White Paper: **May 2023**

What's New with NSX in VMware Cloud Foundation 5.0

Table of contents

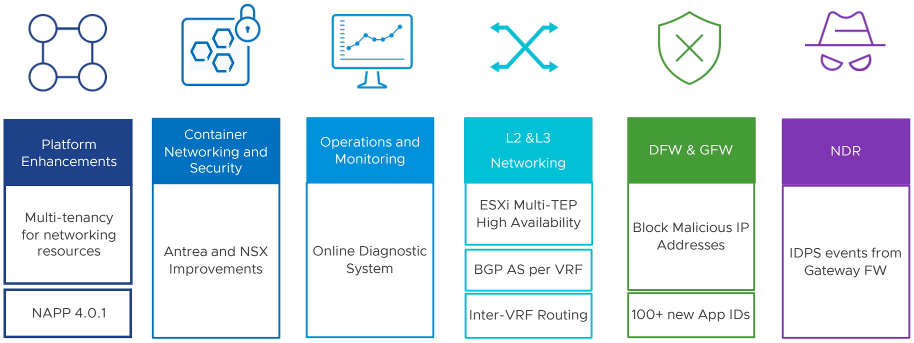
Summary of NSX 4.1.0 Highlights

- VMware Cloud Foundation 5.0 with NSX 4.1.0 support comes with platform enhancements such as multi-tenancy for networking resources and NAPP 4.0.1.1
- Antrea is a Kubernetes-native project that implements the CNI and Kubernetes Network Policy to provide network connectivity and security for pod workloads. NSX 4.1.0 introduces new container networking and security enhancements which allows firewall rules to be created with a mix of VMs and Kubernetes Ingress/egress objects
- Additional Layer 3 networking services are made available to the VMware Cloud Foundation Fabric through the deployment of inter-VRF routing
- Better online diagnostic system that contains debugging steps for troubleshooting specific issues

VMware Cloud Foundation™ is VMware’s comprehensive software-defined infrastructure (SDI) platform for deploying and managing private and hybrid clouds. As part of the newest release of VMware Cloud Foundation, we are announcing the integration of NSX® 4.1.0 and its features that enhance the user and administrator experience.

New enhancements to the network and security fabric in VMware Cloud Foundation 5.0

NSX 4.1.0 adds a variety of new features and enhancements for virtualized networking and security which can be leveraged within a VMware Cloud Foundation 5.0 deployment. Important updates include:



Platform Enhancements	Container Networking and Security	Operations and Monitoring	L2 &L3 Networking	DFW & GFW	NDR
Multi-tenancy for networking resources	Antrea and NSX Improvements	Online Diagnostic System	ESXi Multi-TEP High Availability	Block Malicious IP Addresses	IDPS events from Gateway FW
NAPP 4.0.1			BGP AS per VRF	100+ new App IDs	
			Inter-VRF Routing		

Multi-tenancy support and improvements

Network multi-tenancy refers to the ability of a network infrastructure to support multiple, isolated "tenants," or groups of users or applications that share the same physical network infrastructure but are logically separated and secured from one another.

NSX 4.1 allows enterprise administrators to segment an NSX instance within Cloud Foundation into projects, giving different spaces to project users (tenants) whilst maintaining full visibility and control.

Multi-tenancy can be configured in NSX manager or by using the API and allows multiple NSX users to consume their own objects, see their own alarms and monitor their own VMs with traceflow.

Network multi-tenancy is commonly used in cloud computing environments, where multiple customers or tenants share the same physical infrastructure. It allows cloud service providers to offer a more efficient and cost-effective service by sharing resources between tenants, while still maintaining the security and isolation required to protect customer data and applications.

What is NDR?

NDR or Network Detection and Response is a cybersecurity approach that monitors network traffic to detect and respond to potential threats. It provides real-time visibility, improves threat detection and enables faster incident response to protect the infrastructure from cyberattacks.

How can NDR benefit enterprise security?

1. **Detecting threats** — NDR identifies potential security risk that traditional methods may overlook
2. **Enhancing visibility** — Real-time insights into network traffic, aiding in identifying abnormal of suspicious activities
3. **Enabling faster response** — Allows for prompt detection and response to security incidents, minimizing potential damage
4. **Strengthening security** — By combining threat detection and incident response capabilities, NDR helps enhance the overall security posture of the organization

Container networking and security enhancements

VMware Container Networking with Antrea offers users signed images and binaries, along with full enterprise support for Project Antrea. VMware Container Networking integrates with managed Kubernetes services to further enhance Kubernetes network policies. It also supports Windows and Linux workloads on Kubernetes across multiple clouds.

