guest firewall is present, centrally managing and applying security policies across different operating systems and virtual and physical appliances proved cumbersome.

In zero trust networking, no traffic is allowed unless specifically and granularly allowed for each workload. The way this works is that a micro-firewall is placed in front of each workload. Each firewall instance protects only that workload, and each workload has one of these firewall instances. This distributed firewall can apply centrally managed security policies to each individual firewall instance, making security granular while keeping centralized management feasible.

VMware Aria Operations for Networks tackles this problem by analyzing the flow data it collects and using that data to generate recommended firewall rules for workloads. It simply looks at the traffic at a granular level, takes all it knows about the underlay network and the workload into account, and translates that information into ready-to-go firewall rules that can be easily imported into NSX.

These rules serve as a good baseline to continue to refine an application's security posture, and can be tweaked or added to as new traffic patterns emerge. Of course, these rules are based on the traffic being observed, which may include undesired flows. Generated rule recommendations need an experienced eye and health check to filter out unwanted observations, like SSH or RDP access.

Technically, data collection works at the distributed virtual switch to capture these east-west data flows using IPFIX, which is forwarded to the local VMware Aria Operations for Networks data collector appliance. For other underlay networks, sFlow and NetFlow can be used as well. Note that NSX is not required for this entire security planning process, which makes it suitable for greenfield NSX deployments as well.

VMware Aria Operations for Networks correlates metadata from flows and configuration to determine which flows belong to which VM or container, and which underlying components are involved in delivering the traffic flow.

The Traffic Distribution overview, shown in **Figure 7**, helps admins understand how traffic distribution is built up. The percentage at the top left shows the amount of east-west traffic, expressed as a percentage of total traffic.

The switched and routed percentages are the amount of east-west traffic that are switched and routed, respectively, adding to 100%.

In the lower row, VM-to-VM traffic and Within Host/AWS VPC indicate percentages of "locality," i.e., how much traffic is VM-based and stays within a host or AWS VPC.

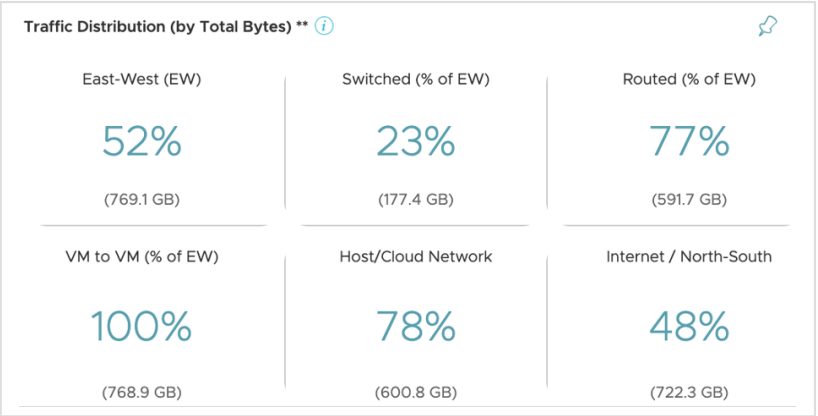


Figure 7: Traffic Distribution overview

Top Ports by Bytes

Port	Count of Flow	Sum of Bytes
527 [stx]	12	200 B
948	2	40 B
378 [dsETOS]	2	40 B
76 [deos]	12	200 B
1013	3	40 B
1262	1	1.9 KB
9415	1	44 B

Figure 8: Top ports by bytes

Finally, the Internet percentage indicates the remainder of traffic that is not east-west but north-south, or internet-facing traffic, as a percentage of all traffic, adding up to 100%, with the first percentage shown.

In similar fashion, the Top Ports by Bytes shows an overview of top ports, as seen in **Figure 8**.

For both the traffic as well as the ports overviews, additional details are available by clicking on a flow percentage or port.

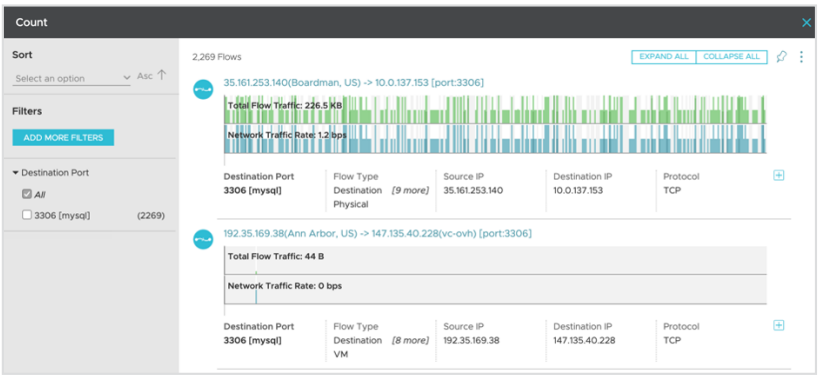


Figure 9: Details for port 3306

Figure 9 shows additional flow details for port 3306. Clicking on any individual flow will show key flow properties (**Figure 10**), like the VM-to-VM path which shows all underlay networking devices and constructs associated with traffic between the two VMs.

Flow Key Metrics offer a timeline view of all flows in a given time period between two specific VMs over a port (**Figure 11**).

