ReSTNSX v5.0

Release and Configuration Notes

First Published: 9/1/2022, Revised 10/1/2022

This document contains system requirements, supported features and bugs for ReSTNSX v5.0

Important Notes

The ReSTNSX appliance **no longer** ships with a 45 day Evaluation License. Users must email info@restnsx.com to receive a limited, temporary license. In evaluations mode, the following limitations are enforced:

- A limit of two data sources (NSX Managers) can be configured
- Tenants count limited to 2
- No additional users or external auth may be provisioned
- vRNI flows are limited to 15
- ASA import to dFW publish is disabled
- Maximum of 10 workflow items can be published to NSX Manager
- For Operations -> dFW, a limit of 20 rule changes / 4 section changes total is enforced when importing NSX rules from CSV or published to NSX Manager. dFW Mover is limited to 1 Section / 15 rules per instantiation.
- For Operations -> N&S, Mover is limited to 15 objects per instantiation.

In evaluation mode, the default login information is as follows:

Username: admin
Password: default

System Requirements

Support matrix and system requirements for ReSTNSX.
Search:

Role	**Version**	**CPU**	**Mem**
ReSTNSX (Small)	5.x	8 vCPU	16GB
ReSTNSX (Med-Large)	5.x	10 vCPU	32GB
vCenter	6.5, 6.7, 7.0	-	-
NSX Manager (-v)	6.3, 6.4	-	-
NSX Manager (-T)	3.0, 3.1, 3.2		
VMCoAWS	M10-M18		

Role	**Version**	**CPU**	**Mem**
vRNI	3.8+		
vRNI Cloud			
Palo Alto	9.x+		
Cisco ASA	8.x+		
Fortnet	All		
Checkpoint	**R40+**		

Showing 1 to 11 of 11 entries

For REST API access, HTTPS (TCP Port 443) must be allowed through any transient firewalls for the ReSTNSX Appliance to access vCenter and NSX Manager. For NSX-T Central CLI and edge node troubleshooting tools, ReSTNSX requires SSH connectivity to the primary NSX Manager / vCenter hosts.

VMCoAWS is supported for direct connect connections and running as an OVA within the compute cluster within a given SDDC. CGW and MGW rules must be added for HTTP for ReSTNSX to connect to NSX Manager and vCenter.

Browser Support

- Chrome 84+ for the best user experience
- Firefox 52+ (Limited Interop Testing)

New Features

General

- Query: Added Security Tags with the effective members (VMs). (NSX-T).
- Query: VM details added to show Guest information and networking (Segment, Tier 1) details. (NSX-T)
- Work Authorizations: Custom email template support for the Request, Approval and Implementation stages of work authorizations. This feature allows the system admin to define custom emails when notifications are sent
- Work Authorizations: Initiate ReSTFUL API calls to 3rd party systems for Request, Approval and Implementation events

Tools

Policy Engine (formerly Policy Sync)

- A new audit file export where the updates made in the latest Policy Engine run for NSX-v dFW rules, IP Sets, Security Groups and Services are reported. The data includes the object definition before and after the policy was run.
- NSX-v to NSX-T Global Manager dFW Sync added
- NSX-T to NSX-T synchronization when a segment is contained in a rule or applied-to. This feature will query the destination NSX-T

manager for a segment matching by name to be placed in the NS Group.

        - If no matching entry is found:
        - Then If source segment = VLAN, collect VM IPs on source segment
            - Else If source segment = Routed, collect Segment IP Subnet
        - Place IP(s)/Subnet(s) in destination NS Group
- Supported versions for Firewall and Security Group synchronization:

Firewall Rules

Show ▾ entries
Search:

	NSX-v	**NSX-T 3.x**
NSX-v	Y	Y
NSX-T 3.x	Y	Y
AWS	N	Y

Showing 1 to 3 of 3 entries
PreviousNext

Clone (New)

- Users can now clone entire NSX-T Security Configurations to another NSX-T manager. This is in addition to Bulk Provisioning (CSV files); NSX Mover (One object type at a time) and Policy Engine (dFW Sections and objects)

Object Analyzer

- For customers who were required to disable stat collection on ESXi hosts, this feature allows Object Analyzer to collect dFW stats directly from ESXi hosts and thus bypassing NSX.

