VMware Aria Operations for Networks Search Query Posters

Get Deeper Insights from Your Infrastructure, Faster
Introduction

As a VMware admin, you know VMware Aria Operations for Networks 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 VMware Aria Operations for Networks 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
4. VMware NSX® Data Center for vSphere®
5. 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 VMware Aria Operations for Networks 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

- Aggregated traffic series for matching flows: series( sum( byte rate )) of flows where host = 'myhost.abccorp.com'
- Top VM pair by total bytes: sum(bytes) of flows group by src vm, dest vm order by sum(bytes)
- VTEP traffic grouped by VMKNIC: sum(bytes) of flows where Flow Type = 'Source is VTEP' or Flow Type = 'Destination is VTEP'
- Total VTEP traffic: sum(bytes) of flows where Flow Type = 'Source is VTEP' or Flow Type = 'Destination is VTEP'
- 'Source is VM' and flow type = 'Destination is Internet'
- 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'
- Internet traffic by source VM: sum(bytes) of flows where Flow Type = 'Internet' group by source vm order by count of flow group by Destination IP Address
- Top VM pair by total bytes: sum(bytes) of flows group by src vm, dest vm order by sum(bytes)
- 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)

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

NSX Manager - Configuration Properties

- 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
- 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 Address Group
- Destination Any
- Destination IP
- Destination IPSet
- Destination Negate
- Destination Security Group
- Destination Vm
- Destination Zone
- Device Group
- Direct Destination Address
- Direct Destination Address Group
- Direct Destination IPSet
- Direct Destination Security Group
- Direct Security Group
- Direct Source Address
- Direct Source Address Group
- Direct Source IPSet
- Direct Source Security Group
- Direction
- IPSet
- indirect Destination Address
- indirect Destination Address Group
- indirect Destination IPSet
- indirect Destination Security Group
- indirect Security Group
- a Source Address
- indirect Source Address Group
- Source Address
- Source Address Group
- Source Any
- Source IP
- Source IPSet

NSX Controller - Configuration Properties

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

NSX Manager - Metrics

- Backup Enabled
- Change
- Event
- IP Address
- Model
- NTP Server Configured
- Name
- Problem
- Serial
- Syslog Server Configured
- Transport Zone
- VM
- Vendor
- Version

NSX Policy Firewall - 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
- Member
- NSX Manager
- Name
- Outgoing Rule Count
- Problem
- Region
- Rule Count
- Security Tag
- Translated VM
- Vendor
- Vendor ID

NSX 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
- 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
**PKS - Kubernetes Search Poster**

**Common Queries**

**Search Flows:** flows where Kubernetes Object = Object name

**View the service scale:**
- Kubernetes pods group by Kubernetes Services

**View the node load:**
- Kubernetes Pods group by Kubernetes Node

**View the node health:**
- MemoryPressure and PIDPressure and DiskPressure and
  Ready of Kubernetes Node

- Example:
  - flows from Kubernetes Namespace='Non-PCI' to Kubernetes Namespace='PCI' to Kubernetes Node
  - Kubernetes Object name of the object to
    Kubernetes Object name of the object
  - Example:
    - flows from Kubernetes Namespace='PCI' to Kubernetes
      Namespace='Non-PCI'

**View the Path topology:**
- Kubernetes service service name to Kubernetes service
  service name
- Kubernetes pod pod name to Kubernetes pod pod name

**Kubernetes Objects**

**Nodes:**
- Kubernetes nodes where Ready = 'True'
- Kubernetes node where Virtual Machine = 'vm-a'

**Flows:**
- flows where Kubernetes service is set
  flows where source Kubernetes node = 'a'

**Services:**
- Kubernetes pods where Kubernetes services is not set
- Kubernetes pods group by Kubernetes Services, Kubernetes Cluster

**Namespace:**
- Kubernetes namespace where L2 Networks = 'a'
- list(Kubernetes Node) of Kubernetes Pod where
  Kubernetes Namespace = 'a'

**Packet drops by 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
  ConnectedTo order by max(Rx Packet Drops)

**Packet drops by 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
  ConnectedTo order by order by (Rx Packet Drops)

**Packet drops by group by namespace**
- nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/
  project:' order by Rx Packet Drops

