

Using vRealize Network Insight

vRealize Network Insight 3.4

VMware vRealize Network Insight 3.4



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1 About vRealize Network Insight User Guide 6

2 Introduction 7

Homepage 8

Navigation 9

3 Search 11

Simple Search 11

Advanced Search 12

Time Control 13

Search Results 14

Filters 14

4 Entity Pages 16

Timeline 16

Property Pins 16

5 Pins 18

Types of Pins 18

Metrics Pins 18

Entity List View Pins 19

Event View List Pins 19

6 Working with Topologies 21

Virtual Machine Topology 21

Path to Internet 22

VM-VM Path 22

VXLAN 23

VLAN 24

L3 Networks 24

NSX Manager 25

Hosts 25

7 Network Address Translation (NAT) 27

NAT Support 27

NAT Flow Support - Examples 27

8 Security Groups 30

9	Micro-Segmentation Planning	32
10	vCenter Tags	36
11	Cross vCenter NSX	37
12	Collaboration Tools	38
	Pinboards	38
13	Settings	40
	Install and Support	41
	Health	41
	Support Tunnel	42
	Online Upgrade of Product	42
	Creating Cluster	42
	Creating Support Bundle	43
	Data Sources	43
	Adding a Data Source	44
	Data Management	45
	Enabling IPFIX Configuration	45
	East-West IPs	47
	North-South IPs	47
	System Events	47
	User-Defined Events	49
	Search-based Notifications	50
	Event Notification Email	51
	Event Notifications	51
	Archiving Problems	51
	Disabling Events	52
	Configuring Event Notification Service	53
	Syslog Configuration	53
	User Management	54
	Add New User	54
	Assign Administrator Role	54
	LDAP	55
	Configuring Mail Server	56
	Simple Network Management Protocol (SNMP)	56
	My Profile	57
	About Page	57
	Customer Experience Improvement Program	58
	Automatic storage expansion for Platform VM	58

14 Help 59

15 Common Data Source Errors 60

About vRealize Network Insight User Guide

1

The *vRealize Network Insight User Guide* provides information about using vRealize Network Insight.

Intended Audience

This information is intended for administrators or specialists responsible for using vRealize Network Insight. The information is written for experienced virtual machine administrators who are familiar with enterprise management applications and datacenter operations.

VMware Technical Publications Glossary










VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.













Introduction

VMware vRealize Network Insight delivers intelligent operations for software-defined networking and security. It helps customers build an optimized, highly-available, and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation planning and deployment, enables visibility across virtual and physical networks, and provides operational views to manage and scale the VMware NSX deployments.

Think of your entire data center as being composed of entities and their relationships. As an example, a virtual machine is an entity, and the virtual machine is part of a Host which is another entity. vRealize Network Insight provides visibility and information on numerous entities that are part of your data center.

Table 2-1.

Entities	Description
	Host
	Problem
	NSX Firewall
	Virtual Machine
	vSphere Distributed Switch
	Physical Switch
	Virtual Port Group
	Cisco Fabric Extender
	Logical Switch

Entities	Description
	Datastore
	Physical Network Interface Card
	Security Group
	Blade
	Router
	VLAN
	Group of VMs
	Configuration Changes
	Router Interface
	Troubleshoot
	Network Access Translation (NAT)
	Mail Server

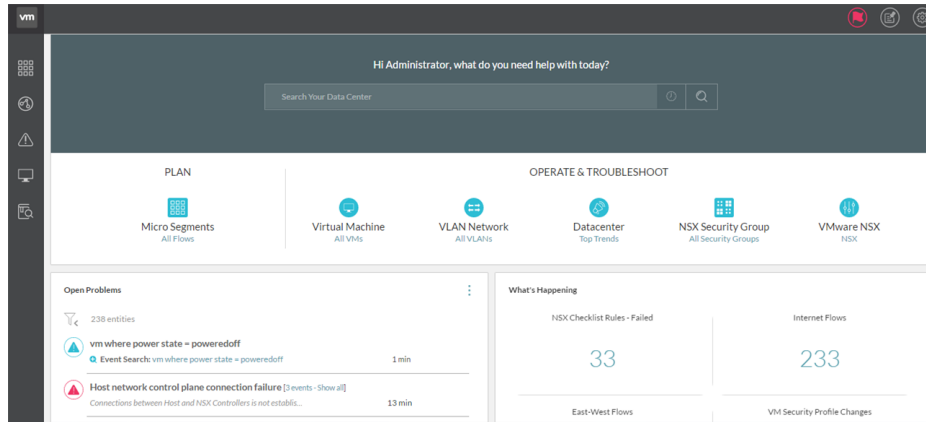
This chapter includes the following topics:


- [Homepage](#)
- [Navigation](#)

Homepage

The VMware vRealize Network Insight homepage provides you a quick summary of what is happening in your entire data center. It provides you a quick access to the important components of vRealize Network Insight of your data center.

The homepage is divided into the following sections:



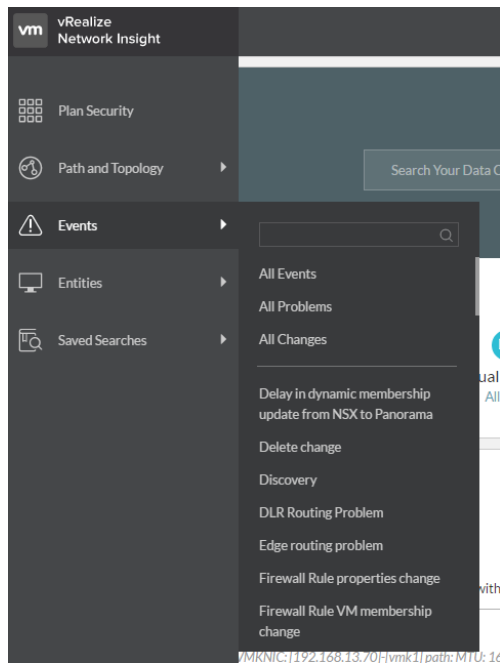
- The Search bar provides you the ability to search across your data center network (and its corresponding entities). You can use the search bar to search for the entities that are available in your data center. The search bar is available at the top of the homepage.
- The **Plan** section enables you to plan the micro-segmentation of the network based on the flows between all the VMs.
- The **Operate and Troubleshoot** section provides visibility, metrics, and analytics for the following components:
 - Virtual Machine (VM)
 - VLAN Network
 - Datacenter
 - NSX Security Group
 - VMware NSX
- The **Open Problems** section provides a quick glance of the critical events that the platform finds in your data center. All such similar events are grouped together. Use **Show All** to view all the events. To view more details of an event, click  (**View Details**).
- The **What's Happening** section provides a quick view of very high-value properties from your data center. To view the property details, click the count of a particular property. This section also contains filters on the left side to filter the events, and expand all and collapse all buttons to view the details of the events.

Navigation

vRealize Network Insight contains a navigation panel on the left that helps users to navigate quickly to the key product features such as Plan Security, Topologies, Entities, Events, and Saved Searches of interest without having to type any search queries.

The Navigation Panel contains the following options:

- **Plan Security:** Allows you to analyze the flows in the environment and helps to plan the micro-segments within the environment. You can select all the entities or select a particular entity and then select the duration to analyze the selected entity.
- **Path and Topology:** Allows you to view any VM to VM path or topology of several entities of the data center.
- **Events:** Allows you to view the events (changes and problems) in your environment. There is also a list of event types so that you can quickly view a specific type of event.
- **Entities:** Displays the list of all the different types of entities present in your environment. You can click any entity type from the given list to view a list of all the entities of that type, the text box above the entities list can be used to narrow down the list based on text entered.
- **Saved Searches:** Displays the searches that have been saved previously.



Search

vRealize Network Insight provides a robust search for all the entities in your environment. When you search for entities, the software displays the entities that match your search query on the **Results** page.

The search-bar uses natural language to search through various aspects of your SDDC. For each search query, the search bar suggests you the next term that you can use to narrow down your search results. For example, when you enter the term **vm**, the search bar displays a possible list of terms that you can add to your existing term to narrow down your search results. The search bar also validates each search query. A check mark denotes a valid search query and a cross mark denotes an invalid search query. The **Help** page provides examples of currently supported queries.

This chapter includes the following topics:

- [Simple Search](#)
- [Advanced Search](#)
- [Time Control](#)
- [Search Results](#)
- [Filters](#)

Simple Search

The features of simple search are as follows:

- Entity Types
 - Example: VM, Host, VLAN, VXLAN, and so on
 - Some pre-defined types can be used to search for multiple related entity types.
 - Example: L2 Network represents VLAN, VXLAN, and Native L2 networks.
 - Auto-complete can be used to explore entity types and other prop
- Event Types
 - Example: MTU Mismatch Event, Membership Change Event, and so on
 - Problems or Changes can be used as keywords to search for all problems or change events

VMs	Show all the VMs
VM 'vm1'	Show VM with name 'vm1'

L2 Networks	Show all L2 networks (VLAN, VXLAN, Native)
Problems	Show all problem events
MTU Mismatch Events	Show all MTU Mismatch Events

- Configuration properties
 - To find entities matching a configuration property value
 - Example: <Name>, <IP Address>, <IP Address 1 - IP Address 2>, and so on
 - Different types of properties: String, Numeric, IP, Range, Reference, and so on
 - Reference is used to represent data center as a graph. So VM has a reference to Host, Cluster and so on
- Metric properties
 - To find all entities with an applicable metric
 - Example: CPU Usage Rate, Network Usage Rate, and so on
- Planning
 - This can be used to plan the security of the data center by analyzing the flows
 - Example: Plan Security Group 'SG_All', Plan Host 'Host-1', and so on
 - "Plan Security" can be used to plan security of the entire data center.
- Path
 - This can be used to show the path between two VMs or the path from VM to Internet
 - VM 'dev1' to VM 'db1'
 - VM 'dev2' to Internet

Note Auto-complete can be used to explore more entity types and properties.

Advanced Search

The features of advanced search are:

- Filtering
 - Search results can be filtered using the properties that they have.

Example:

 - VMs where IP Address = 192.168.0.1
 - VMs where CPU Usage Rate > 90%
 - VMs where host = 'host1'

- Filters can be combined using the following logical operators:

- and
- or
- not

Example:

- VMs where IP Address = 192.168.0.0/16 and Network Rate > 1 Mbps
- VMs where IP Address = CPU Usage Rate > 90% or Network Rate > 1 Mbps

- Projection

- Get properties or metrics.

