VMware vRealize Network Insight Search Query Posters

Get Deeper Insights from Your Infrastructure, Faster
Introduction

As a VMware admin, you know VMware vRealize® Network Insight™ provides a robust search for all of the entities in your environment. It has property and entity terms, as well as aggregate function terms you can tune for best-results infrastructure to cloud to branch planning and analysis.

But we're all busy. And with so little time and so many questions, our team came up with a series of vRealize Network Insight search query cheat sheets to inspire you while getting to insights faster.

Download, view, and display one. Or download, view, and display them all. As a go-to resource or simply an office conversation starter, each guide includes everything you need for results.

Search Guide Topics

1. Flows
2. PKS – Kubernetes
3. VMware NSX – T
4. VMware NSX® Data Center for vSphere®
5. VMware SD-WAN™ by VeloCloud®
6. Virtual machine
Ready Queries

Visual Results

- Choose sample queries in grey
- View properties to search in green
- Find metrics delivered in blue

- View tables and graphs
- Sort options
- Filter results
How to Get Started

When you need results fast, select the search feature in vRealize Network Insight and start typing in the syntax highlighted on a poster.

These are sample searches:

- Discover which VMs have too many snapshots by entering this query: Top 10 vms by snapshot count
- Identify the top talkers from this VM by entering the following: sum(-bytes) of flows where Flow Type = ‘Src is VM’ and Flow Type = ‘Dst is Internet’
- Find out which countries your customers are coming from by entering this query: flow group by Destination Country
- Discover Kubernetes PODs that are failing due to image errors by entering the following: Kubernetes events where Event code = ‘Image-PullBackOff’ in last 24 hours
- Identify unstable internet connections in your SD-WAN by entering this code: SD-WAN Link where Connectivity State != ‘Stable’
Sample Queries

```
- flow where bytes > 100 gb
- flow group by vm
- top 5 flow order by packets
- flow group by Destination Country
- count of flow group by Destination IP Address
- Internet traffic by source VM: sum(bytes) of flows where Flow Type = 'internet' group by source vm order by sum(bytes)
- Internet traffic: flows where Flow Type = 'Source is Internet' and Flow Type = 'Destination is VM' order by bytes
- Sum of bytes between VM & internet: sum(bytes), sum(src bytes), sum(dest bytes) of flows where Flow Type = 'Source is VM' and flow type = 'Destination is Internet'
- Total VTEP traffic: sum(bytes) of flows where Flow Type = 'Source is VTEP' or Flow Type = 'Destination is VTEP'
- VTEP traffic grouped by VMKNIC: sum(bytes) of flows where Flow Type = 'Source is VTEP' or Flow Type = 'Destination is VTEP'
- Aggregated traffic series for matching flows: series(sum(byte rate)) of flows where host = 'myhost.abccorp.com'
- and (flow type = 'source is vm' or flow type = 'destination is vm')

VM flow between hosts:
- flow where Flow Type = 'VM-VM' and Flow Type = 'Diff Host' order by bytes
- sum(bytes) of flow where Flow Type = 'VM-VM' and Flow Type = 'Diff Host' group by vm order by sum(bytes)
```

NSX-V Firewall - Configuration Properties

- Flow
- HIP Profile
- IP Address
- Status
- Target
- Target Negation
- Vendor
- vm series
- Indirect Source IPSet
- Indirect Source Security Group
- Logging Enabled
- Manager
- Manager Model
- Manager Serial
- Manager Version
- Action
- Application
- Application ID GUID
- Appliedto
- Category
- Change
- Configured Destination
- Configured Source
- Destination
- Destination Address
- Destination Any
- Destination IP
- Destination IPSet
- Destination Negate
- Destination Security Group
- Destination VM
- Destination Zone
- Device Group
- Direct Group
- Direct Group Address
- Direct Group Address Group
- Direct Group Security Group
- Direct Group Source Address
- Direct Group Source Address Group
- Direct Group Source Security Group
- Direction
- IPSet
- Indirect Direct Address
- Indirect Direct Address Group
- Indirect Direct Group
- Indirect Direct Security Group
- Indirect Direct Source Address
- Indirect Direct Source Address Group
- Indirect Direct Source Security Group
- Direction
- IPSet
- Indirect Source IPSet
- Indirect Source Security Group
- Indirect Source Address
- Indirect Source Address Group
- Indirect Source Security Group
- a Source Address
- a Source Address Group
- Source Address
- Source Address Group
- Source Any
- Source IP
- Source IPSet
- NSX-V Controller - Configuration Properties