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

**Sample Queries**

<table>
<thead>
<tr>
<th>Common Queries</th>
<th>Supported properties for Configuration Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Flows: flows where Kubernetes Object = Object name</td>
<td>Group by = Ex: Kubernetes pods group by kubernetes services</td>
</tr>
<tr>
<td>View the service scale:</td>
<td>Aggregate Functions</td>
</tr>
<tr>
<td>Kubernetes pods group by Kubernetes Services</td>
<td>max, min, sum, avg</td>
</tr>
<tr>
<td>View the node load:</td>
<td>Ex: sum(MemoryPressure) of kubernetes node</td>
</tr>
<tr>
<td>Kubernetes Pods group by Kubernetes Node</td>
<td></td>
</tr>
<tr>
<td>View the node health:</td>
<td></td>
</tr>
<tr>
<td>MemoryPressure and PIDPressure and DiskPressure and Ready of Kubernetes Node</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>flows from Kubernetes Namespace='Non-PCI' to Kubernetes Namespace='PCI' to Kubernetes Node</td>
<td></td>
</tr>
<tr>
<td>Kubernetes Object name of the object to Kubernetes Object name of the object</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>flows from Kubernetes Namespace='PCI' to Kubernetes Namespace='Non-PCI'</td>
<td></td>
</tr>
<tr>
<td>View the Path topology:</td>
<td></td>
</tr>
<tr>
<td>Kubernetes service service name to Kubernetes service service name</td>
<td></td>
</tr>
<tr>
<td>Kubernetes pod pod name to Kubernetes pod pod name</td>
<td></td>
</tr>
<tr>
<td>Kubernetes pod pod name to Kubernetes pod pod name</td>
<td></td>
</tr>
</tbody>
</table>

**Kubernetes events**

- events where Problem Entity = '<pod/namespace/node Name>'
- events where Event code = 'ImagePullBackOff' in last 24 hours
- events where problem entity.Kubernetes Cluster = '<cluster-a>'

**View Application**

- application where virtual member = 'service-a'
- application where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'
- count of applications where Virtual Member in (kubernetes services)
- list (virtual member) of applications where Name = 'app-1' and virtual member.Kubernetes Cluster is set

**View Tier Information**

- tier where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'
- Flows
  - flows where firewall action = 'DROP' group by Kubernetes Service
  - flows where firewall action = 'DROP' group by source Kubernetes Namespace
  - flows where firewall action = 'DROP' and Flow Type = 'Destination is Internet'

**Packet drops group by 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
  ConnectedTo order by max(Rx Packet Drops)

**Packet drops group by 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
  ConnectedTo order by order by (Rx Packet Drops)

**Packet drops by group by namespace**
- nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/
  project:' order by Rx Packet Drops

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

**Kubernetes Service**

- Annotations Key
- Annotations Key Value
- Change
- Cluster IP
- Cluster IPAddress
- Cluster Netmask
- Cluster Network Address
- Creation Time
- Event
- External IP
- External IPAddresses
- External Netmask
- External Network Address
- Kubernetes Cluster
- Kubernetes Namespace
- Label
- Label Key
- LoadBalancer IP
- LoadBalancer IP Address
- LoadBalancer Netmask
- LoadBalancer Network Address
- Manager
- Name
- Node Condition Status
- Node Condition Status Message
- Node Condition Status Type
- OS Image
- OutOfDisk
- PIDPressure
- Problem
- Ready
- Roles
- Vendor ID
- Virtual Machine
- modelKey

**Kubernetes Node**

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

**Kubernetes Pod**

- Annotations Key
- Annotations Key Value
- Change
- CIF
- Container
- Creation Time
- Event
- HOST
- IP Address
- IPAddress
- Kube-Proxy Version
- Kubelet Version
- Kubernetes Cluster
- Label
- Key
- Logical Port
- Manager
- MemoryPressure
- Name
- Node Condition Status
- Node Condition Status Message
- Node Condition Status Type
- OS Image
- OutOfDisk
- PIDPressure
- Problem
- Ready
- Roles
- Vendor ID
- Virtual Machine
- modelKey

**Kubernetes Data Source**

- Change
- Enabled
- Event
- NI Collector
- NSX Manager
- Problem
- URL

**PKS - Kubernetes Search Poster**

**PKS Data Source**

<table>
<thead>
<tr>
<th>URL</th>
<th>Change</th>
<th>Enabled</th>
<th>Event</th>
<th>NI Collector</th>
<th>NSX Manager</th>
<th>Problem</th>
<th>URL</th>
</tr>
</thead>
</table>