- IP Address of VMs
- CPU Usage Rate, CPU Count of VMs

- 1 Aggregation (SUM, AVG, MAX, MIN) can be used for numeric properties and metrics.

- AVG(CPU Usage Rate) of VMs

- Sorting

- Results can be sorted using the **order by** clause.

- Order: asc or desc (optional)

Example: VMs order by CPU Usage Rate

- Limit the # of results

Example: top 10 VMs order by CPU Usage Rate

- Group By

- Search results can be grouped by a given property into buckets. By default, groups by results are ordered by count of entities in each bucket.

Example: VMs group by Host

This property returns list of hosts with # of VMs on each host

- Group by results can be sorted by applying aggregation on numeric properties and metrics

Table 3-1.

SUM(Bytes) of Flows group by Port order by SUM(Bytes)	Returns list of ports ordered by sum of total bytes for all the flows on that port
SUM(CPU Count) of VMs group by Host order by SUM(CPU Count)	Returns list of hosts ordered by sum of vCPUs of all VMs on every host

Time Control

Time-control allows you to run a search query within the context of a selected time or time range. You can select from a list of presets such as last 24 hours, last 3 days, and so on. You can also specify a particular date and time using the **At** option or even a range using the **Between** option.

Search Results

The search results page provides a detailed list of concerned entities that match a particular search. The page itself provides numerous information that ranges from the list of entities, their corresponding properties, and facets to filter the search results to refine your search.

You can also expand or collapse each entry in the search results to view more information about a particular entry. You can also create a notification for each search.

Note You can point to a particular property in the search results and also in the entity pages to view a tool tip containing more information about that property.

The following graphic shows the search results for the VXLANs where num vms > 0 search query for a time from the past.

vxlan with filter num vms > 0 at Jul 7, 12:24

12 entities

Name	Number of VMs	Segment ID	Network Address	Default Gateway	Primary Controller
Aundh-LS	5	5003	172.16.64.0/24	172.16.64.1	NSX_Control
BMW-LS 1 Problem	2	5003	172.16.73.0/24	172.16.73.1	Host Control
Honda-Ford-LS 1 Problem	2	5004	172.16.75.0/24	Not Set	Host Control
Transit-LS-1	2	5006	172.16.68.0/24	Not Set	Primary Control
Wagholi-LS	2	5002	172.16.66.0/24	172.16.66.1	NSX_Control

Filters

The left pane consists of a series of filter categories that you can use to narrow down the search results. The number of available filters for each category is mentioned in a small box beside the category. View the available filters for that category (along with a short explanation for each filter) and click to apply that filter. You can also use the filter search box to search for a particular filter and vRealize Network Insight automatically shows the filters that match your search query and you can click to apply that filter. Each filter has several properties to refine the search results. When you select a filter property from one of the filters, then the selected property is highlighted in the search results.

Entity Pages

The entity pages provide a comprehensive outlook of the entities that are present in your data center. This information can range from detailed topologies to show relationships with other entities of your data center to detailed metrics about a particular entity.

Each entity page is a collection of pins and each pin shows specific information related to the entity. The information provided is both real time and historical, and an exhaustive list of metrics and properties for the entity.

If you want to visit the Help content, then click **Help** on the top-right corner of the entity page.

Timeline

The timeline provides you the following information:

- The state of the data center at a particular time in the past
- A bird's eye view of events that were detected across a selected time range

Select the time range of the timeline that you want to view.

To view a particular timeline, select the time range by using the **Time Range** option.

Property Pins

The property pins display important attributes in a two-column layout. Some property pins might also display only a singular attribute value. An example of the property pin is the **VM Properties** pin. The **VM Property** pin displays the properties of a VM, such as operating system, IP address, default gateway, logical switches, CPU, memory, power state, and so on.

This chapter includes the following topics:

- [Timeline](#)
- [Property Pins](#)

Timeline

Property Pins

Property pins display important attributes in a two-column layout.

Pins

The information on each entity page is segregated into pins. All the entity pages are made up of pins and each pin contains a specific bit of information related to the entity.

The pins have the following features:

- You can maximize the view of any pin using the More options () button and also view more information about the pin using the **Help** option.
- Pins can also contain filters so that you can drill down on the data that is displayed on the pin.
- Many pins also contain the Export as CSV option so that you can export the data present in the pin in CSV format. You can select the specific properties and the number of CSV rows you want to export in the dialog that is displayed.

This chapter includes the following topics:

- [Types of Pins](#)

Types of Pins

Most of the pins that are available in the software can be categorized into the following:

Metrics Pins

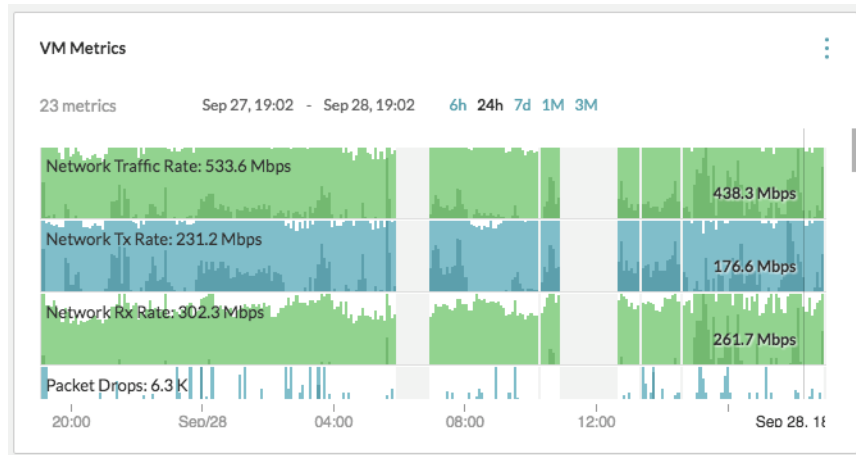
The metrics pins show important metrics pertaining to the selected entity.

The metrics pin uses the cubism graph to display data by dividing each graph into two bands and transposing the higher value one over another. The higher values hence are shown in darker color and are easier to discern.

You can select the particular metric to display from the drop-down present in the pin header and change the selection of entities to display.

The time range can be modified by either using the range presets or entering in a custom date/time.

An example of the Metrics pin is the VM Metrics pin. This pin displays the network traffic rate, network Tx rate, network Rx rate, and packet drops of the virtual machine.



Entity List View Pins

The Entity List View pins display a list of entities that are grouped by a common theme. The list shows important attributes per entity.

You can see more attributes of a particular entity by clicking the magnify icon on the far right. Clicking the entity name takes you to the entity page.

Like other pins, the filter icon houses various facets with which the list can be filtered. An example of the Entity List View pin is the VM Neighbors pin. By default, this pin shows the VMs that are present on the same host. You can also filter VMs by Security Groups, VXLAN, and datastore.

Metrics			
Key Metrics	Neighbor Benchmark	Neighbor Performance	VM Neighbors
Network Usage of Ports in Path to TOR	All Metrics	I/O Metrics	Virtual Disks
Datastore Performance			

VM Neighbors			Host: ddc1-pod2esx...
7 entities			
Prod-Midtier-14 CIDR 10.17.7.14/24	Def Gateway 10.17.7.254	Logical Switches Prod-Midtier	
Lab-Web-19-noip Logical Switches Lab-Web	CPUs 16	Memory (GB) 16	
Prod-DB-5 CIDR 10.17.8.10/24	Def Gateway 10.17.8.254	Logical Switches Prod-DB	

Event View List Pins

The Events List view pins provide a list of events in chronological order for a particular entity or group of entities (that can be selected from the dropdown in the pin header).

You can change how far back in time (from now) should the pin show the events by using the available presets or entering in a custom date/time. Other filter options such as **Event Status** and **Event Type** can be selected by clicking on the filter icon.

In the below image, the events related to VM Prod-db-vm21 and its related entities are displayed. You can click the entity name to view events from other related entities. Using the filter you can filter the events based on their status and their types. An event can be a change or a problem related to an entity.

The screenshot shows the 'Events' section for the entity 'VM: SITED-ESX-01'. At the top, there is a filter icon, a dropdown menu showing '10 events', a date range 'Jan 24, 14:14 - Feb 23, 14:14', and time filters '6h 24h 7d 1M 3M'. Below this, a list of events is displayed, each with an icon, a title, a description, and a time ago indicator.

Icon	Event Type	Description	Time Ago
	Configuration change [5 - Show all]	For Host: 192.168.0.218: VMs has changed. Added 122, deleted 0.	4 days
	Discovery	Virtual Machine: SITED-ESX-01 has been discovered.	4 days
	Delete change	Virtual Machine: SITED-ESX-01 deleted.	8 days
	Configuration change [2 - Show all]	For Virtual Machine: SITED-ESX-01: DVS has changed. Added VDS-Priv-Netw...	8 days

You can search for the events by using the events search query. You can search for open or closed events with queries such as open events or closed events. You can also search for problems with the same modifiers.

Working with Topologies

Topologies are one of the many innovative features that vRealize Network Insight provides. Topologies allow you to view your data center's architecture. You can point your mouse pointer to the entity icons to get their addressable names and click an icon to display a summarized account of their primary attributes.

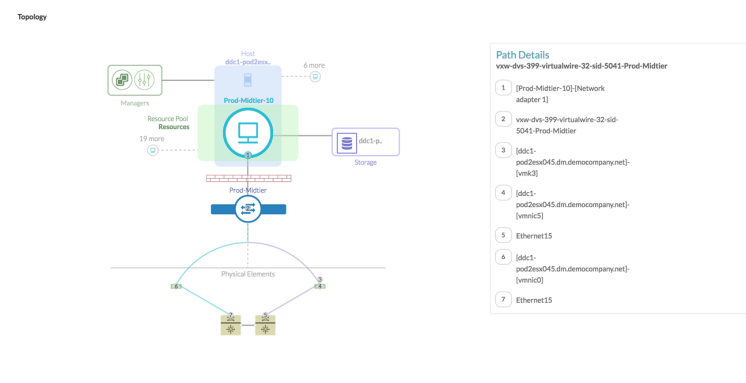
The following topologies can be viewed in respective entity pages:

This chapter includes the following topics:

- [Virtual Machine Topology](#)
- [Path to Internet](#)
- [VM-VM Path](#)
- [VXLAN](#)
- [VLAN](#)
- [L3 Networks](#)
- [NSX Manager](#)
- [Hosts](#)

Virtual Machine Topology

The virtual machine topology provides a comprehensive view of a singular virtual machine in relation to the rest of your data center.