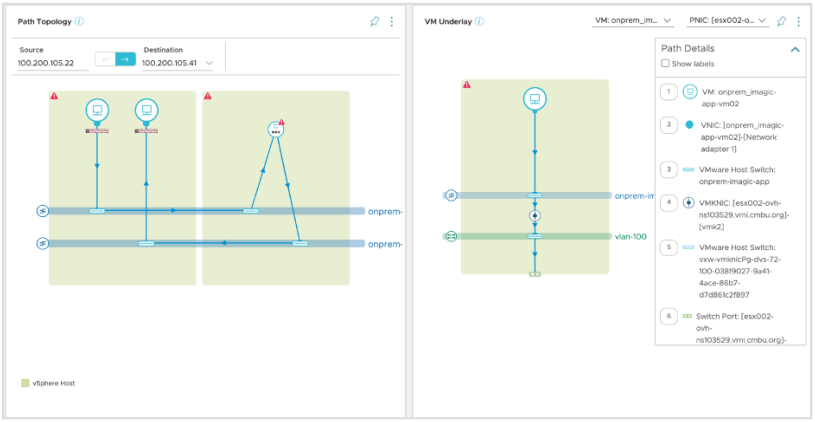


Figure 10: Key flow properties for the port

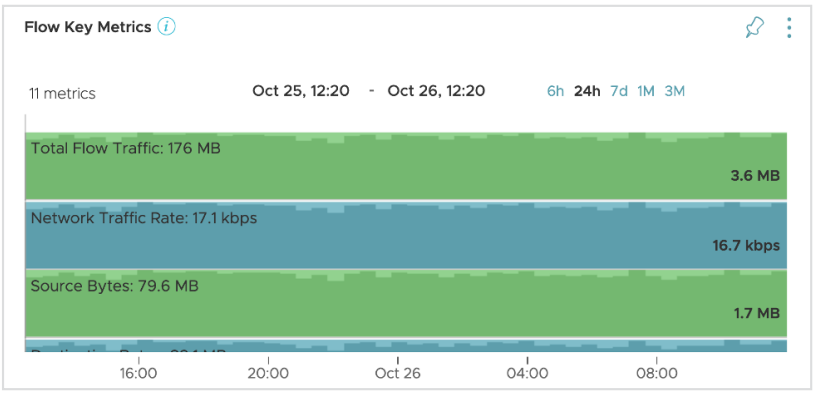


Figure 11: Flow Key Metrics

The Donut Deep Dive

The "donut" in VMware Aria Operations for Networks is way to visualize traffic flows, grouped by a category of your choosing and sliced up per grouping. It allows quick filtering to find the proverbial "needle in the haystack."

The haystack, of course, is the sum of all traffic observed. The needle is the specific flow to be secured using VMware Aria Operations for Networks. Every slice or connection line can be clicked to reveal additional information, diving deeper into the data each time. The donut can be scoped down by parent object (like a vCenter inventory) to limit, for instance, micro-segmentation to a single cluster or data center.

Let's walk through how to use the donut to visualize and isolate specific traffic flows.

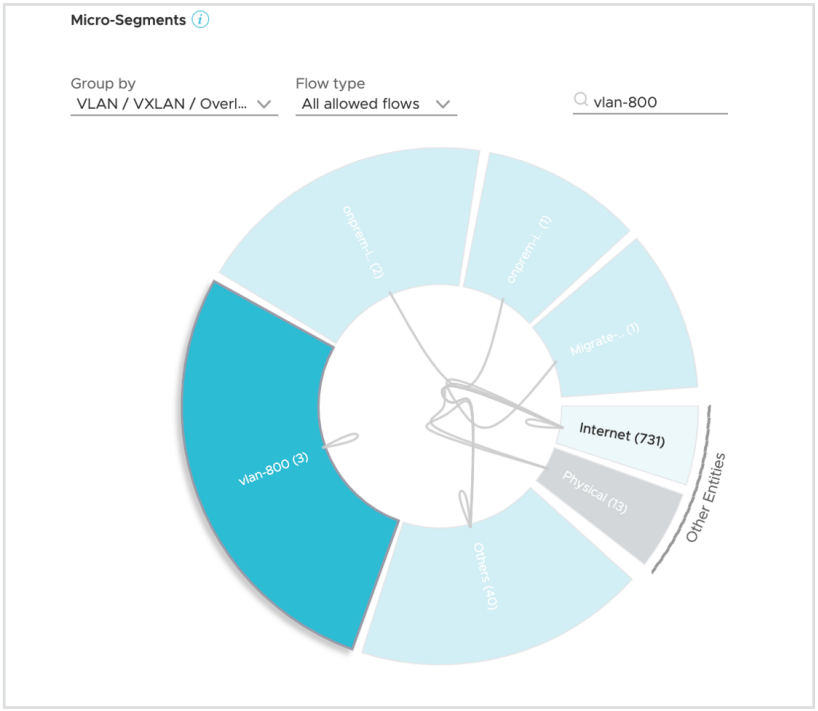


Figure 12: Isolating a specific traffic flow

Start out by grouping traffic in a way that makes sense for what we're trying to isolate. VMware Aria Operations for Networks supports grouping by many different traffic types, like VLAN, VXLAN, subnet, VM metadata (like tag, folder or cluster/VPC), port and more.

In this example, we'll use the overlay chart shown in **Figure 12**. This is a complex visualization, so let's filter on a specific VLAN. This shows only traffic to and from a specific VLAN.

By then filtering a source VLAN, we can visualize all traffic between just these two VLANs and look at the recommended firewall rules for flows between them (**Figure 13**).

By clicking on any of the VLANs in the donut, admins can see an overview of services in this VLAN, services accessed from this VLAN and more

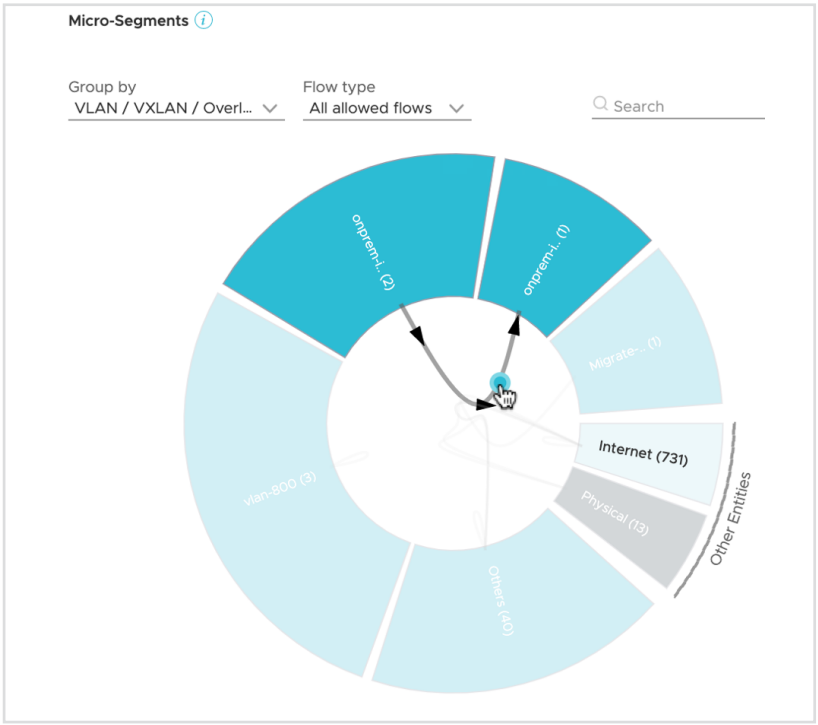


Figure 13: Drilling down on traffic between two VLANs

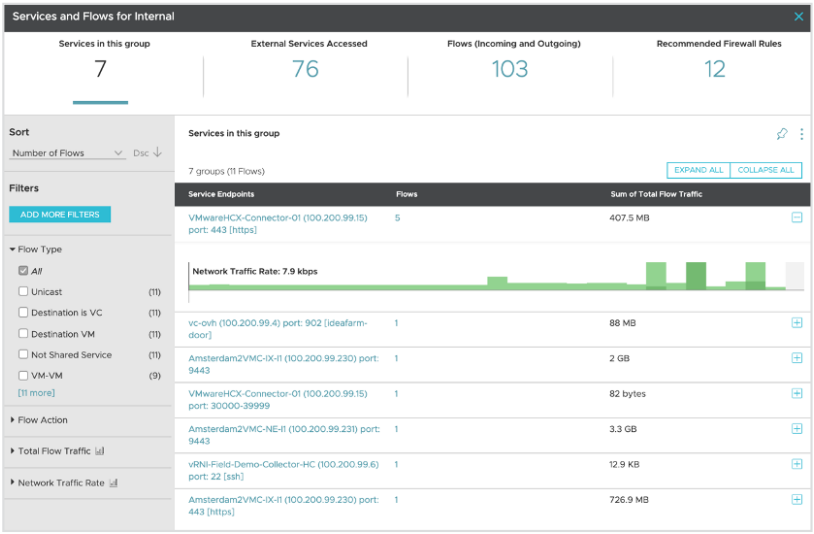


Figure 14: Examining services and flows for a specific VLAN

(**Figure 14**). These overviews provide quick insight into what's running in a specific network slice, along with the other services it is consuming.