Firewall Conversion

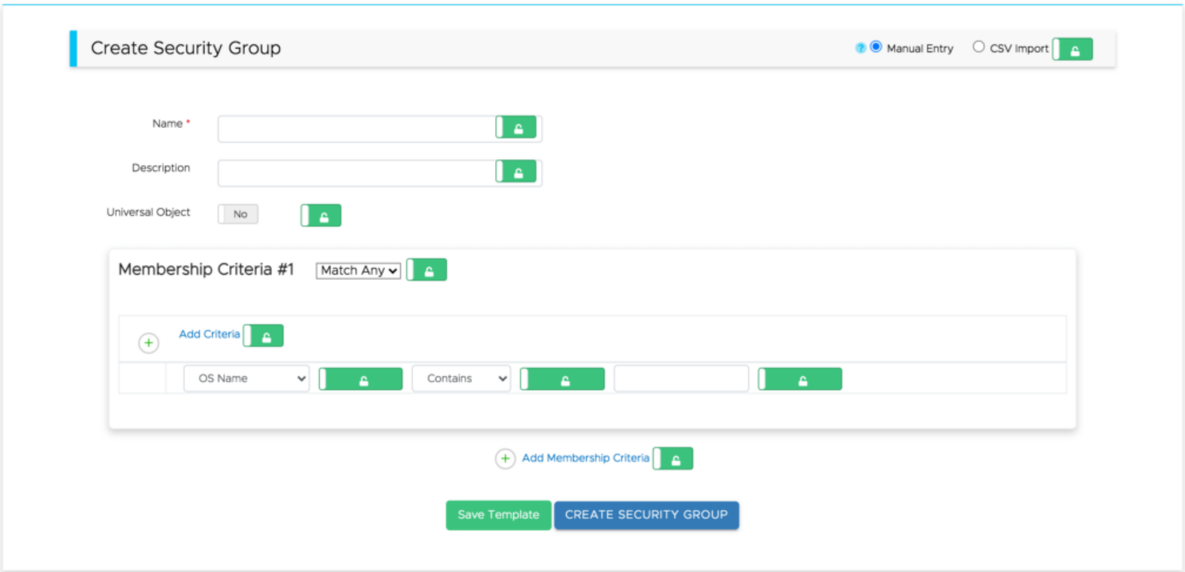
- Added support for Checkpoint firewall rule conversion to NSX-T & VMCoAWS via API GET to Checkpoint Management Server. Note domain name import or NAT rules are currently not supported. Rules can be published to dFW or Tier 1 / CGW.
- Added support for Fortinet firewall rule conversion to NSX-T & VMCoAWS via file import (JSON output of config).

Operations

- Operations > dFW now allows users to preview a rules effective members (source, destination) before publishing to visualize how/if the rule will affect traffic

Workflows

- Custom workflows where an administrator can build a custom workflow with specific permissions. This option allows a workflow creator to define exactly which fields a user can and cannot change. In the example below, an Admin can lock all user fields. Additionally, the drop-downs and text boxes can be set to a specific value that the end user cannot change when they executed the workflow. This feature is available for NSX-v and with 5.x, NSX-T.



Create Security Group

● Manual Entry ○ CSV Import

Name *

Description

Universal Object: No

Membership Criteria #1: Match Any

OS Name | Contains

Reporting

- Difference Reports introduces the capability to compare, on-demand, up to three NSX-T Managers. This feature allows users to compare security configurations and detect variations as slight as differences in object descriptions

Administration

- Data sources can now be enabled to send notifications to 3rd party systems via ReSTFUL API calls. These notifications can be configured on a per user group basis and per object type. For example, when a user modifies a NSX object via ReSTNSX, send an API notification in addition to syslog.
- System report notification maximum email destinations increased to 25 from 3

Multi-Tenant New Features (NSX-T)

- VM page showing more column options to display additional Virtual Machine details (CPU, Memory, Tags, etc...).
- Logging dashboard now limited to user events and system level events filtered out

ReSTNSX - Features Overview

Administration

Enterprise license support. Beginning with ReSTNSX 2.2, customers will have the option of a Standard or Enterprise license. Standard licenses enable all the core features of the platform whereas Enterprise provides advanced functionality such as NSX Mover and Multi-Tenant Administration without requiring separate feature licenses for each capability. To learn more about the different ReSTNSX licensing options, please visit the licensing page.
Note: NSX Mover is available in the current release as a tech preview for non-Enterprise licensed customers. Future releases will require Enterprise licensing to enable this feature

System Features

Query

ReSTNSX provides an easy way to query both NSX and vCenter objects quickly and easily. On every page within the application, users can slide out the Query tab to perform inventory searches. Within that same window, users are able to export the data to CSV, Excel, PDF and the system clipboard for use in ReSTNSX workflows.

Usage Notes:

- VM queries against NSX 6.4 Managers will show the corresponding IP address(es) for any given VM
- With a single click, all searches in query will run and the resulting CSV data will be zipped and downloaded to the user's desktop
- All CSV exports are now ReSTNSX workflow compatible. Users can export data from Query and use them in workflows with little editing of the data

Query Support for NSX-T Objects

- Layer 3 Sections (Policies)
- Logical Switches (Segments)
- NS Groups
- Services
- Tier 0 Routers
- Tier 1 Routers
- Security Tags

Query Support for NSX-v Objects

- Controllers
- Edges
- IP Pools
- IP Sets
- Layer 3 Sections
- Load Balancers
- Logical Switches
- Logical Routers
- Security Groups
- Security Tags
- Services
- Service Groups
- Transport Zones

Query Support for vCenter Objects

- Virtual Machines. Note: VM list is the inventory as reported by NSX Manager
- Clusters
- Hosts

Central CLI (NSX-v, NSX-T)

ReSTNSX's Central CLI provides web-based (HTTPS) API-driven access to the NSX Manager CLI without the need for SSH or leaving the web UI for troubleshooting NSX.