NSX 4.1.0 introduces new container networking and security enhancements which allow firewall rules to be created with a mix of VMs and Kubernetes Ingress/egress objects. Additionally, dynamic groups can be created based on NSX tags and Kubernetes labels. This improves usability and functionality of using NSX to manage Antrea clusters.

Users can leverage the ability to create firewall policies that allow and/or block traffic between different Virtual Machines and Kubernetes pods in one single rule. A new enforcement point is also introduced to include all endpoints and the correct apply-to is determined based on the source and destination group member targets.

Kubernetes Network Policies and Tiers created in the Antrea cluster can now be viewed in the NSX Policy ruleset. Along with this, NSX 4.1.0 also includes Traceflow and UI improvements which allow for better troubleshooting and management of K8s network policies providing for a true centralized management of K8s network policies via NSX.

Improved online diagnostic system

Online Diagnostics provide predefined runbooks that contain debugging steps to troubleshoot a specific issue. Troubleshooting playbooks or runbooks are a series of steps or procedures that are followed to diagnose and resolve issues in a system or application. They are designed to provide a structured approach to troubleshooting and help ensure that issues are resolved quickly and effectively.

These runbooks can be invoked by API and will trigger debugging steps using the CLI, API and Scripts. Recommended actions will be provided post debugging to fix the issue and the artifacts generated related to the debugging can be downloaded for further analysis. Online Diagnostic System helps to automate debugging and simplifies troubleshooting.

Available runbooks include:

- Overlay Tunnel runbook (ESXi)
- Portblock Runbook (ESXi)
- Controller Connectivity Runbook (ESXi)
- pNIC Performance
- ADF Data Collection

Getting started with VMware Cloud Foundation 5.0

Getting started with VMware Cloud Foundation is simple. For a quick hands-on experience, try the VMware Cloud Foundation Hands-on Lab. When you are ready to purchase, there are four ways to purchase VMware Cloud Foundation: (1) directly from VMware; (2) from VMware channel partners; (3) as part of an integrated system from OEM vendors; and (4) as a subscription service from a public cloud service provider.

Networking fabric improvements

NSX 4.1.0 brings to VMware Cloud Foundation 5.0 a number of enhancements at the L2 and L3 networking level designed to improve on failure times and logical segmentation of different network contexts.

NSX 4.1 introduces a more advanced virtual routing and forwarding (VRF) interconnect and route leaking model. With this feature, users can configure inter-VRF routing using easier workflows and fine-grained controls by dynamically importing and exporting routes between VRFs.

Inter-VRF routing is the process of routing traffic between different VRF instances in a network. Its creation of distinct routing enables communication between different VRFs, which are logically separated network domains. This allows for the creation of multiple, independent routing domains within the same physical network infrastructure, providing network segmentation and enhanced security.

Inter-VRF routing is commonly used in service provider networks and large enterprise networks to provide separate routing domains for different customers, departments, or applications, while still allowing for communication between them as needed.

Implementation notes: SDDC Manager workflows do not include the configuration Tier-0 VRF on Edges. Tier-0 VRF on Edges need to be configured manually.

Security improvements

As network attacks become more and more common, it becomes increasingly important to leverage the newest features in terms of security. By deploying NSX 4.1.0 as part of VMware Cloud Foundation 5.0 new Distributed Firewall capabilities together with new NDR features.

- Block Malicious IPs in the NSX Distributed Firewall is a new capability that allows the ability to block traffic to and from Malicious IPs. This is achieved by ingesting a feed of Malicious IPs provided by VMware Contexa. This feed is automatically updated multiple times a day so that the environment is protected with the latest malicious IPs. For existing environments, the feature will need to be turned on explicitly. For new environments, this feature is enabled by default
- Support for IDPS events from the Gateway Firewall — Starting with NSX 4.1.0, IDPS events from the Gateway/Edge firewall are used by NDR in correlations/intrusion campaigns

Network Detection and Response technology enables the security team to visualize attack chains by condensing massive amounts of network data into a handful of “intrusion campaigns.” Network Detection and Response achieves this visualization by aggregating and correlating security events such as detected intrusions, suspicious objects, and anomalous network flows.

Copyright © 2023 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001
VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents.
Item No: What's New with NSX in VMware Cloud Foundation 5.0 5/23