Automatically Generated Firewall Rules

NSX's distributed firewall also sends IPFIX flow data to VMware Aria Operations for Networks, which can add metadata (like firewall rules IDs) and show flows that were blocked by a firewall rule (in addition to NSX, Microsoft Azure also logs dropped flows to VMware Aria Operations for Networks).

This allows VMware Aria Operations for Networks to show flows that are not protected by any rule. One thing to note with VMware Aria Operations for Networks is that it does not give certainty about firewall rules in the traffic path between two VMs with other firewall vendors, requiring admins to keep them straight. Use the visibility features of VMware Aria Operations for Networks to see which firewalls are in the path and manually determine which rules may be at play.

Firewall Rule Recommendations

The Recommended Firewall Rules are context sensitive, based on the "group by" selection in the visualization "donut." If you group by VLAN, the rules are on a per-network basis. If you group by VMs, the rules are on a per-VM basis.

VMware Aria Operations for Networks will always try to create the minimum number of rules in a recommendation to create the best manageable configuration, but that does depend on your inputs. Generally, you'll want to segment based on "applications," which balances granularity (too many rules) with specific control over security policies.

NSX isn't the only source that records blocked flows, as Microsoft Azure also logs the flows that get blocked by Azure security policies. Selecting the "Dropped Flows" option causes Azure flows to turn up.

It's important to note that while VMware Aria Operations for Networks can easily export the rule recommendations to NSX, the rules can be used with other micro-segmentation technology as well.

VMware Aria Operations for Networks can export these recommended rules if you've grouped by application, application tier, or security group. Options for export formats include:

- CSV (generic format, human readable, easy to transform, combine and edit)
- YAML (when dealing with Kubernetes, and only available when grouping by Kubernetes Namespace or Service)
- XML (for NSX deployments)

With all of this said, there are some best practices to properly do micro-segmentation that are hard to codify into VMware Aria Operations for Networks. In Martijn Smit's VMware Aria Operations for Networks Cookbook,[1] he described these best practices, which are summarized here:

- Start by segmenting traffic on the boundary of an application. This secures the application as a whole from the outside, and is akin to perimeter-based DMZ security.
- Scoping VMware Aria Operations for Networks to an application will secure any back-end tiers in a 3-tier application—web front-end, application server, and database in the back-end—so that any external user can only access the front-end, not the back-end. This will also codify application dependencies on external services into an actual firewall rule, explicitly allowing the traffic and making it harder to block by accident.
- Segment and secure traffic within an application based on application tier, which protects different tiers of the applications by allowing only specific types of traffic flows. In VMware Aria Operations for Networks, scope the donut to the specific application you're protecting to get the right firewall rule recommendations.
- Perform micro-segmentation on a VM level. This limits connectivity between VMs in the same tier to allow only the necessary traffic flows. In VMware Aria Operations for Networks, scope by application and group by VM to view the recommended firewall rules.

If you already have NSX integrated, this is a good time to look at unprotected flows. Show only those flows not already protected by NSX, which will filter out any flows already protected by the first two bullet points in the previous list.

[1] https://lostdomain.org/vrealize-network-insight-cookbook/

In Search Of …

The search functionality is fundamental to VMware Aria Operations for Networks. Anything you do in the interface is actually a search command. The search is powered by Elastic Search, and the search language is their Regexp Query language, which is a natural language that's easy to learn and translates well to the technical nature of VMware Aria Operations for Networks.

The search looks through all traffic flow data, as well inventory across vSphere, NSX, VMware Cloud on AWS, native AWS (EC2) and Azure, and events, as well as metrics across time.

Search is a very powerful feature. As VMware Aria Operations for Networks collects networking telemetry and configuration, tracks changes and more, there's a wealth of data available to the admin. By mastering the search language, admins can take full advantage of the VMware Aria Operations for Networks data collection.

To help admins learn the language, VMware has created "search posters," which serve as a quick reference to build more advanced search queries. Even though the search box in the UI has auto-completion, using the reference posters can help admins create those advanced queries, listing property and entity terms, function terms and other items to add to a query.

In short, VMware Aria Operations for Networks has a search term for any and all pieces of data it collects from environments. There are search posters specifically for flows, Kubernetes, NSX-T, NSX-v, and VMs (including AWS). All the posters are contained in a single PDF[2].

Searches and search results are reusable using *pinboards*, which are pages with dashboards based on the searches you saved.

[2] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/datasheet/products/vmw-vrni-search-poster.pdf

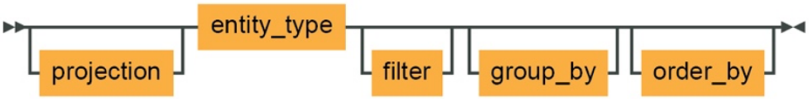


Figure 15: Search query format

Constructing searches can be a little bit daunting, but once you grasp the basic structure of a query (**Figure 15)**, it's a matter of understanding what entities, properties, filters, and groupings are available (using the posters mentioned earlier or the autocomplete in the interface).

For instance, consider the following query:

- sum(bytes) of Flows where Application = 'SavedApp' group by Country

sum(bytes) is the projection, **Flows** is the entity_type, **Application = 'SavedApp'** is the filter, and **Country** is the grouping. The search is logically aware of various constructs; for instance, it understands if an IP address falls into a subnet, if a source IP address resides in a certain country (using GeoIP databases), and more.

There are many entity types, including VM, host, VLAN, flow, application. These are logically sorted into, for instance, VMware Cloud on AWS (VMC), AWS and Azure. Some of these types collate multiple specific types into a single category, called a meta entity. For instance: Azure, VMC, vSphere and AWS VMs are all VMs in the search.

Entities and Projections

Entities have properties. For instance, a VM has an IP address. Or a VM runs on a given host. Or the VM has a given amount of RAM. Using the *where* filter, specific properties can be searched for. *Reference traversal* queries allow search queries to reference a specific property, like a host's memory usage, when looking for an unrelated entity, like a VM.