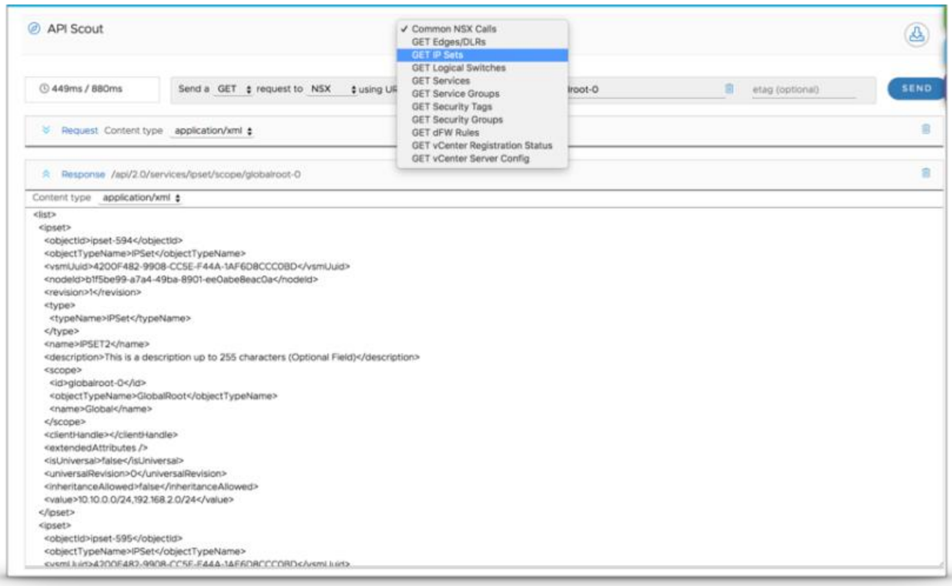
Highlights include:

- Easy buttons allowing users to click an icon to run pre-defined CLI commands such as "show logical-switch list all" without typing one character.
- Enhanced command output with Intelligent Hyperlinks that allows easy buttons to run additional nested commands that are context aware.
- For any CLI command, users can save the commands for future use with a single click.
- Color picker for saving text, hyperlink and background color. These settings are saved per user.

API Scout (NSX-v, NSX-T)

API Scout provides in-application access to the NSX Manager and vCenter APIs without having to use an external client. Based upon the active data source, users can perform GET, PUT, POST functions without the complexity of auth/session cookies or having to leave the UI for API access. Additionally, common API calls for each data source type are provided for easy access.

Personal favorites can also be stored. The URI is stored in the user profile along with personalized, searchable URI history



449ms / 880ms

Send a GET request to NSX using UR… lroot-0

Request Content type application/xml

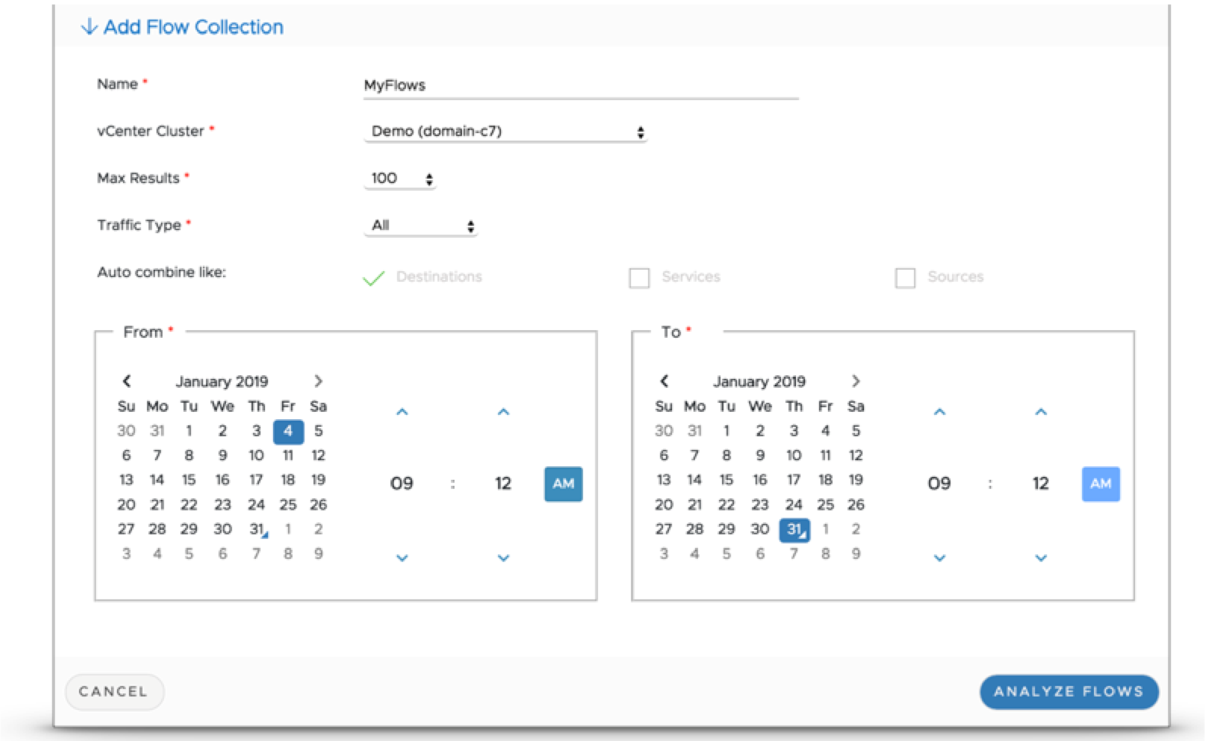
Response /api/2.0/services/ipset/scope/globalroot-0