- Activated
- Change
- Event
- Enabled
- IP Address
- Join Status
- Ldr
- Majority Status
- Manager
- Master
- NSX Manager
- Name
- Network Address
- Problem
- Role Name
- Scope
- Status
- Upgrade Available
- VM
- VXLAN
- Vendor ID
- Version

NSX-V Manager - Metrics

- Incomplete tcp flow drop count
- Outbound expire flow drop count
- Wrong collector flow drop count

NSX-V Security Group - Configuration Properties

- All Direct Child Group
- All Parents
- Change
- Child
- Direct Destination RuleSets Type
- Direct Incoming Rules
- Direct Outgoing Rules
- Direct Source RuleSets Type
- Event
- Excluded
- IP Address
- IPSet
- Incoming Rule Count
- Indirect Destination RuleSets Type
- Indirect Incoming Rule Count
- Indirect Incoming Rules
- Indirect Outgoing Rule Count
- Indirect Outgoing Rules
- Indirect Source RuleSets Type
- Manager
- Manager Model
- Manager Serial
- Manager Version
- Member
- NSX Manager
- Name
- Outgoing Rule Count
- Problem
- Region
- Rule Count
- Security Tag
- Translated VM
- Vendor
- Vendor ID

NSX-V Policy Firewall - Configuration Properties

- All Direct Child Group
- Child
- Direct Destination RuleSets Type
- Direct Incoming Rules
- Direct Outgoing Rules
- Direct Source RuleSets Type
- Event
- Exclude
- IP Address
- IPSet
- Incoming Rule Count
- Indirect Destination RuleSets Type
- Indirect Incoming Rule Count
- Indirect Incoming Rules
- Indirect Outgoing Rule Count
- Indirect Outgoing Rules
- Indirect Source RuleSets Type
- Manager
- Manager Model
- Manager Serial
- Manager Version
- Member
- NSX Manager
- Name
- Outgoing Rule Count
- Problem
- Region
- Rule Count
- Security Tag
- Translated VM
- Vendor
- Vendor ID

NSX-V Policy Based VPN - Configuration Properties

- All Parents
- Change
- Event
- IP Address
- IP Range
- IP Address Range end
- IP Address Range start
- Translated VM
- Vendor ID
- Network Address
- Problem
- Scope
- Tag
- Manager
- NSX Manager
- Name
- Network Address
- Problem
- Scope
- Tag
- Manager
- NSX Manager
- Name
- NSX Manager
- Name
- NAT
- Indirect Incoming Rules
- Indirect Outgoing Rules
- Direct Destination RuleSets Type
- Direct Incoming Rules
- Direct Outgoing Rules
- Direct Parent Security Group
- Direct Source RuleSets Type
- Indirect Destination RuleSets Type
- Indirect Source RuleSets Type
## PKS - Kubernetes Search Poster

### Sample Queries

#### Common Queries
**Search Flows:** flows where Kubernetes Object = Object name
**View the service health:** flows from Kubernetes Pod name to Kubernetes Services
**View the node load:** Kubernetes Pods group by Kubernetes Node
**View flow compliance:** Example: flows from Kubernetes Namespace 'Non-PCI' to Kubernetes Namespace 'PCI'

#### Kubernetes Objects
**Nodes:** Kubernetes nodes where Ready = 'True'
**Services:** pods where Kubernetes services is not set

#### Packet drops group by Kubernetes pod
nsx-t logical port where (ConnectedTo in (Kubernetes Pods where (Kubernetes Cluster is set) and Rx Packet Drops > 0) group by (max(Rx Packet Drops)

### Configuration Properties

**Kubernetes Service**
- **Annotations Key**
- **Annotations Key Value**
- **Change**
- **Cluster ID**
- **Cluster IP**
- **Cluster Network Mask**
- **Cluster Network Address**
- **Creation Time**
- **Event**
- **External IP**
- **External IP Addresses**
- **External Network Mask**
- **External Network Address**
- **Kubernetes Cluster**
- **Kubernetes Namespace**
- **Label**
- **Label Key**
- **LoadBalancer IP**
- **LoadBalancer IP Address**
- **LoadBalancer Network Address**
- **Manager**
- **Name**
- **Node Port**
- **Port Name**
- **Problem**
- **Protocol**
- **Selectors**
- **Selectors Key**
- **Target Port**
- **Type**
- **Vendor ID**
- **modelKey**