Reference traversal in this example will find all VMs running on a host with high memory usage.

The filter weeds out unwanted results, like packet drops less than 1%, throughput higher than 1 Gbit, and so on. Filters can have operators: *equal to*, *not equal to*, *in*, *more than*, *less than*, *and*, *or*, *like*, and so on. Time is another way to filter results, allowing time ranges, rolling periods (the last 3 days, for instance) or specific time/dates.

Projections in a search query are a way to pull up specific properties of an entity that are not part of the default search result. Using this search capability to pull up specific property for a specific (range of) entities is the quickest way of navigating the VMware Aria Operations for Networks UI. These can be saved to pinboards and customized to enable powerful fit-for-purpose customization of the UI.

In addition, VMware Aria Operations for Networks has a couple of specific operators that further enhance the search. Most notably are *count* and *list*, which count or list the results (for instance, the number of flows from a specific VM). To do calculations based on search results, VMware Aria Operations for Networks supports *Max*, *Min*, *Sum,* and *Avg*.

The *series* projection combines metrics from multiple objects into a single line graph, like the throughput of all VMs on a single host. These metrics ca be any metric in VMware Aria Operations for Networks.

Specifying an order in the search query will sort the results by the parameter specified, while grouping bunches together results in a more human-readable, summarized form.

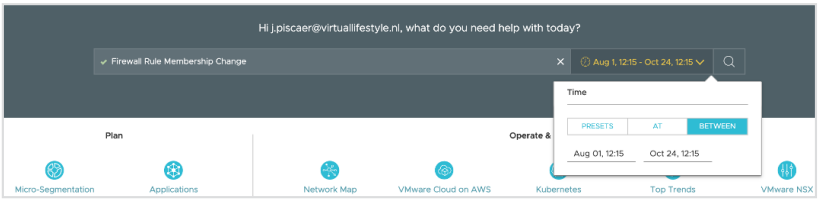


Figure 16: The search results will display all changes made to firewall rule memberships

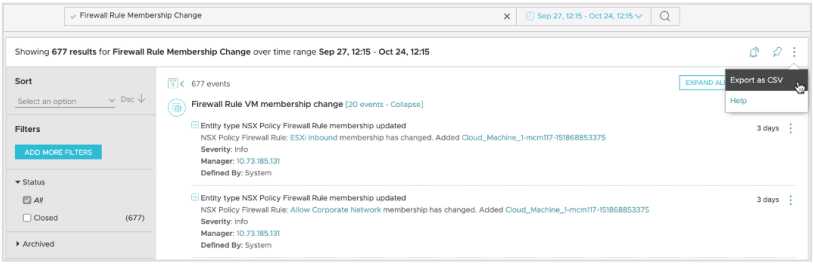


Figure 17: Exporting configuration changes for auditing or other purposes

Audit Trails

The same search functionality can be used to track changes to firewall rules (**Figure 16**). This is very is useful for troubleshooting and auditing.

In addition, the donut can be used to visually confirm the lack of traffic flows between applications, to satisfy regulatory and compliance auditors. Each combination of scope and grouping can be saved into a report to include in an audit, as shown in **Figure 17**.

User-Defined Events

In addition to built-in alerts, admins can create alerts for changes to any entity in VMware Aria Operations for Networks. These user-defined events can be triggered when the search results, like a change in search results. The event will then send an email to the pre-defined email addresses.

Next Up

Now that you've used VMware Aria Operations for Networks for application visibility and security planning, we'll look into using it for cloud migrations.

CHAPTER 3

Cloud Migration

IN THIS CHAPTER:

- Increase agility, speed of delivery, and scalability by moving to the cloud
- Which parts of the application are suitable candidates in terms of security and bandwidth consumption
- Map application dependencies, minimize risks during migrations

Plan for Cloud Migration

When you're going to migrate applications to the cloud, the most important thing to know is which moving parts are involved, and how they'll react to the migration changes. A thorough knowledge of the topology and dependencies of your application is a key factor in successfully migrating an application to the cloud, especially in hybrid cloud scenarios where an application stretches the on-premises data center and a public cloud VPC.

To that end, understanding the application you're about to migrate from a networking perspective is imperative. With VMware Aria Operations for Networks, answering some of the hard questions around application topology and application dependencies is a lot easier.

In the bi-directional complexity of external services (or users) accessing an application, important factors include networking routes/topology,

external resources the application needs to function (and where those run), and the bandwidth requirements of each of these relationships.

While determining which applications, app tiers, or components need to be migrated together, a proper migration scenario necessitates dependencies outside of the group you're migrating. The trick is to minimize those dependencies (in terms of bandwidth and traffic flows).

This chapter won't go into detail about the reasons *why* an application should move. Some of the many reasons could include performance, resilience, availability, cost, security, adjacency to services only offered in the cloud, adjacency to the edge where the application's users are, and more. It could be as simple as the underlying infrastructure reaching its economic and technical end of life.

The advantages of moving applications to the cloud, however, are abundant, even when it's as simple as lifting and shifting applications from on-premises infrastructure to cloud infrastructure.

Lower Operational Risks

By leveraging the visibility into application dependencies and traffic flows between application components, admins can start drafting the boundaries of applications (or application components with larger applications) that need to be migrated together to minimize risk.

Migration risk comes down to a couple of factors:

- Changing topology impacts application
- Changes required during the migration

We'll take a look at both.

Changing Topology Impacts Application

Risks in changing topologies usually comes down to three factors: latency, bandwidth, and security.

When moving only parts of the application to the cloud, latency between components can change. While in many cases this should not constitute a problem, in some cases, latency can in fact cause issues. This is often seen in storage-related traffic flows.

Another consideration when changing the topology of applications by migrating only part of the app is bandwidth. With egress traffic from the cloud being taxed, traffic between application tiers can become expensive.

Using VMware Aria Operations for Networks to mitigate this risk by understanding the flows between tiers can prevent unexpected cloud costs. In addition, migrating only parts of the application can put traffic load onto an ill-sized interconnect between the cloud and an on-premises data center.

More broadly speaking, changing the topology during migrations may trigger certain limitations or bottlenecks that weren't an issue before. Limits and bottlenecks exist in many forms, from blocked ports to limits in the number of VMs, to limits outside of the networking realm.

VMware Aria Operations for Networks

In addition to gaining visibility into the networking aspects of workloads, companies should consider using VMware Aria Operations for Networks to get visibility into compute and storage requirements. Its built-in Migration Planning feature helps you do capacity planning and cost analysis for AWS, VMware Cloud on AWS, Microsoft Azure, and other clouds.

To get visibility into application components, tiers, and the interaction of traffic between them, use the Application constructs to identify bandwidth requirements, and size interconnects and bandwidth allocations (and cloud contracts) appropriately.