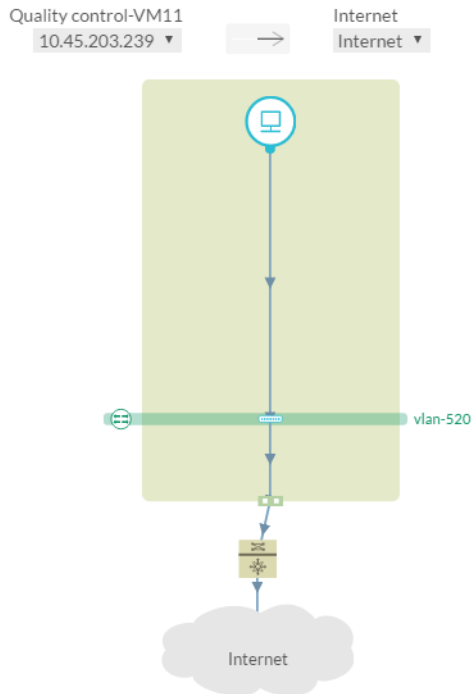


Path to Internet

For each virtual machine that is present in your environment, vRealize Network Insight shows you how the VM is connected to the Internet by using an animated path in the **Path to Internet** pin.

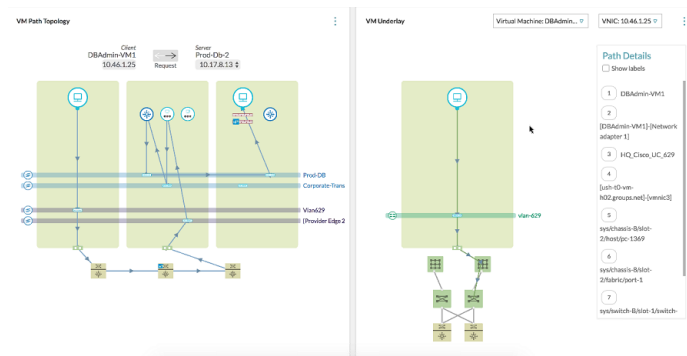
The path populates all the components (both virtual and physical) that exist between the virtual machine and the Internet. It draws an animated path that connects each component in a sequence. The path direction can also be reversed by using the arrows situated above the visualization.

Point your mouse pointer to the entity icons to get their addressable names. Click an icon on the path to display a summarized account of its primary attributes. You can also maximize the pin to see the path details.



VM-VM Path

The VM-VM path topology draws a detailed connection that exists between any two virtual machines in your environment.



The topology involves both Layer 3 and Layer 2 components. This topology can be viewed using the search query `vm_name_1 to vm_name_2`. If a path exists, the VM-VM path visualization proceeds to populate all the components that exist between `vm_name_1` to `vm_name_2` and also draws an animated path. If the routers are physical, then they are shown outside the boundary.

In the VM Path topology, if you hover your mouse on any of the routers, edges, or LDRs that are involved in the path, the complete routing or NAT information is shown.

The VM Underlay section that is on the right side of the VM Path topology shows the underlay information of the VMs involved and their connectivity to the top of the rack switches and the ports involved. In the VM underlay section, the components are labeled if you select **Show labels** under **Path Details**. In this section, the drop-down list at the top shows the endpoint VMs and the active VMs at the edges. For each edge VM, the neighboring drop-down list shows the ingress and the egress interface IP addresses. Based on the selection, the underlay path for that particular interface is shown. .

You can also reverse the path direction using the arrows on top of the topology map.

The topology map gives more visibility regarding the ports involved in the VM-VM path. In the **Path Details** section, the name of the actual port channel is shown.

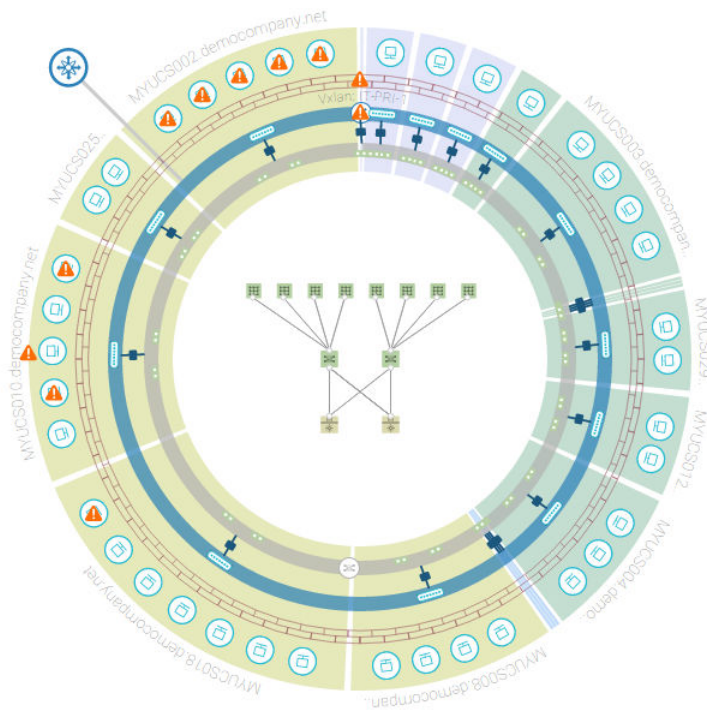
Note

- There is no complete visibility for layer 2 on the physical front. If a packet is traversing from one switch to another, there may be multiple switches involved. But the topology does not show the switches in the underlay network.
-

VXLAN

Virtual eXtensible Local Area Network (VXLAN) overlay networking technology is an industry standard that is developed by VMware jointly with the major networking vendors.

The VXLAN topology is an innovative visualization that gives you an overview of the selected VXLAN. The following diagram elucidates the various components that make up the visualization:



Overview	
VXLAN Network	
Open Problems	4
Configuration Changes	None
Segment ID	5001
Number of VMs	38
Network Address	172.16.151.0/24 172.16.150.0/24
Default Gateway	172.16.150.1
Underlay VLAN ID	218
Underlay Subnet	172.16.69.0/24
Hosts	MYUCS008.dem...

Note Both virtual and physical components can be visualized in this manner.

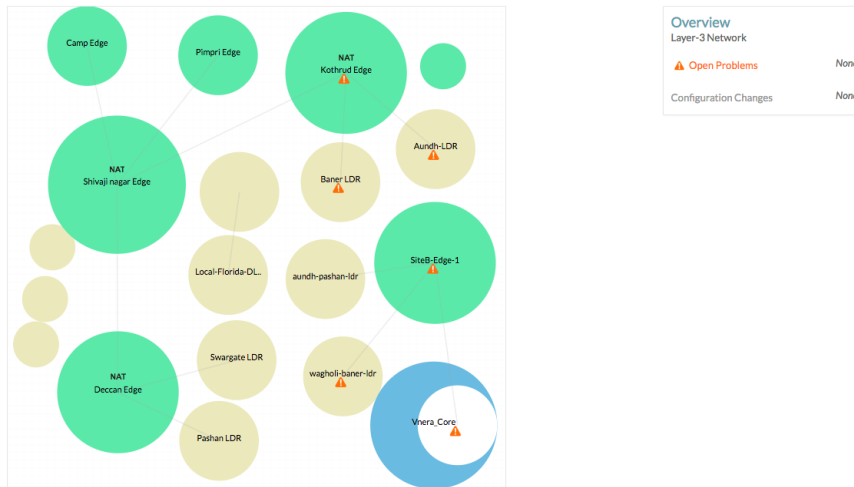
VLAN

Virtual LANs (VLANs) enable a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments.

The VLAN topology is constructed in a similar manner as the VXLAN topology.

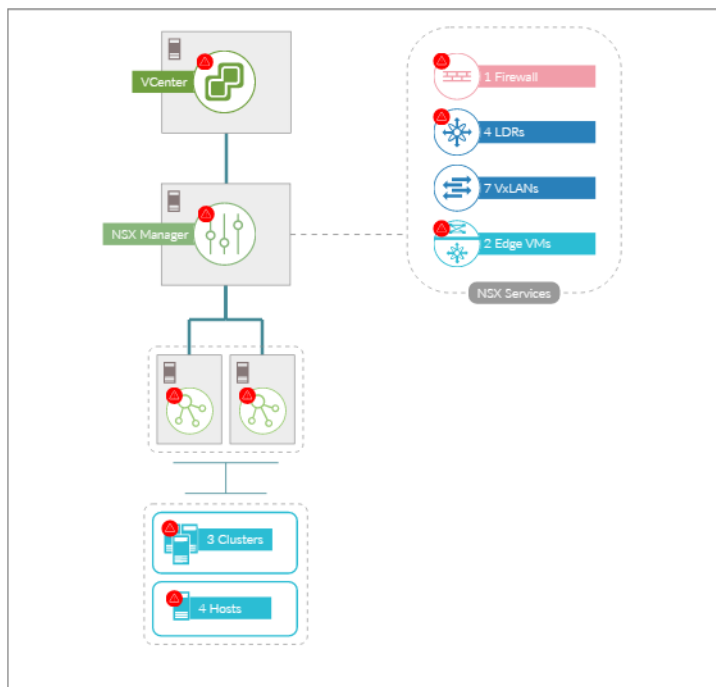
L3 Networks

The L3 Networks topology provides an overview of your entire network. An Edge in the topology which has NAT rules configured is shown with the word NAT.



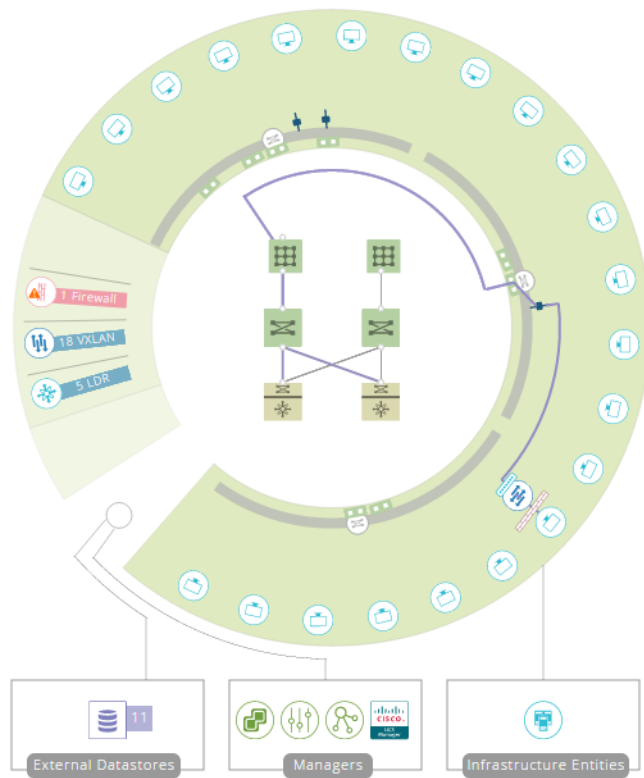
NSX Manager

The NSX Manager topology shows the components that are associated with the NSX Manager.