**Kubernetes Node**
- **Annotations Key**
- **Annotations Key Value**
- **Change**
- **Creation Time**
- **Event**
- **Kubernetes Cluster**
- **L2 Networks**
- **Label**
- **Label Key**
- **Manager**
- **Name**
- **Problem**
- **Router**
- **Vendor ID**
- **modelKey**
- **status**

**Kubernetes Pod**
- **Annotations Key**
- **Annotations Key Value**
- **Change**
- **CIFS**
- **Contents**
- **Creation Time**
- **Event**
- **HOST**
- **IP Address**
- **IPAddress**
- **Kubernetes Cluster**
- **Kubernetes Namespace**
- **Kubernetes Node**
- **Kubernetes Services**
- **Label**
- **Label Key**
- **Logical Port**
- **Manager**
- **Name**
- **Kubernetes Pod Name**

**Kubernetes Data Source**
- **Change**
- **Enabled**
- **Event**
- **NSX Manager**
- **Problem**
- **URL**

### PKS - Kubernetes Search Poster

#### Show <config Propert> of Kubernetes object
**Supported properties for Configuration Queries**
- **Group by:** Ex: Kubernetes pods group by kubernetes services
- **Aggregate Functions:**
  - max, min, sum, avg
- **Ex:** sum(MemoryPressure) of kubernetes node

**Kubernetes Objects**
- **Nodes:**
  - Kubernetes nodes where Ready = 'True'
- **Services:**
  - pods where Kubernetes services is not set

**Packet drops group by Kubernetes pod**
nsx-t logical port where (ConnectedTo in (Kubernetes Pods where (Kubernetes Cluster is set) and Rx Packet Drops > 0) group by (max(Rx Packet Drops)

**Packet drops group by Kubernetes node**
nsx-t logical port where (ConnectedTo in (Kubernetes Nodes where Kubernetes cluster is set) and Rx Packet Drops > 0) group by (max(Rx Packet Drops)

**Packet drops group by Kubernetes services**
nsx-t logical port where (ConnectedTo in (Kubernetes Pods where (Kubernetes Cluster is set) and Rx Packet Drops > 0) group by (max(Rx Packet Drops)

**Packet drops group by Kubernetes namespace**
nsx-t logical port where (Rx Packet Drops > 0) group by (max(Rx Packet Drops)

**Pods count**

**Nodes count**
Sample Queries

top 10 nsx-v firewall rules order by connection count
sum(bytes) of flows where Flow Type = 'Src is VM' and Flow Type = 'Dst is Internet'
sum(Session Count) of flows by firewall rule order by sum(session count) where firewall ruled = 1032
host group by Firewall Status
host group by Hostprep Feature Status
host group by Hostprep Feature Version
vmware vm group by Firewall Rule
NSX-V Controller group by Upgrade Available
Security group where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set

Un-Protected Flows
Flows where firewall rule is not set
List of firewall rules which are not hit by any flow in last 30 days
NSX firewall rule where flows is not set in last 30 days
Flows hitting specific rule id's / firewall rules/specific security group/specific application
Flow where rule id in (1011, 1012, 1013)
Flow where firewall rule like rule1
Flow where security group like sg!Flows hitting on an application,Flow where application = app1
Flow where application = app1 and tier = TierName
New Firewall rules
New firewall rules in last 24 hours
New firewall rules in last 30 days

NSX-V Controller - Configuration Properties

version
change
ID
IP Address
Join Status
Majority Status
Manager
Master
NSX Manager
Name
Network Address
Problem
Role Name
Scope
Status
Upgrade Available
VM
VXLANT
Vendor ID

NSX-V IPSet - Configuration Properties

All Parents
Change
Event
IP Address
IP Address
IP Address Range
end
IP Address Range
start
Translated VM
Vendor ID
Network Address

All Direct Child Group
All Parents
Child
Direct Destination RuleSets
Type
Direct Incoming Rules
Direct Outgoing Rules
Direct Source RuleSets
Type Event
Excluded
IP Address
IPSet
Incoming Rule Count
Indirect Destination RuleSets
Type
Indirect Incoming Rule Count
Indirect Incoming Rules
Indirect Outgoing Rules
Indirect Source RuleSets
Type
Manager
Manager Model
Manager Serial
Manager Version
Member
Member
NSX Manager
Name
Outgoing Rule Count
Problem
Region
Rule Count
Security Tag
Translated VM
Vendor
Vendor ID