Changes During the Migration

Migrations are often done on an application-by-application basis. These types of migrations introduce complexities during migration, like the need to stretch layer-2 broadcast domains between the on-premises data center and the public cloud VPC.

Stretching VLANs across data centers can have significant impact, and the act of stretching itself, if not done correctly, can introduce network outages, or have an impact on latency, bandwidth, or cost. Stretched VLANs are susceptible to many different kinds of outages, so they require significant hand-holding and monitoring.

VMware Aria Operations for Networks and HCX

HCX Is the Go-To Tool for Migrations

VMware HCX[3] is a migration tool for virtualization workloads, often used to move workloads to VMware Cloud on AWS. When coupled with VMware Aria Operations for Networks, cloud migrations become much easier and highly automated.

HCX takes the insights from VMware Aria Operations for Networks, like application boundaries and dependencies, and groups workloads into migration waves to minimize the impact of cloud migration.

[3] https://cloud.vmware.com/vmware-hcx

The automated integration[4] between VMware Aria Operations for Networks and HCX means transitioning information from VMware Aria Operations for Networks to HCX is no longer an error-prone, manual process. Instead, the automation transfers VMware Aria Operations for Networks application insights into HCX Mobility Groups.

HCX's true power lies in its ability to seamlessly extend existing, on-premises, environments to the public cloud, allowing workloads to move without changing any networking properties like IP addressing.

This is a major advantage for traditional applications that were not designed for dynamic environments, and HCX helps breathe new life into these (often mission-critical) applications. In addition, HCX actively optimizes traffic flows to and from these applications (with features like Promixity Routering) and allows migrations between incompatible versions of vSphere.

Next Up

Once you get VMware Aria Operations for Networks up and running, it's time to make it work for you. That's the topic of Chapter 4.

[4] https://flings.vmware.com/vrealize-network-insight-and-hcx-integration

CHAPTER 4

Day-to-Day Operations

IN THIS CHAPTER:

- Troubleshooting and optimizing performance
- Tackling virtual and physical network bottlenecks
- Managing network configuration and health

VMware Aria Operations for Networks is an analytics platform for networking. That means it's very well suited to do troubleshooting of operational and configuration issues on a day-to-day basis.

Its strength lies in correlating and surfacing data in a way that is meaningful for networking admins. This can be anything from creating path topologies of traffic flow between two VMs and mapping all intermediate networking devices, to analyzing dependencies between applications, to keeping track of configuration changes (to things like firewall rules) to determine the root cause of issues or track compliance.

Troubleshoot and Optimize Performance

VMware Aria Operations for Networks is capable of showing the VM Path Topology with all underlay network constructs that make up the path between two VMs. With the complexity of network virtualization, it can sometimes be hard to figure out what devices, virtual constructs, and configuration are at play between two VMs.

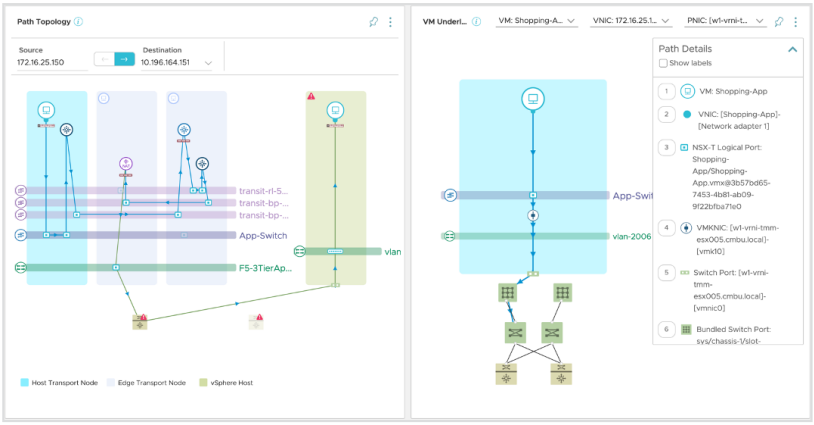


Figure 18: VM Path Topology and VM Underlay

This problem gets exacerbated when applications stretch between an on-premises data center and the public cloud: the number of devices shoots up, and all of them could potentially be the culprit behind an issue.

Figure 18 shows the VM Path on the left. This view displays routers, edges, and logical distributed routers between two VMs, offering a complete routing and NAT view of the network between two VMs.

The right-hand image shows the VM Underlay, displaying all underlay components like switches and switch ports involved in the VM-to-VM path.

Each view can show a detailed, text-based "Path Details" table, shown at the right side in **Figure 18**. This gives admins a 360-degree view of each hop in the physical and virtual network, displaying VMs, physical switches and switchports, virtual switches, routers, and NICs.

Clicking on any component in this topology map will reveal additional details. This view is available for VMs, ESXi hosts, distributed virtual port groups, VLANs, switch ports, logical ports, physical VRFs, NSX-T transport nodes, NSX firewalls, and more.

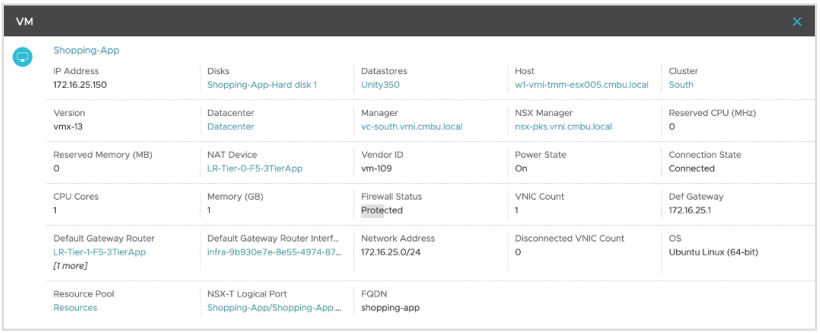


Figure 19: Detailed popup troubleshooting window

Using this path topology overview and the ability to dive into configuration details (**Figure 19**) right from the VMware Aria Operations for Networks interface is very powerful, and allows fine-grained troubleshooting from a single interface, with a wealth of operational telemetry and configuration available to identify the root cause quickly and easily.

VMware Aria Operations for Networks's ability to contextualize information, showing you only what's relevant, is an ability that shouldn't be underestimated. It's extremely useful for identifying faulty traffic flows and troubleshooting configuration issues in the underlay network or distributed logical router bridging issues.

Tackling Virtual and Physical Network Bottlenecks

VMware Aria Operations for Networks can actively track a set of traffic flows and trigger an alert based on outliers, both static and dynamic thresholds and top talkers.

Outlier detection determines statistical deviation from a known nominal state. For instance, when a web server in a load-balanced group of web servers starts acting significantly differently than the others, the outlier detection sends out an alert. For outlier detection to work,

admins must create application tiers or security groups in VMware Aria Operations for Networks containing the group of objects (a minimum of three) to be monitored.