Hosts

The host topology shows how VMs of a particular host are connected to the virtual and physical components of your data center and also how the host itself is connected with your data center.



Network Address Translation (NAT)

7

vRealize Network Insight lists both SNAT and DNAT rules that are configured on the VMware NSX® Edge. The NAT Rules query lists all the SNAT and DNAT rules.

The VM to VM path also includes and shows the Edge NAT gateways configured in the path. Only the NAT rules configured on the Uplink interface of the VMware NSX® Edge are processed by the VM to VM path. The nested NAT hierarchy is also supported.

This chapter includes the following topics:

- [NAT Support](#)

NAT Support

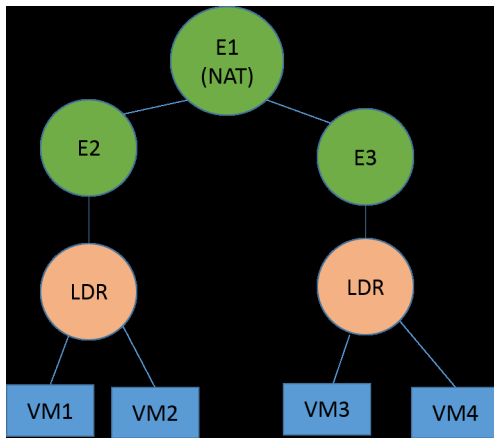
The NAT flow support in vRealize Network Insight is as follows:

- Only NSX-based edges are supported.
- Only edges with defined uplinks are supported.
- Only edges with NAT-defined uplinks are supported.
- The flow of the following NAT domains are reported:
 - Default domain
 - The single child domain of the default NAT domain

NAT Flow Support - Examples

This section consists of few examples for the supported NAT flow in vRealize Network Insight.

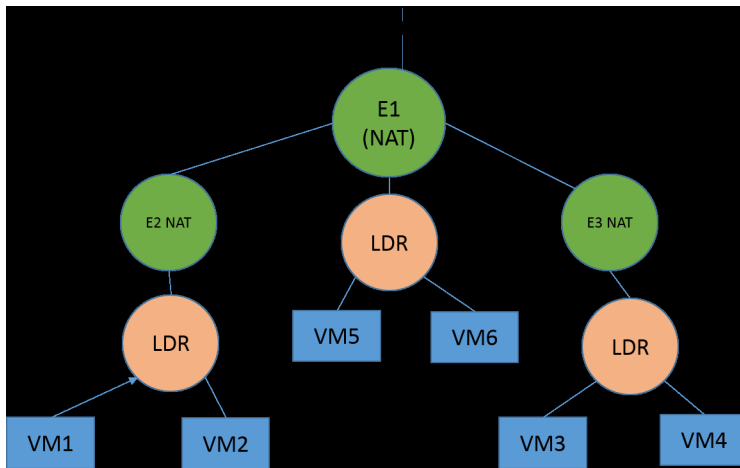
Example 1



In the above topology, E2, E3, LDRs, VMs (VM1, VM2, VM3, VM4) are part of NAT domain E1. Anything above E1 such as uplink of E1 is part of default NAT domain. The above topology consists of the following:

The flow from VM1 to VM2 and vice versa is reported in vRealize Network Insight. Similarly the flow from VM3 to VM4 and vice versa is reported.

Example 2



The above topology consists of the following:

- VM1 and VM2 are part of E2 domain.
- VM3 and VM4 are part of E2 domain.
- E2 and E3 NAT domains are child domains of E1 NAT domain.
- E1 is the single child of default NAT domain.
- VM5 and VM6 are part of E1 NAT domain.

In the above topology, the following flows are reported in vRealize Network Insight:

- Flow from VM5 to VM6

- Flow from (VM1, VM2) to (VM3, VM4)

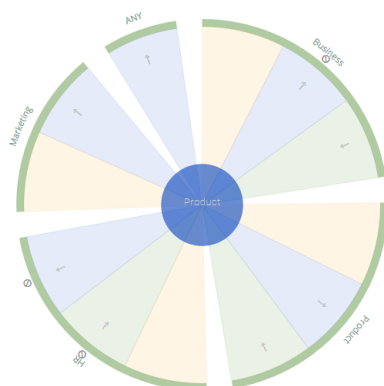
Security Groups

Security Groups are a set of groups that are managed through a common set of permissions.

The Security Group topology has the following two views:

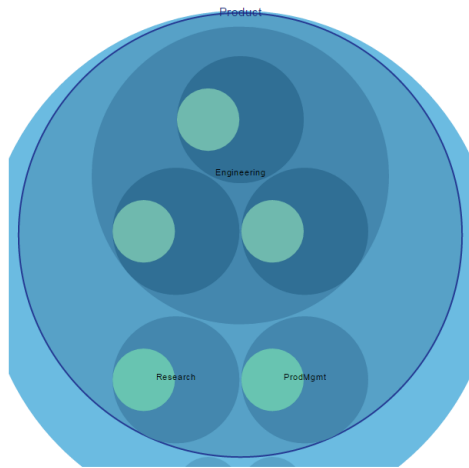
Firewall View

The Security Group firewall topology displays the relation between the selected Security Group and other Security Groups by showcasing the firewall rules that are applicable between the Security Groups.



Container View

The Security Group container topology displays how the Security Group is structured with respect to its parent Security Groups or children (Security Groups or other entities).



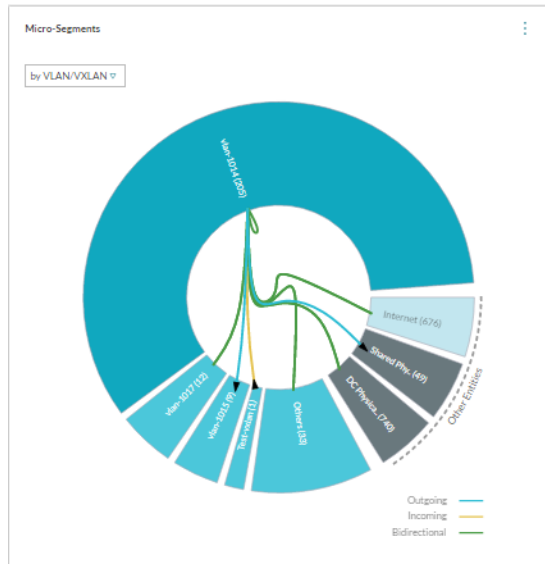
Micro-Segmentation Planning

The micro-segmentation planning topology shows all the flows that are present in your environment by dividing the flows into segments.

In vRealize Network Insight, a flow is a 4-tuple. It includes:

- source IP
- destination IP
- destination port
- protocol

You can analyze the flows by selecting scope and segment them accordingly based on entities such as VLAN/VXLAN, Security Groups, Application, Tier, Folder, Subnet, Cluster, VM, Port, Security Tag, Security Group, and IPSet. The blue lines denote the outgoing flows, the green lines denote the incoming flows, and the yellow lines denote the flows that are bidirectional. You can click any of the segments to view its details.



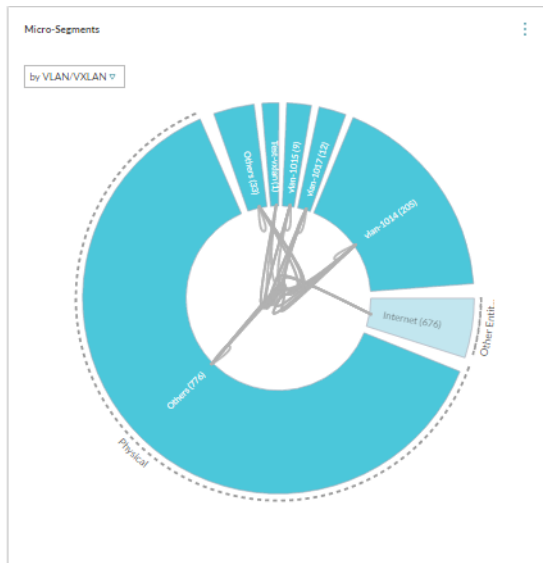
The VMs that are outside the selected scope are grouped as **Other Entities** in the micro-segmentation planning topology.

You can also analyze the flows by creating subgroups as per Physical, Other Virtual, and Internet

Group By	Also show groups for
by VLAN/VXLAN	Physical
by Application	Other Virtual
by Tier	Internet
by Subnet	✓ None
by Folder	
by Cluster	
✓ by VM	
by Port	
by Security Tag	
by Security Group	
by IPSet	

categories.

Each group is expanded into a wedge. In the following topology, the wedge for **Physical group** is seen.



There is also a Traffic Distribution pin that shows the amount of traffic that is flowing in different parts of your data center.

The Flows pin shows that the flows for different time intervals segregated by ports. You can either view all the flows or view the flows between two entities. You can filter the flows by Allowed and Blocked flows. Flows can be viewed by either Total Bytes or by Allowed Session Count. For the flows that are protected by a firewall, a Protected by Firewall sign is used to denote that the flows in that port that are protected by a firewall.

Application-Centric Micro-Segmentation

An application is a collection of tiers. Each tier in an application is a collection of VMs based on the user-defined filter criteria. The applications allow you to create a hierarchical group of VMs and visualize traffic/flows between the tiers of the same application. The traffic/flows can be visualized between applications.