Content type application/xml

```
<list>
 <ipset>
  <objectId>ipset-594</objectId>
  <objectTypeName>IPSet</objectTypeName>
  <vsmUuid>4200F482-9908-CC5E-F44A-1AF6D8CCC0BD</vsmUuid>
  <nodeId>b1f5be99-a7a4-49ba-8901-ee0abe8eac0a</nodeId>
  <revision>1</revision>
  <type>
   <typeName>IPSet</typeName>
  </type>
  <name>IPSET2</name>
  <description>This is a description up to 255 characters (Optional Field)</description>
  <scope>
   <id>globalroot-0</id>
   <objectTypeName>GlobalRoot</objectTypeName>
   <name>Global</name>
  </scope>
  <clientHandle></clientHandle>
  <extendedAttributes />
  <isUniversal>false</isUniversal>
  <universalRevision>0</universalRevision>
  <inheritanceAllowed>false</inheritanceAllowed>
  <value>10.10.0.0/24,192.168.2.0/24</value>
 </ipset>
 <ipset>
  <objectId>ipset-595</objectId>
  <objectTypeName>IPSet</objectTypeName>
  <vsmUuid>4200F482-9908-CC5E-F44A-1AF6D8CCC0BD</vsmUuid>
```

Security Planner (NSX-v, NSX-T)

ReSTNSX's Security Planner integrates into VMware's vRealize Network Insight (vRNI) platform for easy firewall rule creation in NSX Manager. With this integration, Security Planner will connect to vRNI via API methods to collect IP flow information based upon vCenter cluster and time range (up to 30 days prior to the current date). Upon collecting the data, flows are automatically de-duplicated with additional options for the user to optimize the flows. In the initial release of Security Planner, flows with like IP destinations are automatically combined.



Add Flow Collection

Name * MyFlows

vCenter Cluster * Demo (domain-c7)

Max Results * 100

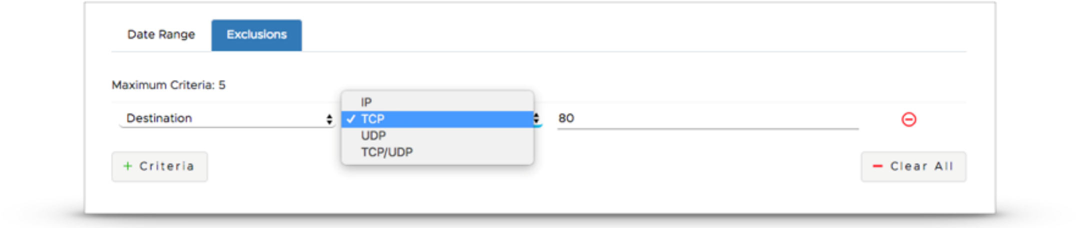
Traffic Type * All

Auto combine like: ✓ Destinations □ Services □ Sources

From * January 2019, 4, 09 : 12 AM

To * January 2019, 31, 09 : 12 AM

Users can publish the same analyzed flows against NSX-v and NSX-T. Additionally, users are able to apply flow filters to exclude specific IP sources, destinations or TCP/UDP ports to narrow the flow collection.