Outlier detection can be scoped to incoming or outgoing traffic, traffic type (east-west, north-south) or a specific network port. A sensitivity setting controls the amount of deviation tolerated before triggering an alert.

Thresholds are straightforward: VMware Aria Operations for Networks sends out an alert if the threshold is breached. Static thresholds are based on a fixed number to be exceeded; dynamic thresholds are determined automatically, based on deviations from past behavior.

Thresholds in VMware Aria Operations for Networks also include minimums (like a traffic slow down), not just maximums. Thresholds can also be scoped to a specific flow (such as a fixed source, destination, and port).

Leveraging Automation

While its search capabilities are a powerful way to automate VMware Aria Operations for Networks and get meaningful insights quickly, the results are only available inside of VMware Aria Operations for Networks. To get customized data in and out of VMware Aria Operations for Networks, the API or PowervRNI[5] (a PowerShell module) is necessary. What these do, in a nutshell, is allow specific searches to be fired at VMware Aria Operations for Networks—the results are returned from outside the application.

Most commonly, tying applications together via the API or scripts is done to transport data from one system to another. In the case of VMware Aria Operations for Networks, the goal could be to automate the automatic, periodic discovery of new applications from a CMDB,

[5] https://powervrni.github.io/

or to complement the data in the CMDB by exporting the contextual information from VMware Aria Operations for Networks to the CMDB.

That can create issues around locating the data's source, which many organizations struggle with. They have to decide where the primary copy of information like application tiers and components are kept, and which systems look at this primary system of record to request that data to use in their own context.

In addition, using VMware Aria Operations for Networks as a data source for Security Information and Event Management (SIEM) or Security Operation Center (SOC) processes is a popular use case for automation.

This replaces the alerting functionality in VMware Aria Operations for Networks, where specific SIEM or SOC software is used to ingest the events from VMware Aria Operations for Networks, and use their native alerting, triggers, or analytics for security purposes.

Manage Network Configuration and Health

The deep insights VMware Aria Operations for Networks produces can be used to optimize applications and reduce the mean-time-to-recovery (MTTR) of outages.

Using data representations like top talkers or high latency connections, admins can actively scour the data in VMware Aria Operations for Networks to look for inconsistencies and possible optimizations to continuously improve network efficiency.

Keeping track of changes in the network is no longer something humans are capable of doing manually in the hybrid world, with applications and networks spanning the on-premises data center and public clouds.

The visibility into operational telemetry and configuration tracking by VMware Aria Operations for Networks helps admins to stay informed

about the network's state and health and be able to quickly identify changes that cause outages. VMware Aria Operations for Networks helps admins surface deviations from a nominal state, alerting about anomalies happening on the network, either by configuration or behavioral change, then suggesting ways to resolve the issue—automatically, where possible.

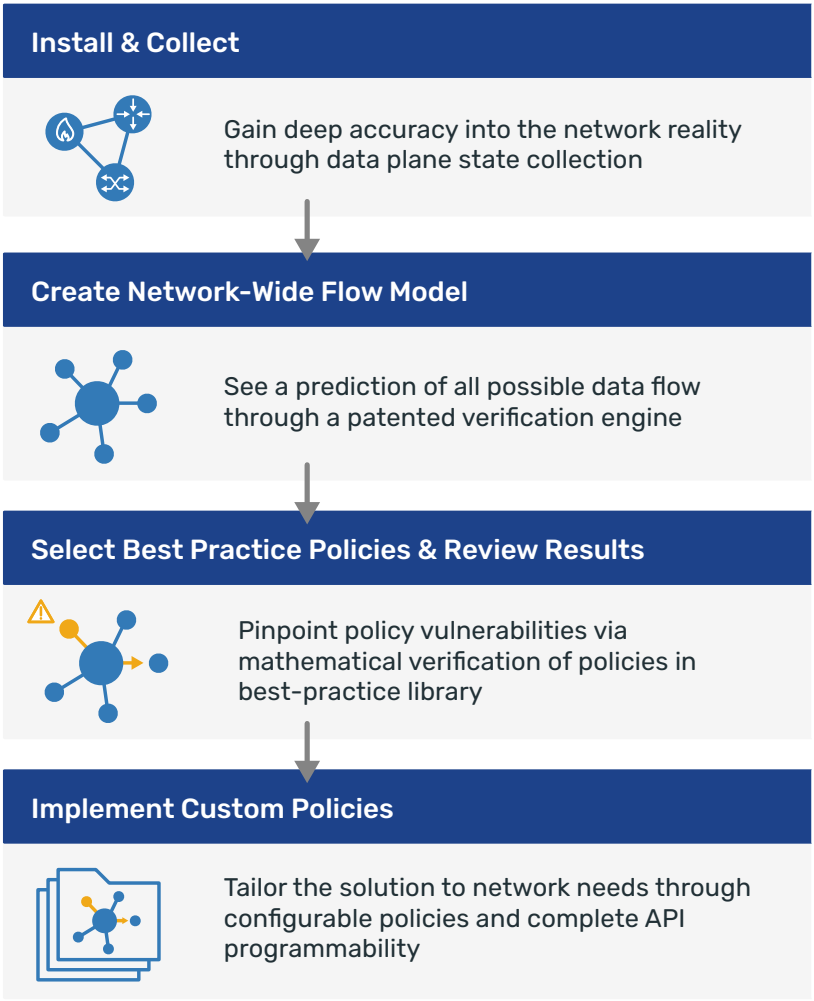


Figure 20: How Assurance and Verification works

Assurance and Verification

As networks have become crucial in the delivery of applications and services, their complexity has increased exponentially. Managing and operating networks is no longer something humans can do—the scale and complexity have grown beyond what our brains can handle with acceptable error margins.

The Assurance and Verification in VMware Aria Operations for Networks helps admins prevent network outages and improve network reliability and network security (**Figure 20**). Its key capability is the data collection from each networking device, and the translating of its state and configuration into a intent-based model that predicts data flow behavior.

This feature works by building a deep understanding of the network. It uses that to model all the ways data can flow, with specific knowledge about each individual device, and how data can flow through that device. It understands how routers, firewalls, load balancers, and more operate across vendors, models, and protocols (**Figure 21**).