To add application:

- 1 In the Search box, type application, and press Enter.
- 2 Click **Add Application**.
- 3 On the **Add Application** page, in the Application Name box, type a name for the application, which you want to create.
- 4 In the Tier section, type a name of the tier, which you want to create under Application (parent level). You can create a tier for VMs or physical machines as per requirements.
- 5 In the Virtual Machines/IP Addresses box, select the appropriate VMs by any of the following conditions:
 - **VM PROPERTIES**
 - VM Names - Name of the VMs, which you want to group in the tier you are creating
 - IP Addresses - IP Addresses of the VMs or physical machines, which you want to group in the tier you are creating. The count of the IP addresses is shown at the right side of the field.
 - VMs with Service Ports - Service ports of the VMs, which you want to group in the tier you are creating
 - Custom Search - It is an open search
 - **VMs IN**
 - Application - Select this option if the VMs are located in any previously created application
 - Cluster - Select this option if the VMs are located in any cluster
 - Folders - Select this option if the VMs are located in any folder
 - VXLAN - Select this option if the VMs are located in any VXLAN
 - VLAN - Select this option if the VMs are located in any VLAN

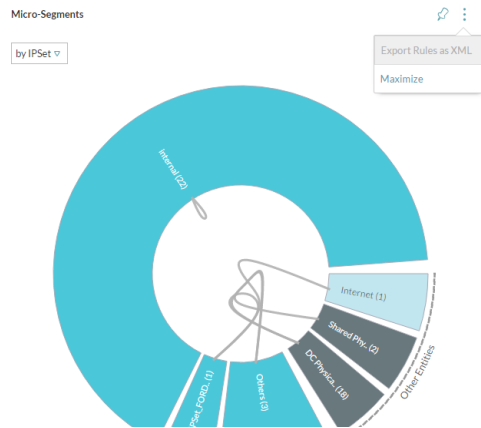
Note For entering multiple values, set apart the individual values by comma.

Optional: In case, you want to create multiple tiers under one application, click **Add Tier**.

- 6 Select Analyze Flows to view the flows before you finally add the application. You will be able to see the tiers based on VMs or physical addresses accordingly.
- 7 Click **Save** to create the application.

Exporting Rules

You can export rules as XML for the entire topology. You can find this option in the Micro-Segmentation Planning page as follows:



You can also export rules related to the underlying security groups belonging to multiple NSX managers. To import these rules in NSX, you can use scripts. Contact vRealize Network Insight support to get a copy of the sample script.

vCenter Tags

vRealize Network Insight provides vCenter tags for search and planning.

You can perform a search of VMs based on the vCenter tags and custom attributes. For example, you can use the following query for search by using tags:

```
vm where tag = '{keyname}:{value}'
```

Every tag belongs to a category. In the above example, the keyname is the category to which the tag belongs and value is the name of the tag.

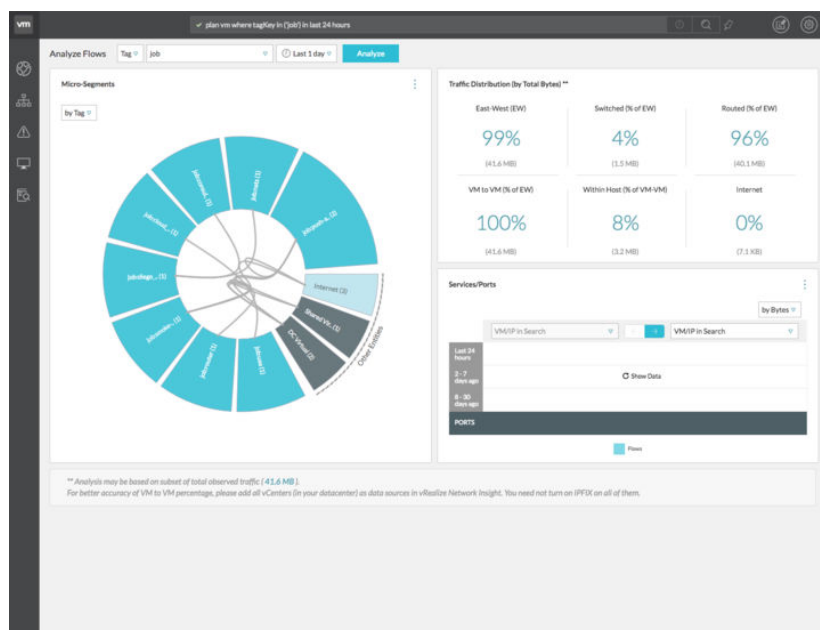
You can also provide an alternate name to a VM by using vCenter tags or custom attributes by using the name key. This alternate name is shown as the other names property. It is also possible to search and make path queries using the alternate name.

For example, the following queries are supported:

```
vm "other-name-1"
vm "other-name-1" to vm "other-name-2"
```

In this example, other-name-1 and other-name-2 are custom attributes with the name key or tags belonging to the name category.

You can also analyze the flows in the network by using the vCenter tags as shown in the figure.



Cross vCenter NSX

In a cross-vCenter NSX environment, you can have multiple vCenter Servers, each of which must be paired with its own NSX Manager.

One NSX Manager is assigned the role of primary NSX Manager, and the others are assigned the role of secondary NSX Manager. The primary NSX Manager is used to deploy a universal controller cluster that provides the control plane for the cross-vCenter NSX environment. The secondary NSX Managers do not have their own controller clusters. The primary NSX Manager can create universal objects, such as universal logical switches. These objects are synchronized to the secondary NSX Managers by the NSX Universal Synchronization Service. You can view these objects from the secondary NSX Managers, but you cannot edit them there. You must use the primary NSX Manager to manage universal objects. The primary NSX Manager can be used to configure any of the secondary NSX Managers in the environment.

The following Universal objects are supported:

- Universal LDR
- Universal Transport Zone
- Universal Logical Switch
- Universal Firewall Rule
- Universal Security Group
- Universal IPSets
- Universal Service
- Universal Service Groups
- Universal Segment Range

Collaboration Tools

All parts of the application are denoted as pins; fundamental units that can be saved and grouped to club data that you think can be useful together and to share them with other members of your team. You can pin a search query and also the pins that are available for an entity.

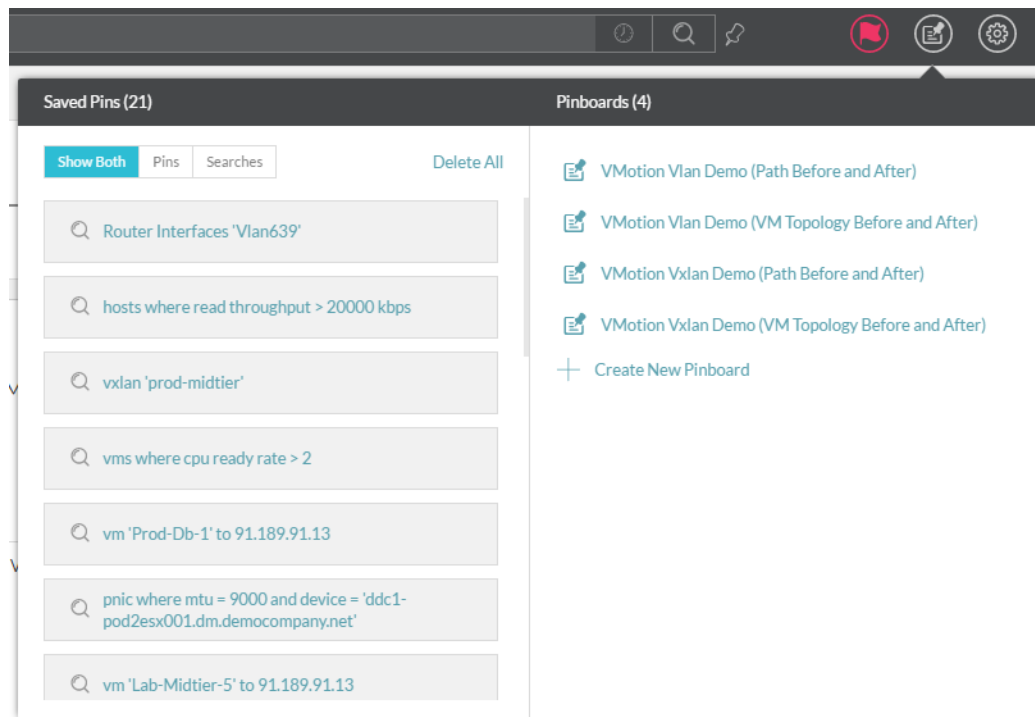
To add a pin, click the Pin icon. All your saved pins are displayed in Pinboards section which can be invoked by clicking the Pinboard icon in the header.

This chapter includes the following topics:

- [Pinboards](#)

Pinboards

Pinboards are how you group pins together.



To create a new pinboard:

- 1 Click **Pinboards** and select the pins that you want to add to the pinboard from the **Saved Pins** section.

- 2 Click **Create New Pinboard**.
- 3 Enter the name of the pinboard, add a note related to any information that you want to share with others, and enter the email IDs or name of the users with whom you want to share the pinboard and click Create.

To add a pin to an existing pinboard, after selecting the pin, click Add beside an existing pinboard where you want to add the pin.

To view the shareable URL of a pinboard, in the Pinboards section, click the link icon beside a particular pinboard.

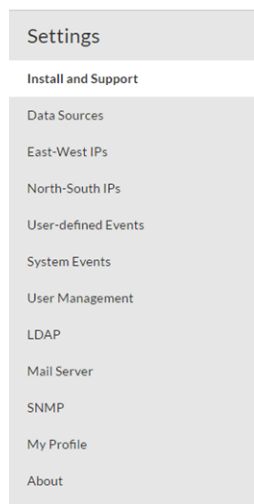
Settings

The **Settings** page provides controls to manage data providers, users, and notifications.

To go to the **Settings** page:

- 1 On the top-right hand corner in the Home page, click the Profile icon.
- 2 Click **Settings**. The **Settings** page appears as shown.

You can configure the following on the Settings page:



This chapter includes the following topics:

- [Install and Support](#)
- [Data Sources](#)
- [Data Management](#)
- [Enabling IPFIX Configuration](#)
- [East-West IPs](#)
- [North-South IPs](#)
- [System Events](#)
- [User-Defined Events](#)
- [Search-based Notifications](#)
- [Event Notification Email](#)


- [Event Notifications](#)
- [Syslog Configuration](#)
- [User Management](#)
- [LDAP](#)
- [Configuring Mail Server](#)
- [Simple Network Management Protocol \(SNMP\)](#)
- [My Profile](#)
- [About Page](#)
- [Automatic storage expansion for Platform VM](#)

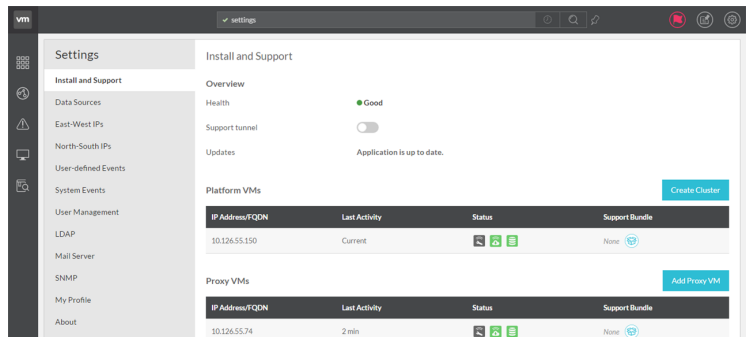
Install and Support

The Install and Support page provides an overview of the system as well as helps you to create cluster and add proxy VM to the existing vRealize Network Insight setup.