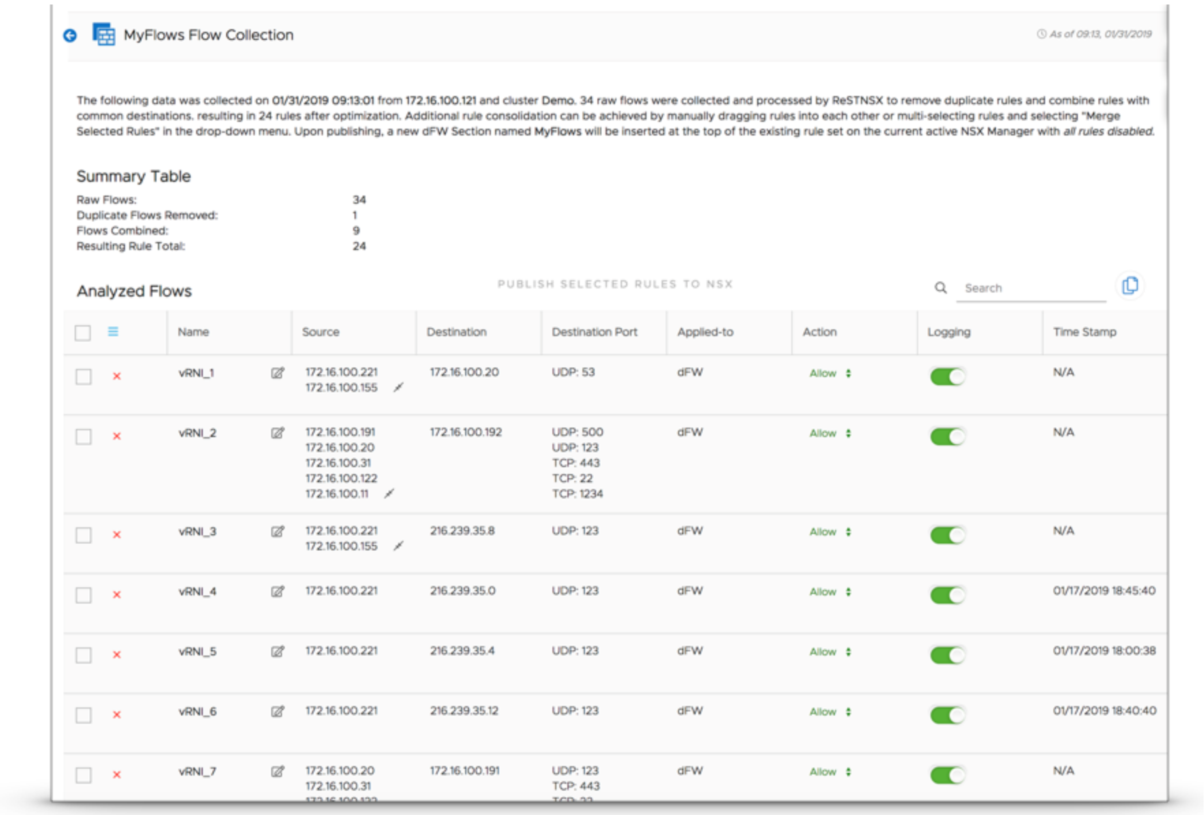


Maximum Criteria: 5

Destination ✓ TCP 80

Once the flows are collected, the processed flows are displayed for further editing:

- Drag/drop rules to combine together
- Multi-select of rules to combine together
- Single or multi-select of rules to transform IP Source and/or destination to IPSets
- When connected to NSX Managers of version 6.4 or greater, users may choose to resolve the raw IPs to VM-IDs to be used in the rule set



MyFlows Flow Collection

As of 09:13, 01/31/2019

The following data was collected on 01/31/2019 09:13:01 from 172.16.100.121 and cluster Demo. 34 raw flows were collected and processed by ReSTNSX to remove duplicate rules and combine rules with common destinations. resulting in 24 rules after optimization. Additional rule consolidation can be achieved by manually dragging rules into each other or multi-selecting rules and selecting "Merge Selected Rules" in the drop-down menu. Upon publishing, a new dFW Section named MyFlows will be inserted at the top of the existing rule set on the current active NSX Manager with *all rules disabled.*

Summary Table

Raw Flows:	34
Duplicate Flows Removed:	1
Flows Combined:	9
Resulting Rule Total:	24

Analyzed Flows

□	≡	Name	Source	Destination	Destination Port	Applied-to	Action	Logging	Time Stamp
□	×	vRNI_1	172.16.100.221 172.16.100.155	172.16.100.20	UDP: 53	dFW	Allow	●	N/A
□	×	vRNI_2	172.16.100.191 172.16.100.20 172.16.100.31 172.16.100.122 172.16.100.11	172.16.100.192	UDP: 500 UDP: 123 TCP: 443 TCP: 22 TCP: 1234	dFW	Allow	●	N/A
□	×	vRNI_3	172.16.100.221 172.16.100.155	216.239.35.8	UDP: 123	dFW	Allow	●	N/A
□	×	vRNI_4	172.16.100.221	216.239.35.0	UDP: 123	dFW	Allow	●	01/17/2019 18:45:40
□	×	vRNI_5	172.16.100.221	216.239.35.4	UDP: 123	dFW	Allow	●	01/17/2019 18:00:38
□	×	vRNI_6	172.16.100.221	216.239.35.12	UDP: 123	dFW	Allow	●	01/17/2019 18:40:40
□	×	vRNI_7	172.16.100.20 172.16.100.31 172.16.100.122	172.16.100.191	UDP: 123 TCP: 443 TCP: 22	dFW	Allow	●	N/A

These rules are now ready to publish to NSX Manager. Select individual or all rules to be published. Upon doing so, a new Section in dFW will be created at the top of the rule set. In this section, all vRNI flows that were selected are present.

Note: Upon publish, all rules in this new section are disabled by default. To enable the rules, click the global select box and "Enable Selected" from the global drop-down menu.

Operations

ReSTNSX Operations provides real-time, instant creation, modification and deletion of NSX objects. In comparison to work-flows with bulk object creation and roll-back, Operations is designed for performing the typical Day 2 tasks and common management functions. Operations is divided up into NSX System for managing the NSX Manager settings and Networking/Security Objects; Networking for logical switching, DLR and ESG management; Security for dFW and eFW; and Load Balancing.

NSX System

Real-time operations for NSX Manager settings

- Network settings, including IP, DNS, NTP and Syslog
- Security modes (FIPS) and Cipher selection
- Service status and status toggle for vPostgres, RabbitMQ, Universal Synch, Management, SSH and Lookup URL
- Backup settings, including FTP server, scheduling and items to be excluded

dFW Management

Real-time operations for dFW

Create, Edit, Delete, Import and Export (via CSV and point-click) dFW rules.

Support for firewall generation and object generation numbers to see if the firewall rule has been successfully published to the hosts and clusters. If they are out of synch, the host or cluster will be marked orange with the user's ability to force a re-synch of the rules and objects.
Support for dFW mover to copy sections, rules and dependent objects between NSX Managers.
dFW Mover copies L3 Rules and Sections from a source NSX manager to one or more NSX Managers. Below are application notes related to behavior between the source and destination sections
Sections and Rules: Matched by Name

If matched, the section on the target manager will be replaced with the same rule names

Else, the new section will be created to the top of the dFW section list

Objects referenced in the rule: Matched by Name

If the source object matches the destination object name, Mover will use the existing destination object.

Supported objects include:
IP Sets
Virtual Machines
Security Groups
Logical Switches
Services
Service Groups
Edge Service Gateways

Else, the user has the option to create the dependant object on the target.