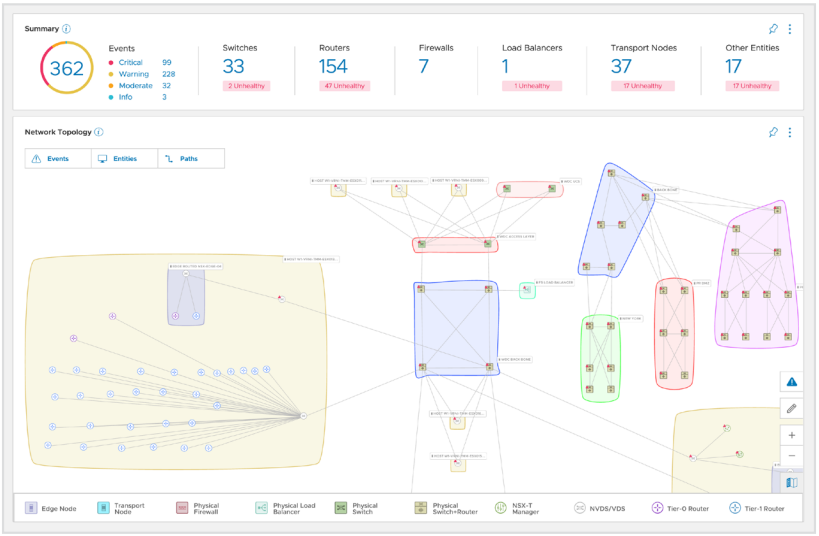


Figure 21: The VMware Aria Operations for Networks network map

Using this deep and specific understanding of a network, it verifies the business intent and policies that match the model. It surfaces security policy violations, vulnerabilities, and configuration errors.

For instance, Assurance and Verification verifies if devices and network intents meet the configurations of the overlay and underlay networks, showing wrongly allowed or blocked paths due to configuration issues.

Managing Security at Scale Is Hard

Operationally, managing security at scale is a huge challenge. There are many moving parts, and with multiple disparate technologies across the on-premises data center and multiple public cloud vendors and environments, keeping track of interaction and topology across the hybrid cloud is an important part of troubleshooting and operations.

Dashboards like the NSX Manager in **Figure 22** help admins with an at-a-glance view of what exactly NSX manages. These include

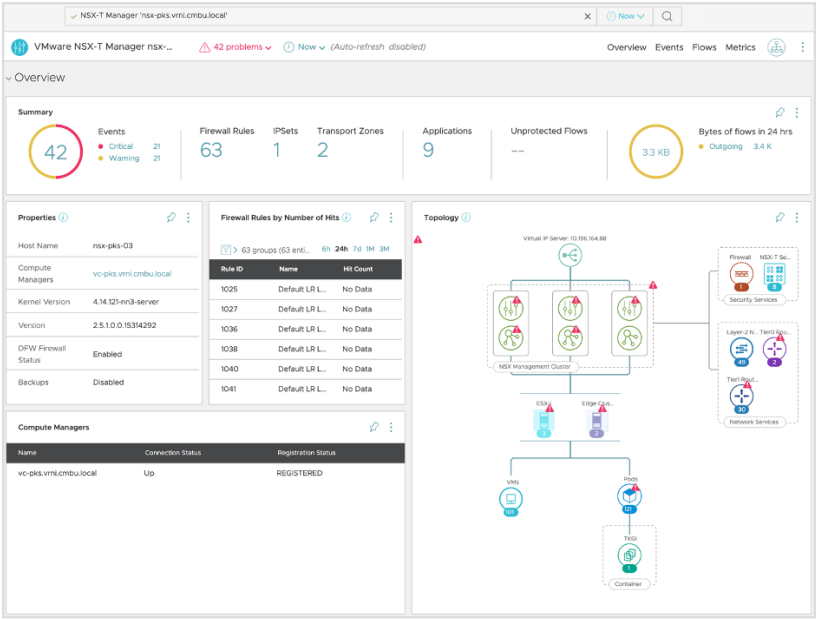


Figure 22: The NSX-T dashboard

the topology of logical NSX objects, including vCenter, clusters and hosts, and NSX Manager and Controllers. VMware Aria Operations for Networks allows admins to dive deeper into object status and other issues.

Part of the power of VMware Aria Operations for Networks is in the extensive visualization of adjacent networking services for NSX objects. VMware Aria Operations for Networks shows detailed topology, device properties, recent events (and changes), and potential issues for all NSX objects, from the Manager and Controllers to individual provider edge services.

Additionally (and too often forgotten), are the checklists of best practices VMware Aria Operations for Networks uses to check the operational state and health of the security infrastructure. These lists are constantly being updated, refreshed, and expanded into additional products and technologies. An example can be seen in the "NSX Checklist Rules" box.

Monitoring Public Clouds

Even in the cloud, VMware Aria Operations for Networks can construct a meaningful picture of the logical network topology. While public cloud providers don't let you see inside their physical networking infrastructure, there are many logical networking constructs, including virtual network ports, subnets, routing tables, virtual private gateways, and peering connections that VMware Aria Operations for Networks can monitor and query to build an inventory. This can be seen in the example in **Figure 23**, which illustrates the path between an on-premises VM and an AWS VPC.

Automatic Audits

No one wants to see the auditor at their door, whether it's the IRS or a compliance officer for your largest vendor. But VMware Aria Operations for Networks can audit changes to security and networking automatically, alerting/triggering admins on specific user-defined events.

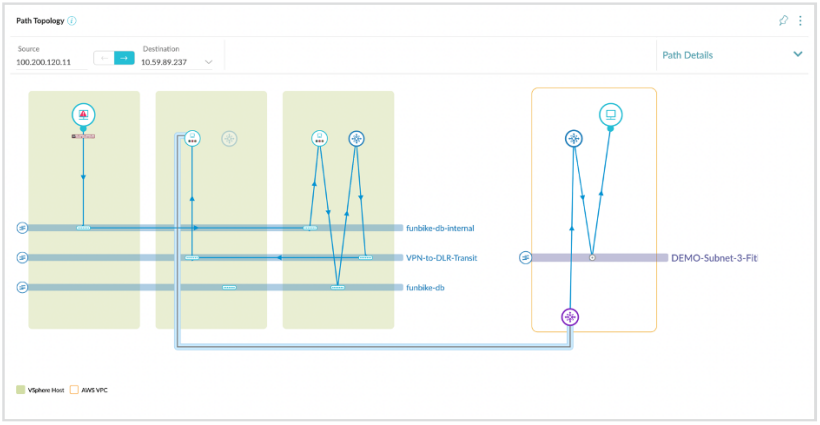


Figure 23: Path topology between two VMs in a hybrid cloud configuration

It's also platform agnostic, so it doesn't matter if the networking components are part of the on-premises vSphere/NSX data center, an AWS VPC or VMware Cloud on AWS—VMware Aria Operations for Networks can monitor changes to these components and send alerts to IT staff.

For the most part, the underlying networking constructs for routing and switching aren't the most important factors to monitor. Instead, it makes more sense to monitor changes to security policies, as those are more likely to have a material impact if things go wrong.

VMware Aria Operations for Networks pulls in security policies from on-premises vSphere/NSX, VMware Cloud on AWS and native AWS EC2 (Network ACLs, DMZ-like border security and Security Groups—think micro-segmentation) to create a timeline, and tracks changes to all of these from a single page.