Note The terms **Proxy** and **Collector** are used interchangeably in the documentation.

To go to the **Install and Support** page:

- 1 On the top-right corner of Home page, click the Profile icon , and then click **Settings**.
- 2 In the Settings section, click **Install and Support**.



Health

The **Health** indicator is available in the **Overview** section on the **Install and Support** page.

The **Health** indicator turns red if any of the following malfunctioning events occur:

- If proxy stops collecting flow data
- If platform stops processing data due to some reason; for example, insufficient disk space
- If search indexer lags behind, resulting in outdated search result

The overall health indicator displays the number of irregularities, with a Red light on. The individual irregularities are listed with their details, when the number of problems against overall health, is clicked on. In case of normal functioning, the health indicator shines a Green light.

Support Tunnel

The **Support Tunnel** option is available in the **Overview** section on the **Install and Support** page.

The support tunnel allows support engineers to remotely connect to the customer platform and proxy VMs on the SSL secured connection. When a customer wants the product support team to look into a problem for troubleshooting, they can choose to turn on the support tunnel for the support engineers.

Note Ensure that the traffic to `support2.ni.vmware.com` on port 443 is allowed

Online Upgrade of Product

The **Update** option is available in the **Overview** section on the **Install and Support** page.

The **Update** option lets you know if the latest version of the product is available for an upgrade. A notification message appears in the product, and you can opt to upgrade to the latest version from the UI itself. To upgrade to the latest version:

- 1 In case a latest version is available, a message appears on the upper-right corner of the browser window.
- 2 Click **View details** in the notification.
- 3 You can view the new features, which are available in the new version.
- 4 Click **Install now** to start the upgrade.

Alternatively,

- 1 If a newer version is available, the information is displayed in the **Overview** section at the **Update** option.
- 2 Click **View Details**, to view the new features, which are available in the new version.
- 3 Click **Install now** to start the upgrade.

Creating Cluster

You can create clusters from the **Install and Support** page.

Prerequisites

At least two additional platforms are required. The additional platform VMs should be deployed and powered on.

To create cluster


- 1 Click **Create Cluster** for **Platform VMs**.

- 2 On the **Create Cluster** page, enter the following information:
 - **IP Address/FQDN:** Enter the IP address or FQDN of the new platform that you want to add.
 - **Password:** Enter the support user password of the platform VM. If you have not changed the password yet, then refer the *Default Login Credentials* section in *vRealize Network Insight Installation Guide* for the password.
- 3 To keep adding more platforms, click **Add more** and enter the IP address/FQDN and the support user password.
- 4 Click **Submit**. Click **Yes**.
- 5 After creating a cluster, the user needs to log in to the product again.

Creating Support Bundle

In order to look into the logs for inspecting the details and identifying anomalies, bundles of support logs are created.

To create support bundle:

- 1 In the Platform VMs or Proxy VMs table, in the Support Bundle column, click the Create Support Bundle icon .

Note Only two support bundles can be present at one given time, so while creating a new one, if there are already two support bundles present, the older one is deleted.

- 2 Click **Yes** to confirm creation of a new support bundle.

A new support bundle is created.

Data Sources

Data sources provide the application the ability to gather data from certain aspects of your data center. These range from your NSX installation to physical devices such as Cisco[™] Chassis 4500 and Cisco[™] N5K.

For each added Data source, the following information can be viewed at a glance:

- **All:** Displays all the available data sources.
- **With Problems:** Displays the data sources where vRealize Network Insight has found a problem.
- **With Recommendations:** Displays auto generated recommendations from vRealize Network Insight for the data sources that require additional information.

For each data source, you can view the following details:

Table 13-1.

Properties	Description
Device Type (nickname)	Displays name of the Data source.
IP Address/FQDN	Displays IP address or FQDN details for the Data Source.
Last Collection	Displays the last collection time on which the data is collected.
Actions	Displays options to edit, delete, and turn off data source.

Adding a Data Source

To add a Data Source

- 1 Go to **Settings** page and click the **Data Sources** tab.
- 2 Click **Add new source** and provide the required information in the text boxes.

Table 13-2.

Properties	Description
Source Type	Select the data source type from the drop-down menu.
IP Address/FQDN	Enter the IP Address/FQDN details
Username	Enter the username you want to use for a particular data source
Password	Enter the password

- 3 After entering the information in the fields, click Validate. If the validation is successful, you can add advanced data collection sources for the data source (not all data sources contain this feature).
Following advanced data collection sources are available:
 - For VMware vCenter, you can enable NetFlow (IPFIX). For more information on IPFIX, read the Enabling IPFIX configuration on VDS and DVPG section.
 - For VMware NSX Manager, you can enable automatic NSX Edge Population using SSH to allow vRealize Network Insight to collect advanced data. However, for NSX Manager 6.2 and above, Use NSX central CLI instead of ssh option can be selected to allow vRealize Network Insight to collect data for NSX Edge directly from NSX Manager using the NSX Central CLI. This feature also requires NSX Manager credentials with System Admin privileges.
 - Many data sources also use SNMP (Simple Network Management Protocol) for richer data collection. For such data sources, select the SNMP version and enter the community string to allow vRealize Network Insight to collect richer data from the data source.
- 4 Enter the required details in the fields for advanced data collection sources.
- 5 Enter Nickname and Notes (if any) for the data source and click **Submit** to add the data source to the environment.

Data Management

In vRealize Network Insight, you can specify for how long do you want to retain your data.


Note vRealize Network Insight supports data retention on an enterprise edition only.

The data is divided into four categories:

- Events
- Entities and Configuration Data
- Metrics
- Flows

Different policies can be configured and controlled for each category. You can configure the policy as per your requirement.

To configure data management:

- 1 On the top-right corner of the Home page, click  and then click **Settings**.
- 2 In the **Settings** section, click **Data Management**.
- 3 When you log in for the first time, this page shows the default data.
- 4 Click the information icon on more information on how data occupies the disk.
- 5 Click **Change Policy** to change the data retention period for the various categories of data. Once you make the changes, the information is recorded in the database.
- 6 Click **Submit**.

Note The retention period for low-resolution metrics is longer than the high-resolution metrics.

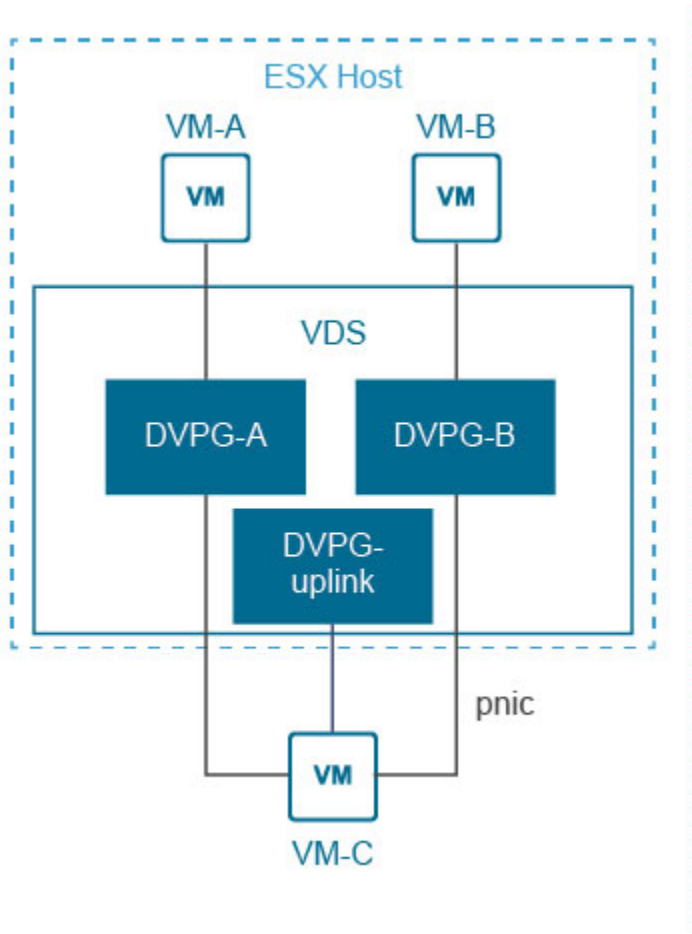
Enabling IPFIX Configuration

IPFIX is an IETF protocol for exporting flow information.

A flow is defined as a set of packets transmitted in a specific timeslot, and sharing the same 5-tuple values - source IP address, source port, destination IP address, destination port, and protocol. The flow information may include properties such as timestamps, packets/bytes count, Input/Output interfaces, TCP Flags, VXLAN ID, Encapsulated flow information, and so on.

A VDS in vSphere environment can be configured to export flow information using IPFIX. Flow monitoring has to be enabled on all the port groups attached to the VDS. If packets arrive on port X of a VDS and exit from port Y, a corresponding flow record is emitted if flow monitoring is enabled on port Y.

To analyze the complete information of any session, IPFIX data about packets in both the directions is required. Refer following diagram where VM-A is connected to DVPG-A and is talking to VM-C. Here DVPG-A will only provide data about the C→A packets, and DVPG-Uplink will provide data about A→C packets. To get the complete information of A's traffic, IPFIX should be enabled on DVPG-A, DVPG-uplink.



vRealize Network Insight Proxy VM has built-in collector/receiver for IPFIX flow information. You can enable the IPFIX information collection in the vCenter Data Source settings at various levels of granularity. To enable IPFIX information at vCenter level select the Enable NetFlow (IPFIX) on this vCenter check box when you are adding the vCenter.

After you select the check box, a list of available VDS in the vCenter is displayed. Select the VDS for which you want to enable IPFIX.