Supported objects include:
IP Sets
Services
Service Groups
Security Groups

Import and Export (via CSV) is another option for copying rules between NSX managers. When exporting rule sets from dFW Operations into a ReSTNSX compatible template, you can use the file for importing into other NSX Managers via two methods

1. dFW Operations. Once a user exports the current rule set from the main menu (Global Actions -> Export Rules (CSV)), the file can be stored for use against other NSX Managers by selecting a new data source and importing by clicking Global Actions -> Import Rules (CSV). The user is then presented an option to Merge or Replace the rules on import.
2. dFW Workflow. Using the same export for Global Actions -> Export Rules (CSV), users can navigate to Predefined Calls -> Security -> dFW and import the ruleset into a workflow for publishing against NSX.

Note: For CSV export, rule names with commas is not supported as it will create conflicts in the comma-based CSV import/export.

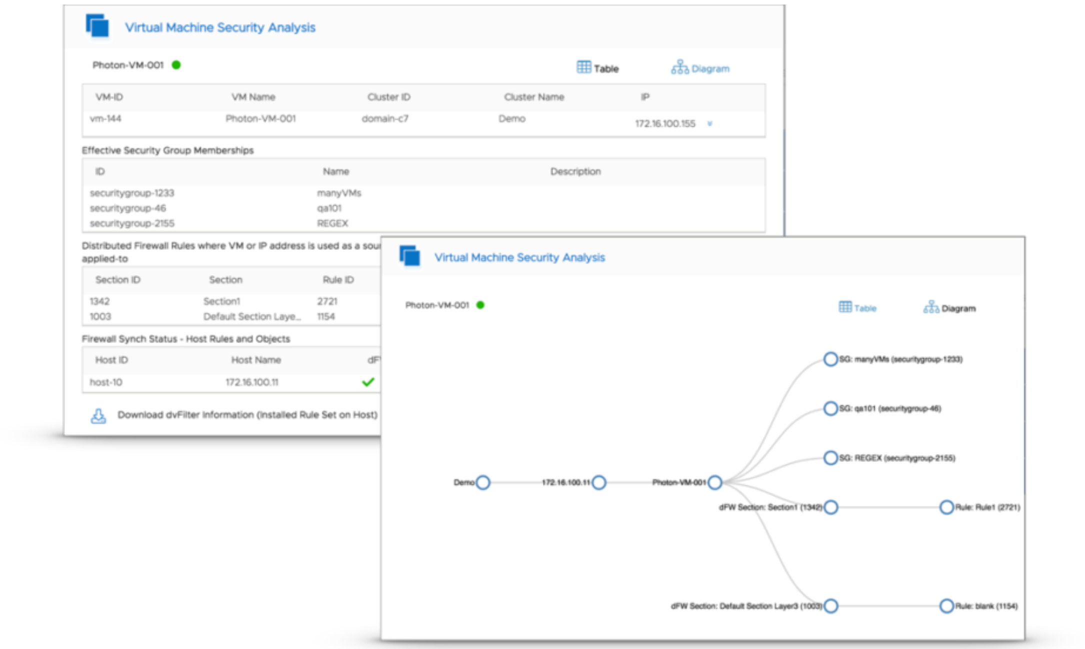
dFW Exclusion Management

VM exclusion lists just got easier with a table-based view to easily add / remove VMs from the dFW exclusion list. With this new feature, users can easily filter based upon VM name and select / multi-select adding or removing from the exclusion list.

VM Troubleshooter / Analyzer

Real-time visibility into VM Security Status

Within dFW, users can now select an individual VM to analyze its security posture - including which Security Groups and dFW Sections / Rules it belongs to; the current status of dFW rules and objects on the host where it resides and the ability to download a copy of the installed dvFilter information. Additionally, a visualization of the same security posture data in a relationship diagram is provided.



Virtual Machine Security Analysis

Photon-VM-001 ●

VM-ID	VM Name	Cluster ID	Cluster Name	IP
vm-144	Photon-VM-001	domain-c7	Demo	172.16.100.155

Effective Security Group Memberships

ID	Name	Description
securitygroup-1233	manyVMs	
securitygroup-46	qa101	
securitygroup-2155	REGEX	

Distributed Firewall Rules where VM or IP address is used as a sou applied-to

Section ID	Section	Rule ID
1342	Section1	2721
1003	Default Section Laye...	1154

Firewall Synch Status - Host Rules and Objects

Host ID	Host Name	dF
host-10	172.16.100.11	✓

Download dvFilter Information (Installed Rule Set on Host)

Virtual Machine Security Analysis

Photon-VM-001 ●

Table
Diagram
Demo
172.16.100.11
Photon-VM-001
SG: manyVMs (securitygroup-1233)
SG: qa101 (securitygroup-46)
SG: REGEX (securitygroup-2155)
dFW Section: Section1 (1342)
Rule: Rule1 (2721)
dFW Section: Default Section Layer3 (1003)
Rule: blank (1154)

Networking and Security Objects - N&S - (NSX-v, NSX-T)

Real-time operations for N&S objects

Create, Edit and Delete N&S objects instantly through ReSTNSX. The following objects are supported in this release:

- IP Sets
- Security Groups
- Security Tags
- Security Tag associations
- Services
- Service Groups
- Context Profiles

Logical Switching

- Create, Edit, Delete - Logical Switches
- Attach / Detach virtual machines
- Create, Edit, Delete - Transport Zones
- Edit Segment IDs

Routing

- Create, Edit, Delete - DLRs
- Create, Edit, Delete - ESG Templates
- Edit Logical Switch associations

Load Balancing

Real-time operations for NSX Load Balancers

Within ReSTNSX, users can now create, edit and operate their NSX load balancers easier than ever before. In a single dashboard, users can monitor critical alerts and manage all edge load balancers of a given NSX domain.