This unified view of security policies across separate technologies is very helpful for security admins to keep track of the security posture and move multi-cloud management from the unconscious realm to the conscious.

Managing Cloud Security

One of the issues with cloud is that it's so easy to start using it without involving the IT department. In many cases, this leads to an unintentional multi-cloud environment in which multiple business units have started using cloud infrastructure without involving IT.

And even when IT is involved, differing requirements will push different business units to different clouds, as each public cloud has begun to specialize in different areas like ML. The chances of your organization actively using different public clouds in addition to the on-premises data center are approaching 100%.

In other words, it's not a question of *if* you're using multiple public clouds, but rather *how conscious* IT teams are of this reality and their exposure in the areas of multi-cloud security and compliance.

From a security perspective, VMware Aria Operations for Networks allows IT to keep track of traffic flows between different on-premises and cloud estates and correlates these flows between them to gain insights into unprotected traffic flows.

Many enterprise IT environments are expanding into the public cloud. And as cloud usage shifts from pre-production sandboxes to running production environments, IT teams need visibility into the security and compliance status, as well as operational networking status.

And with the many disparate environments and configurations across the on-premises data center and public cloud instances, keeping track of changes and status can be a challenge. VMware Aria Operations for Networks is designed to gain insights into traffic flows and security analysis to make the right decisions managing workloads across the on-premises data center and public cloud alike.

VMware Aria Operations for Networks supports Amazon Web Services (AWS), VMware Cloud on AWS, Microsoft Azure, Azure VMware Solution, Google Cloud VMware Engine, and Oracle Cloud VMware Solution. It

also provides visibility into native AWS constructs like VPCs, Security Groups, Tags, and Firewall Rules. VMware Aria Operations for Networks analysis of cloud traffic flows provides security and micro-segmentation insights, allowing you to plan micro-segmentation and understand traffic flows, regardless of where your workloads are running.

VMs on VMware Cloud on AWS are first-class citizens on VMware Aria Operations for Networks. VMs running on VMC are easily found with a simple search query (vm where SDDC Type = VMC), but other VMC objects (and AWS objects) like firewalls are easily found as well.

Kubernetes

Kubernetes is becoming a force to be reckoned with, especially in the cloud. VMware Aria Operations for Networks supports VMware Tanzu and vanilla Kubernetes to gain insights into container workloads. In similar vein to on-premises NSX and AWS, VMware Aria Operations for Networks makes any and all Kubernetes objects and inventory available for search, filtering, and topology maps.

The Kubernetes dashboard provides a quick overview of the deployment status of entities like services, pods, and namespaces.

The dashboard in **Figure 24** shows Kubernetes namespaces, including pod count, services overview, and worker nodes participating in a given namespace. The dashboard also shows top-talking services, as well as service interactions in the namespace.

To map out topologies, VMware Aria Operations for Networks supports VM-to-pod, pod-to-pod, any-to-pod, and pod-to-any. It creates similar path topology and underlay maps for container-based workloads, as well.

The key to understanding how VMware Aria Operations for Networks integrates with Kubernetes is that it treats Namespaces, Pods, and Services like first-class citizens, like VMs, in the VMware Aria Operations for Networks world, giving admins insights into traffic flows, application boundaries, and dependencies.

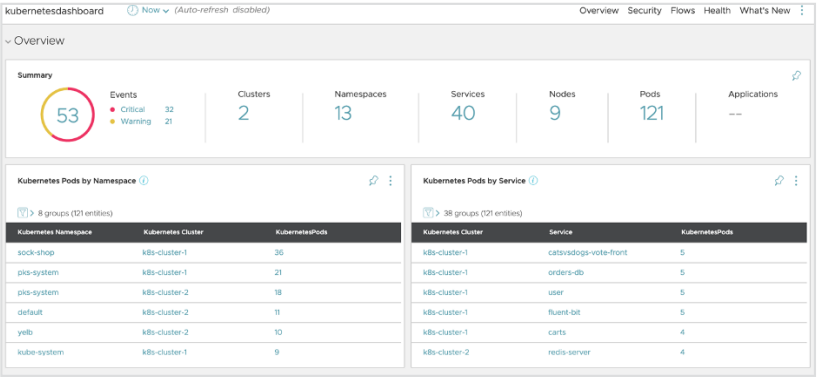


Figure 24: The Kubernetes dashboard

Mission Control for Mission-Critical Network Visibility

Congratulations, you've made it through the jungle! Throughout this Gorilla Guide you've seen the importance of visibility into your network. Cloud migrations; managing hybrid and multi-cloud environments at scale; adding container-based applications to the mix; and the complexity of managing networks across multiple technology vendors are some of the topics you've learned about. All of them make it challenging to first gain, then maintain, insights into your network.

VMware Aria Operations for Networks offers a curated way to get those mission-critical benefits. To start with, its strong application focus helps you keep track of what's important. And the tooling to help you get visibility into application boundaries, dependencies, and traffic flows are indispensable in the security planning phase of micro-segmentation. It's also incredibly valuable when planning cloud migrations.

As you can see, VMware Aria Operations for Networks is an indispensable part of a modern infrastructure. Its insights into multi-vendor networks, providing vendor-agnostic, agentless telemetry to your networks' state and configuration, put your IT team in the role

of *mission control*. That control makes it simple to tackle networking bottlenecks while also pinpointing configuration issues and security vulnerabilities automatically.

It should be clear by now that managing networks without the right tooling is impossible. VMware Aria Operations for Networks is the toolbox you need for network visibility—it's essential for managing complexity across on-premises and hybrid infrastructures that span one or many clouds.

But don't take our word for it—try the trial at https://www.vmware.com/products/aria-operations-for-networks.html#network_insight_form.

ABOUT VMWARE

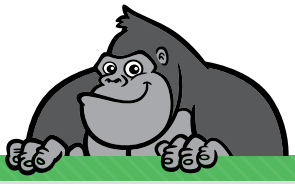
VMware Aria Operations™ for Networks is VMware's solution for end-to-end network visibility, troubleshooting, and predictive analytics. VMware Aria Operations for Networks supports use cases across the Software Defined Data Center, VMware NSX, VMware Cloud on AWS, Azure, AWS, and Kubernetes. VMware Aria Operations for Networks is a tool that can troubleshoot applications down to traffic flows and the network stack. VMware Aria Operations for Networks analytics capabilities minimizes risk during application migrations, optimizes network performance, and confidently manages the scaling of NSX deployments. VMware Aria Operations™ for Networks Universal can be deployed as a SaaS or deployed on-premises with the option to move to SaaS later during the subscription which makes the solution easy to use and operate to run applications better. The VMware Aria Operations™ for Networks Assurance and Verification creates a digital twin and models the network to maximize uptime and validates that business intents are compliant in the network.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/