A notification icon is displayed for the VDS where one of the hosts has unsupported version of ESXi. If vRealize Network Insight has detected that IPFIX is already configured for a VDS with some other IP address apart from vRealize Network Insight Proxy VM then it displays an Override button. You can click Override to view the list of DVPGs under that VDS.

The list of available DVPGs for the selected VDS is displayed. By default all the DVPGs are selected. Turn Manual Selection on to select specific DVPGs for which you want to enable IPFIX. Select the desired DVPGs and click Submit.

Note The DVPG with a notification icon denotes that it is the uplink DVPG and it cannot be deselected.

East-West IPs

The IPs that are within the range of RFC1918 standard are considered private IPs. The IPs that are outside the RFC1918 are treated as Internet IPs. However, users can specify their East-West IPs (datacenter public IPs) that they want to be treated as non-Internet IPs while tagging flows and micro-segmentation, even if these are outside the private IP address range as defined by RFC1918.


To specify public IPs to be treated as non-internet IPs

- 1 On the top-right corner of Home page, click the Profile icon, and then click **Settings**.
- 2 In the Settings section, click **East-West IPs**.
- 3 In the IP Addresses box, enter specific IPs, or IP ranges, or subnets, which are to be treated as non-internet IPs.
- 4 Click **Save**. The IP Addresses Saved confirmation message is displayed upon successful saving.

North-South IPs

The IPs that are in the RFC1918 space are categorized as North-South IPs. The users can specify their North-South IPs while tagging flows and micro-segmentation.

To specify North-South IPs:

- 1 On the top-right corner of Home page, click the Profile icon , and then click **Settings**.
- 2 In the Settings section, click **North-South IPs**.
- 3 In the IP Addresses box, enter specific IPs, or IP ranges, or subnets.
- 4 Click **Save**. The IP Addresses Saved confirmation message is displayed upon successful saving.

System Events

The event is defined either by the system or the user. The system events are predefined events.

The system events are listed in the System Events page under Settings. The following fields are specified for each event. You can filter the events based on these fields.

Table 13-3.

Field	Description
Event	This field specifies the name of the event.
Severity	<p>This field specifies the severity of the event. You can set it to the following values:</p> <ul style="list-style-type: none"> ■ Critical ■ Moderate ■ Warning ■ Info
Type	This field specifies if the event denotes a problem or a change.
Entities	This field specifies that the event is configured to either include or exclude entities for event generation. By default, the value is All.
Notifications	This field specifies the types of notifications that are sent. The notifications can be sent by email or SNMP trap or both.
Enabled	This option is selected if the event is enabled.

When you hover the mouse on each event, you can see **More Information**. By clicking this option, you can see the description, event tags, and entity type for that event.

You can perform the following tasks on the system events:

- Disable an event for a particular entity
- Edit an event
- Perform bulk edit

Perform bulk edit

- 1 In the **System Events** page, when you select multiple events, the options **Enable**, **Disable**, and **Edit** appear above the list.
- 2 Click **Edit**.
- 3 In the **Edit** page, you have the following options:
 - **Override existing values:** In this option, only the fields that you edit will get overwritten.
 - **Add to existing:** In this option, you can add to the existing values such as email addresses and event tags.
- 4 Click **Submit**.

Edit an event

- 1 Click the edit icon after the **Enabled** column for a particular event.
- 2 You can add or remove event tags if required.
- 3 You can change the severity.

- 4 Check Include/Exclude entities if you want the event to be enabled or disabled for selected entities.
- 5 To create inclusion rules:
 - a Select **Inclusion List**.
 - b Specify the entities which you want to include for the event under **Conditions**.
- 6 To create exclusion rules:
 - a Select **Exclusion List**.
 - b Specify the entities which you want to exclude for the event under **Conditions**.

Note

- You can create multiple rules in both inclusion and exclusion lists.
 - When you select NSX Manager, you can add exceptions in both the lists. You can define exception if you want the inclusion or the exclusion rule to hold exception for a particular entity.
 - You can also specify Custom Search by writing your own query to include or exclude entities.
-

- 7 Select **Enable Notifications** if you want to configure when the notifications have to be sent. Specify the email address and the frequency at which you would like to receive the emails.

Disable an event for a particular entity

- 1 You can select an event in the **Open Problems** widget in the Homepage. You can also enter **Problems** in the search bar and select an event from the list.
- 2 Select a particular event and click **Archive**.
- 3 Select **Disable all events of this type in future for** and select an entity or all entities.
- 4 Click **Save**.

Note The changes made in severity, tags, or inclusion/exclusion rules will reflect for the future events. The existing events continue to show the old configuration.

User-Defined Events

The user-defined events are based on search.

All the user-defined events are listed on the **User-defined Events** page under **Settings**. The following fields are specified for each event.

Table 13-4.

Field	Description
Name (Search Criteria)	This field specifies the name of the event and the search criteria for the event.
Severity	This field specifies the severity of the alert. You can set it to the following values: <ul style="list-style-type: none"> ■ Critical ■ Moderate ■ Warning ■ Info
Type	This field specifies if the event denotes a problem or a change.
Notify when	This field specifies when the notification has to be sent.
Created By	This field specifies who created the event.
Enabled	This option is selected if the event is enabled.

You can edit or delete the event. While editing it, you can specify the email address and the frequency of the email notification.

Search-based Notifications

The search-based notifications can be categorized as follows:

- System-based notification
- User-defined notification

System-based notification parameters are predefined and upon activating notification alert, notification in the form of mails are sent. User-defined notifications are set by users, based on their requirements. You can create email notifications based on your search query. After you run a search, on the Results page, the **Create notification** option is displayed. For each search, you can:

- Select the condition when you want to receive the notifications.
- Define how frequently you want to receive the notifications.
- Enter the email recipients for each notification (by default, your email ID is present in the receiver's list; you can also add multiple email IDs).

For a user-defined search:

- It is mandatory for you to assign a name to the search-based notification.
- It is mandatory to select the severity of a search-based event that is marked as a problem.
- The user-defined events are uniquely identified by the search criteria.
- You can specify the notification frequency as **Immediately** or **As a daily digest**.

You can manage your notifications from the **Settings > Search-based Notifications** page. On the **Search-based Notifications** page, you can view the existing notifications, edit them, activate or deactivate them, and also delete unwanted notifications.

Event Notification Email

The notifications are sent in the form of emails.

To set up notification, users have to first configure the mail server. To know how to configure mail server, see [Configuring mail server](#).

Specifying Notification Events for Emails to be sent

Users can specify events for which mail notifications are to be sent.

To specify events

- 1 On the **Settings** page, click **Search-based Notifications**, or simply search for any information using the Search box.
- 2 On the Search-based Notifications page, click the **Create Notification** icon. A notification dialog box is displayed.
- 3 In the **Receive notification when** box, select the event on the occurrence of which notifications are to be sent.
- 4 In the **Notify** box, select the frequency at which the notifications are to be sent.
- 5 If the event is undesirable, select the **Mark it as a problem** check box.
- 6 Enter the email addresses to which the notifications are to be sent, and then click **Save**.

Note To verify whether the notification mail is correctly set up, click **Send test Email**.

Event Notifications

vRealize Network Insight contains a list of predefined system events (system problems and system changes) for which you can receive automated email notifications every four hours.

You can view the list of notifications on the **Settings > System Notifications** page.

Archiving Problems

Archiving a Problem

- 1 Click the Show All link (if there is more than one instance of an event) to display all instances of the event.
- 2 Hover on the instance of the event that you want to archive to display a set of icons, and then click the Archive icon.

- 3 In the Event specific dialog box
 - a Select This event from the You are about to archive list, if you want to archive only this event.
 - b Select All events of this type from the You are about to archive list, if you want to archive all events of the same type in the system.
- 4 Click **Save**.

Viewing all archived events

- 1 On the Home page, type events in Search box and press **Enter**. A list of events is displayed.
- 2 On the left hand pane, in the Archived facet, select True checkbox (highlighted in the screenshot below).

You can view all archived events here.

To restore an archived event

- 1 On the Archived event, click the Archived icon . (See the preceding section on To view an archived event to know how to go to the Archived events page).
- 2 In the Event specific dialog box
 - a Select This event from the You are about to restore from archive list, if you want to restore only this event.
 - b Select All events of this type from the You are about to restore from archive list, if you want to restore all similar type of events.
 - c Click Save to complete restoring.

Disabling Events

Users can selectively disable events and prevent notifications from being sent in future.

To disable event notification

Method 1

- 1 On the event, click the **Show All** link (if there is more than one instance of an event) to display all instances of the event.
- 2 Hover on the instance of the event, whose notification you want to disable. This displays a set of icons, click the Archive icon .
- 3 In the Event specific dialog box, select the **Disable all events of this type in future** checkbox, and then click **Save**.

Method 2

- 1 On the top-right corner of **Home** page, click the **Profile** icon, and then click **Settings**.
- 2 In the **Settings** section, click **Event Notifications** to see a list of all enabled and disabled events.

- 3 On the enabled event that you want to disable, in the **Enabled** column, click the left-side space of the respective slider.
- 4 In the **Confirm Action** dialog box, click **Yes**.

Configuring Event Notification Service

Users can enable customer notifications for different events

To set notification services

- 1 On Settings, go to Event Notification, and click the (edit) icon corresponding to the problem, for which you want to enable e-mail notifications and SNMP.
- 2 In the Edit System Notification dialog box, enter the email address to which you want the email notification to be sent. In the Email Frequency box, select the time frequency at which you want to receive notifications.
- 3 Select the Enable SNMP trap for this event checkbox to set SNMP notifications.
- 4 Click **Save**.
- 5 Once successfully enabled, the respective mail and SNMP icons appear, as highlighted in the screenshot below.

Syslog Configuration

You can configure remote syslog servers for vRealize Network Insight by using the **Syslog Configuration** page.

While every proxy server can potentially have a different remote syslog server, all the platform servers in a cluster use the same remote syslog server.

In the current release, the vRealize Network Insight problem events and platform/proxy server syslogs are sent to the remote syslog server.

Currently, vRealize Network Insight supports only UDP for communication between vRealize Network Insight servers and remote syslog servers. So ensure that your remote syslog servers are configured to accept syslog traffic over UDP.

To configure syslogs:

- 1 In the **Settings** page, click **Syslog Configuration**. The **Syslog Configuration** page has the configured syslog servers and their mappings to the virtual appliances listed. If you are accessing this page the first time, then the syslog is disabled by default and the list of servers on this page does not appear.
- 2 To add a syslog server:
 - a Click **Add Syslog Server**.
 - b Enter IP Address, nickname, and port number of the server. The standard port number for UDP is 514.