Provisioning

For creating new load balancers, ReSTNSX provides a 5 step create wizard that will build and deploy load balancers quickly and easily. Every step required for a valid configuration is provided.

Operations

ReSTNSX also provides full life-cycle management of NSX load balancers. Within the dashboard, users can: Create, Edit and Delete:

- Virtual Servers
- Application Profiles
- Server Pools
- Application Rules
- Service Monitors

Diagnostics and Troubleshooting

In addition to the dashboard metrics, ReSTNSX provides a load balancer troubleshooting tool that will run a series of diagnostic commands to help isolate problems. The tool performs a series of CLI-based troubleshooting commands and presents the output while highlighting potential configuration issues. The tool can be run on a virtual server by virtual server basis and provide insight into problem areas within seconds.

- Note: In v2.6, Pool side certificates are not supported for Pool-side SSL

NSX Mover

Real-time replication of Networking and Security N&S Objects

With NSX Mover, Administrators can easily copy N&S objects and dFW rules between NSX Managers of the same or different type instantly. Objects are copied in real-time to the destination NSX-v or NSX-T Manager without having to login to the remote system. Copying can be done from source to one or many remote NSX Manager(s). If the data sources (NSX Managers) are configured into Groups, users are able to select the Group and ReSTNSX will copy the objects and/or firewall rules to multiple destinations at once.

Migrate vCenter VM Tags to NSX Security tags. Any VM Tag that exists in vCenter can be migrated to NSX Security Tags and applied to a VM in one easy step. Navigate to Operations -> N&S Objects -> Tags and select "Import VM Tag" from the main menu to select a VM Tag. Note: only VM Tags currently applied to VMs will be imported. Upon importing and conversion of the tag to a security tag, it will automatically be applied to the same VM the vCenter tag was applied to.

Users can select a single or multiple dFW rules and/or sections to copy across Managers.

To access the Mover tool, navigate to the N&S object types of interest in your origin datasource, select a single or multiple object, and navigate to the drop-down menu and select "Copy Selected To..."

Supported objects types are listed below. To learn more about NSX Mover, please see the ReSTNSX Overview page.

Show entries

Search:

Object	NSX -v 6.3	NSX -v 6.4
IP Set	Y	Y
IP Pool	Y	Y
Services	Y	Y
Service Groups *	Y	Y
Security Groups* , **	Y	Y
Security Tags	Y	Y

Showing 1 to 6 of 6 entries
PreviousNext

** NSX Mover's analytics engine determines if dependent objects exist and will prompt the user if they wish to create the dependent objects on the destination system. Examples of objects that could have dependencies include Service Groups and Security Groups where they may be referencing other objects that do not yet exist.*

*** NSX Mover supports Security Groups for migrating dependent objects such as IPSets and Security Tags. Logical Switches and Virtual Machines will be supported in future release.*

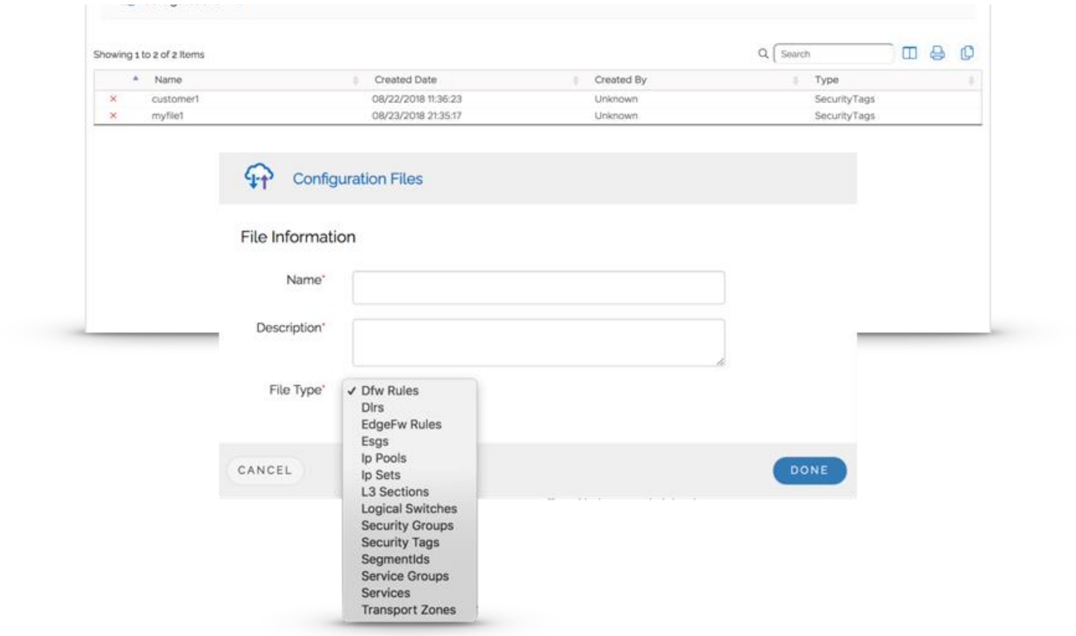
Reporting

Administrators, Auditors and IT Managers now have access to a unified reporting fabric to gain visibility into all of the ReSTNSX managed domains - regardless of NSX version or location. ReSTNSX now provides three report types:
System Reports - Environment summary, service status and configuration details of each NSX Manager under ReSTNSX management are provided by a daily report or on-demand. Difference reports that will highlight the NSX configuration differences between the latest collected inventory and service status with the previous collections. Users may also select custom retention intervals. The default storage policy is to retain the previous 14 days of configurations for comparison. The maximum allowed setting is 180 days.