Problem
Scope
Scope
Tag
Manager
NSX Manager
Name
Netmask
Indirect Incoming
Rules
Indirect Outgoing
Rules
Direct Destination RuleSets
Type Direct Incoming Rules
Direct Outgoing Rules
Direct Parent Security Group
Direct Source RuleSets Type
Indirect Destination RuleSets
Type Indirect Source RuleSets Type

NSX-V Security Group - Configuration Properties

NSX-V Policy Based VPN - Configuration Properties

NSX-V Firewall - Configuration Properties

NSX Manager
Name
Packet Type
Port
Port Range
Port Range Display
Problem
Protocol
Protocol Port Range
Rule ID
Rule Type
Scope
Section ID
Section Name
Security Group
Sequence ID
Service
Service Any
Service Profile
Shared
Source
Source Negate
Source Security Group
Source User
Source Vm
Source Zone
Event
Flow
HIP Profile
IP Address
Status

Manager Version
Manager Serial
Manager Name
Manager
Member
Member
NSX Manager
Name
Outgoing Rule Count
Problem
Region
Rule Count
Security Tag
Translated VM
Vendor
Vendor ID

NSX Manager
Target
Target Negation
Vendor
Vendor
vm series
Indirect Source IPSets
Indirect Source Security Group
Problem
Logging Enabled
Manager
Manager Model
Manager Serial
Manager Version
ACTION
Application
Application ID GUID
Appliedto
Destination Any
Destination Address Group
Destination Any
Destination IP
Destination IPSets
Destination Negate
Destination Security Group
Destination Vm
Destination Zone
Device Group
Direct Destination Address
Direct Destination Address Group
Direct Destination Security Group
Direct Security Group
Direct Source Address Group
Direct Source IPSets
Direct Source Security Group
Direct Vm
Direction
IPSet
Indirect Destination Address
Indirect Destination Address Group
Indirect Destination Security Group
Indirect Security Group
Indirect Source Address
Indirect Source Address Group
Source Address
Source Address Group
Source Any
Source IP
Source IPSets
### SD-WAN™ by VeloCloud® Search Poster

#### Sample Queries

**VeloCloud Link**
- VeloCloud Edge
- VeloCloud Cluster
- VeloCloud Event

**VeloCloud Profile**
- VeloCloud Cluster
- VeloCloud Event

**VeloCloud Segment**
- VeloCloud Enterprise
- VeloCloud Object

**VeloCloud Datasource**
- VeloCloud Enterprise
- SDWAN Application
- SDWAN Edges

**VeloCloud Layer2 Network**
- SDWAN Application
- SDWAN Edges

**VeloCloud Gateway**
- SDWAN Application
- SDWAN Edges

---

<table>
<thead>
<tr>
<th>Total packets, Lost Packet Ratio, Retransmitted Packet Ratio of SDWAN Edge Application where edge = ‘Hillsboro, CA Hub’</th>
</tr>
</thead>
</table>

For more information, refer to the [VeloCloud® Search Poster](https://www.vmware.com/vsphere/overview/#search-poster).

---

**SD-WAN Application - Metrics**
- Change
- Event
- Network
- Profile
- Primary Gateway
- SDWAN Edge
- Segment
- Source Bytes
- Retransmitted Packet Ratio
- Packets
- Lost Packet Ratio
- Destination Bytes
- Bytes Rate
- Bytes
- Link State
- Uptime
- packets
- bytes

**VeloCloud Link - Metrics**
- Link Uptime
- VeloCloud Link State UP
- VeloCloud Bytes Received
- VeloCloud Bytes Sent
- VeloCloud Link Downstream Average Throughput
- VeloCloud Link Downstream Bandwidth
- VeloCloud Link Downstream Jitter
- VeloCloud Link Downstream Latency
- VeloCloud Link Downstream Packet Loss
- VeloCloud Link Transactional Quality Score
- VeloCloud Link Upstream Bandwidth
- VeloCloud Link Upstream Jitter
- VeloCloud Link Upstream Latency
- VeloCloud Link Upstream Packet Loss
- VeloCloud Link Video Quality Score
- VeloCloud Link Voice Quality Score
- VeloCloud Packets Received
- VeloCloud Packets Sent
- VeloCloud Total Bytes
- VeloCloud Total Packets

---

**VeloCloud Edge Application - Metrics**
- Change
- Event
- Name
- Problem
- Vendor ID

---

**VeloCloud Site - Configuration Properties**
- vendorId
- name
- edges
Want to do more with VMware networking?

Try a quick introduction to vRealize Network Insight – Lightening Lab

Save time.
Collaborate more.
Find answers faster.
VMware vRealize Network Insight Cloud