- c To test the configuration, click **Send Test Log**.
 - d Click **Submit**.
 - e If it is the first server that you have added, then enable syslog at the top of the page.
- 3 To map the server to platforms and proxies:
- a Click **Edit Mapping**.
 - b Select the syslog server for All Platforms and Proxy servers.
 - c If you do not want to enable syslog on any proxy server or on the platform, select the **No server** option.
 - d Click **Submit**.

Note After you make the changes, it might take a few minutes for them to be effective.

User Management

The admin user can add new users and configure memberships and other settings of existing users. The users with membership role of administrator only can view the **User Management** tab.

Add New User

- 1 In the **Settings** page, click **Create new user**, and provide the required information in the form.

The form has the following text boxes:

Table 13-5.

Properties	Description
Name	Enter the name of the user.
Email (Login ID)	Enter your email or login ID if any.
Role	Select the role from drop-down list.
Password	Enter the password.
Re-enter new password	Re-enter the password for confirmation.

- 2 Click **Add User** to save the user information.

Assign Administrator Role

You can assign an administrator role to any LDAP user.

Even if that particular user is not logged in, you can still assign the administrator role to that user. To assign the administrator role:

- 1 In the **Settings** page, click **User Management**.
- 2 Click the **LDAP Users** tab.

- 3 Click **Assign Admin Role**.
- 4 Provide the login ID of the user to whom you want to assign the administrator role.
- 5 Click **Add User**.
- 6 Once you add the user, you can see the login ID in the LDAP Users tab.
- 7 To change the role, click the edit icon next to the login ID in the LDAP Users tab.

LDAP

vRealize Network Insight supports the following two types of users:

- User created on vRealize Network Insight Platform VM
- LDAP users

To allow the LDAP users log into vRealize Network Insight, configure the LDAP service in the vRealize Network Insight Platform as follows:

To enable LDAP-based User Authentication

- 1 On the **Settings** page, click **LDAP**, and then click **Configure**.
- 2 In the **Configure LDAP** page, type the appropriate domain, LDAP Host URL, and LDAP credentials in the respective boxes. See the following table for individual field descriptions.

Table 13-6.

Field	Description
Domain	This is typically the last part of the user email address after the '@' sign. Example: For an user logging in as johndoe@example.com, this field will be example.com
LDAP Host URLs	You can specify multiple LDAP Host URLs separated by commas.
Restrict access to specific groups	You can select this option if you want only the group members to access the application.
Username	User with necessary rights to log in using the settings provided.
Password	Password of the user.

Optionally, you can provide access only to specific groups by selecting the Restrict access to specific groups check box.

- a Click **Add more under Group DN** to add groups in the inclusion list.
 - b In Base DN, type the Base DN, the point from which the server starts searching for users.
- 3 Click **Submit** to configure LDAP.

After the LDAP configuration is successful, a new drop-down menu is available on the login screen where users can select whether they want to log in locally or using their LDAP credentials.

The LDAP credentials are not saved anywhere.

Configuring Mail Server

To configure mail server

- 1 On the top-right corner of Home page, click the **Profile** icon, and then click **Settings**.
- 2 Click **Mail Server**.
- 3 Select the SMTP server checkbox.
- 4 Enter appropriate values in the boxes.

Table 13-7.

Field	Description
Sender Email	This is the sender's email address.
SMTP Hostname/IP Address	This is the hostname or IP of the SMTP server.
Encryption	The following encryption options are available: None, TLS, and SSL.
SMTP Port Number	This is the Port number of SMTP server (default 25).

Optionally, for additional security, select the Authentication checkbox, and enter the username and password.

Note To verify whether the notification mail is correctly set up, click **Send test Email**.

- 5 Click **Submit** to complete the configuration.

Simple Network Management Protocol (SNMP)

The product supports the following two versions of SNMP:

- 1 v2c
- 2 v3

Configuring SNMP service

- 1 On the top-right hand corner in the Home page, click the Profile icon, and then click **Settings**.
- 2 On the **Settings** page, click **SNMP**, and then click **Configure SNMP Service**.
- 3 On the **Configure SNMP Service** page, in the Version box, select SNMPv2c or SNMPv3 protocol.

Note SNMPv2c protocol does not require authentication. SNMPv3 protocol supports authentication.

- 4 In the Destination IP Address/FQDN box, enter the IP address of the SNMP agent, or enter the Fully Qualified Domain Name (FQDN).
- 5 In the Destination Port box, enter **162**.

- 6 If you select the SNMPv2c protocol, in the Community String box, enter **Public**. If you select the SNMPv3 protocol, in the Username box, enter the name of the user you created in the SNMP agent.

For SNMPv3, additionally,

- Select the **Use Authentication** checkbox.
- Select an authentication protocol, and then enter the password you had set for the particular user in the SNMP agent. Optionally, in the Privacy Protocol and Privacy Phrase boxes, select a privacy protocol and a privacy phrase respectively.

To verify whether the configuration is correctly done, click **Test SNMP trap**, and then find whether the trap has been sent to the SNMP agent.

- 7 Click **Submit**.

My Profile

The logged-in user can change the password on this tab. Change your password here and save Changes.

To change your password

- 1 Under **Settings**, click **My Profile**. The **Change Password** window opens.
- 2 On the **My Profile** page, fill in the following information and click Save.

Table 13-8.

Properties	Description
Current password	Enter your current password.
New password	Enter the new password.
Re-enter password	Re-enter the new password for confirmation.

About Page

This page displays the license details and the product version number that you are currently using.

Change License

In the event of expiry of evaluation license, when you log in to the product, a message appears stating that the license has expired and that you need to renew your license. Follow the steps below to change license.

To change license:

- 1 Click the link contained in the Expiry message to go to the Change License page. Alternatively, in **Settings**, click **About**, and then click **Change License**.

- 2 In the **Change License** page, in **New License Key**, enter the new license key you received from VMware.
- 3 Click **Validate**.
- 4 Click **Activate**.

Customer Experience Improvement Program

You can join or leave the Customer Experience Improvement Program (CEIP) for vRealize Network Insight at any time.

vRealize Network Insight gives you the opportunity to join CEIP when you initially install and configure the product. After installation, you can join or leave CEIP by following these steps.

When you install and configure vRealize Network Insight, you can enable or disable CEIP as follows:

- 1 In the **About** page, under Customer Experience Improvement Program, click **Modify**.
- 2 The CEIP window pops up. To enable CEIP, check **Enable**. This action activates CEIP and sends data to <https://vmware.com>.
- 3 To disable CEIP, uncheck **Enable**.
- 4 Click **Submit**.

Automatic storage expansion for Platform VM

To expand the storage available to the Platform VM, a new hard disk needs to be added using the VMware vCenter. Once the disk is added, the product will automatically recognize and start using the newly added storage seamlessly.

Help

The **Help** page provides a list of supported search queries and parameters with supported properties that are currently supported by the application. To view the Help page, click the drop-down on the top right corner and then click **Help**.

Search Queries

The search queries demonstrate the power of the search system in the application and provide a non-exhaustive list of queries with a brief description of what each of them signify. These clickable queries can be used to quickly get a glimpse of your provisioned environment.

Supported Properties

The supported properties tab provides a list of properties per entity that can be used to target specific attributes while writing search queries. For example: Memory is one of the supported properties for hosts and can be used like hosts where memory = 5GB to view hosts who have 5GB of memory installed.

Common Data Source Errors

When you add a data source, you can come across several errors. This table contains the list of common errors with the cause and resolution for each.

Table 15-1.

Error Text	Cause	Resolution
Invalid Response from Data Source	vRealize Network Insight Proxy was unable to process the information received from the Data Source as the information was not in the expected format.	In some data providers this problem is observed intermittently and might go away in the next polling cycle. If it occurs consistently, contact support.
Data Source is not reachable from Proxy VM	Data source IP address on SSH/REST (port 22 or 443) is either not reachable from the vRealize Network Insight Proxy VM or the data source is not responding. This error occurs while adding the data source.	Verify connectivity to the data source from vRealize Network Insight Proxy VM on port 22 or 443. Make sure data source is up and running and the firewall is not blocking connection from vRealize Network Insight Proxy VM to the data source.
No NSX Controller found	An NSX Controller has been selected in the NSX Manager data source page but there is no NSX Controller installed.	Install an NSX Controller on NSX Manager and then select NSX Controller check box on the NSX Manager data source page.
Data source type or version mismatch	Provided data source IP Address/FQDN is not of selected data source type.	Verify that provided data source IP Address/FQDN is of selected data source type and version is supported by vRealize Network Insight
Error connecting to data source	vRealize Network Insight Proxy VM is unable to connect to the data source. This error occurs after adding the data source.	Verify connectivity to the data source from vRealize Network Insight Proxy VM on port 22 or 443. Make sure that the data source is up and running and firewall is not blocking connection from vRealize Network Insight Proxy VM to the data source.
Not found	vRealize Network Insight Proxy VM is not found.	Check if pairing is done between vRealize Network Insight Proxy VM and vRealize Network Insight Platform VM.
Insufficient privileges to enable IPFix	The user who is trying to enable IPFIX in vCenter does not have the following privileges: DVSwitch.Modify; DVPortgroup.Modify	Provide adequate privileges to the user.

Error Text	Cause	Resolution
IP/FQDN is invalid	The IP/FQDN provided on the data source page is not valid or does not exist.	Provide valid IP/FQDN address.
No data being received	vRealize Network Insight Platform VM is not receiving data from vRealize Network Insight Proxy VM for that data source.	Contact Support.
Invalid credentials	Provided credentials are invalid.	Provide the correct credentials.
Connection string is invalid	The IP/FQDN provided on data source page is not in proper format	Provide valid IP/FQDN address.
Recent data may not be available, due to processing lag	vRealize Network Insight Platform VM is overloaded and lagging behind in processing data.	Contact support.
Request timed out, please try again	Could not complete request in specified time.	Try again. If the issue is not fixed, then contact support.
Failed for unknown reason, please retry or contact support	Request failed for some unknown reason.	Try again. If the issue is not fixed, then contact support.
Password authentication for SSH needs to be enabled on device	SSH login using password is disabled on the device added	Enable password authentication for SSH on the device being added for monitoring.
SNMP connection error	Error connecting to the SNMP port	Verify if SNMP is configured correctly on the target device.