Activity Reports - Filtered real-time, system log events that can be sorted by username for insight into a user’s action over time.
Tenant Reports - A combination of the System and Activity reports. Data is filtered to provide insight into any given ReSTNSX configured tenant. Similar to the System reports, the Tenant report provides Administrators and Auditors a configuration summary on a tenant-by-tenant basis. Tenant reports reflect real-time information for configuration and user activity.
Read more about ReSTNSX reports ...

Workflows

ReSTNSX now provides a central repository for CSV Configuration Files. In addition to uploading the CSVs directly into a given workflow, users can now also reference the files stored on the ReSTNSX appliance. Users are also able to upload multiple types and versions of files that can be re-used in workflows by multiple users.



Showing 1 to 2 of 2 items

	Name	Created Date	Created By	Type
×	customer1	08/22/2018 11:36:23	Unknown	SecurityTags
×	myfile1	08/23/2018 21:35:17	Unknown	SecurityTags

Configuration Files

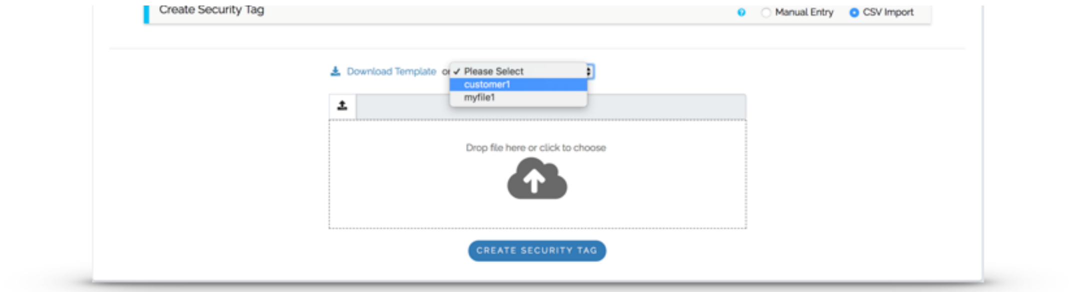
File Information

Name*

Description*

File Type*

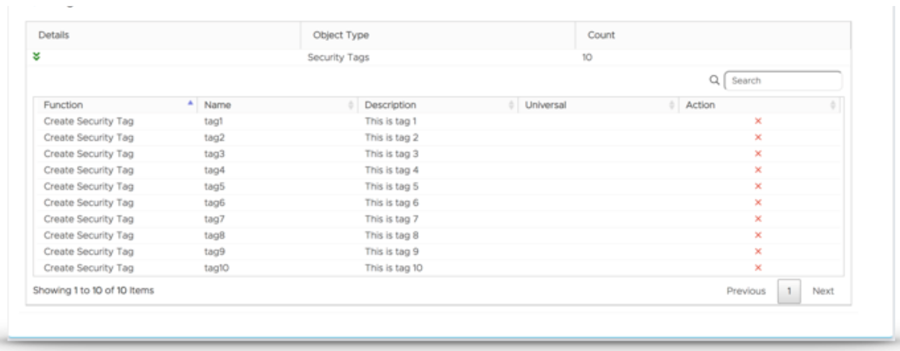
Configuration File Repository - Supporting multiple CSV types



Create Security Tag

○ Manual Entry ● CSV Import

Reference the available files in a workflow



Details	Object Type	Count
✓	Security Tags	10

Function	Name	Description	Universal	Action
Create Security Tag	tag1	This is tag 1		✕
Create Security Tag	tag2	This is tag 2		✕
Create Security Tag	tag3	This is tag 3		✕
Create Security Tag	tag4	This is tag 4		✕
Create Security Tag	tag5	This is tag 5		✕
Create Security Tag	tag6	This is tag 6		✕
Create Security Tag	tag7	This is tag 7		✕
Create Security Tag	tag8	This is tag 8		✕
Create Security Tag	tag9	This is tag 9		✕
Create Security Tag	tag10	This is tag 10		✕

Showing 1 to 10 of 10 Items

Generate the NSX Configuration for Deployment

Upgrading ReSTNSX

Upgrades to ReST NSX leverage configuration export for easy migrations. When exported, the following information is retained:

- Local Users
- Saved Workflows
- Custom Wizards
- Tenant Information
- Data Sources
- System Settings
- CSV Workflow Files
- Central CLI Favorites

By exporting this information, upgrades are performed in parallel to the production platform. Once the new version of ReSTNSX is online, simply import the previously exported configuration file and the system is online. Administrators can manage the same NSX environment(s) with both ReSTNSX versions at the same time and

Note: When both systems are online, configuration settings are not synchronized between the different versions and must be maintained separately until the old version is decommissioned.