**Configuration Properties**

<table>
<thead>
<tr>
<th>Kubernetes Service Properties</th>
<th>Kubernetes Node Properties</th>
<th>Kubernetes Pod Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annotations Key</td>
<td>Annotations Key Value</td>
<td>Change</td>
</tr>
<tr>
<td>Annotations Key Value</td>
<td>Change</td>
<td>Creation Time</td>
</tr>
<tr>
<td>Change</td>
<td>Event</td>
<td>Kubernetes Cluster</td>
</tr>
<tr>
<td>Kubernetes Cluster</td>
<td>L2 Networks</td>
<td>Label</td>
</tr>
<tr>
<td>Label</td>
<td>Key</td>
<td>Manager</td>
</tr>
<tr>
<td>Manager</td>
<td>Name</td>
<td>Problem</td>
</tr>
<tr>
<td>Problem</td>
<td>Router</td>
<td>Vendor ID</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>modelKey</td>
<td>status</td>
</tr>
</tbody>
</table>

**Kubernetes Cluster**

<table>
<thead>
<tr>
<th>Name</th>
<th>Problem</th>
<th>URL</th>
</tr>
</thead>
</table>

**Pod: NSX-T Logical port where connectedto.modelKey in (modelKey of Kubernetes nodes) order by Tx Packets desc**

<table>
<thead>
<tr>
<th>NSX-T Logical port where connectedto.modelKey in (modelKey of Kubernetes pods) and Rx Packet Drops &gt; 0 new Kubernetes pod in last 1 hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes count</td>
</tr>
</tbody>
</table>

**Kubernetes Objects**

<table>
<thead>
<tr>
<th>Pod</th>
<th>NSX-T Logical port where connectedto.modelKey in (modelKey of Kubernetes nodes) order by Tx Packets desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX-T Logical port where connectedto.modelKey in (modelKey of Kubernetes pods) and Rx Packet Drops &gt; 0 new Kubernetes pod in last 1 hour</td>
<td></td>
</tr>
</tbody>
</table>
### Sample Queries

- **Build your own query**
  - `sum(bytes) of flows group by src vm, dest vm order by sum(bytes)`

- **Top VM pair by total bytes**
  - `flows where Flow Type = 'Source is Internet' and Flow Type = 'Destination is VM' order by bytes`
### VMware NSX® Data Center for vSphere® Search Poster

#### Sample Queries
- **top 10 nsx-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 rule id = 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 90 days
  - Flows hitting specific rule id’s / firewall rules/specific security group/specific application
  - Flow where flow id in (101, 102, 103)
  - Flow where firewall rule like rule1
  - Flow where security group like sg1
  - 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

#### VMware Aria Operations for Networks

---

### NSX-V IPSet - Configuration Properties
<table>
<thead>
<tr>
<th>All Parents</th>
<th>Change</th>
<th>Event</th>
<th>IP Address</th>
<th>IP Address</th>
<th>Region</th>
<th>Scope</th>
<th>Status</th>
<th>Upgrade Available</th>
<th>VXLAN</th>
<th>Vendor ID</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### NSX Manager - Configuration Properties
<table>
<thead>
<tr>
<th>Backup Enabled</th>
<th>Change</th>
<th>Event</th>
<th>IP Address</th>
<th>Model</th>
<th>NTP Server Configured</th>
<th>Name</th>
<th>NSX Manager</th>
<th>Name</th>
<th>Outgoing Rule Count</th>
<th>Problem</th>
<th>Region</th>
<th>Rule Count</th>
<th>Scope</th>
<th>Status</th>
<th>Upgrade Available</th>
<th>VXLAN</th>
<th>Vendor</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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 | Direct Destination RuleSets | Indirect Destination RuleSets Type | Indirect Incoming Rule Count | Indirect Outgoing Rule Count | Indirect Source RuleSets Type | Indirect Source RuleSets Type | Type
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### NSX-V Policy Based VPN - Configuration Properties
<table>
<thead>
<tr>
<th>Change</th>
<th>Event</th>
<th>Local Address</th>
<th>Local Address</th>
<th>Local Endpoints</th>
<th>Local Network</th>
<th>Manager</th>
<th>Peer VPN Connection</th>
<th>Peer VPN Gateway</th>
<th>Peer VPN Session</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### NSX-V Policy Firewall - Configuration Properties
<table>
<thead>
<tr>
<th>Change</th>
<th>Event</th>
<th>Exclusion</th>
<th>Firewall Status</th>
<th>Manager</th>
<th>Model</th>
<th>Name</th>
<th>Published Version</th>
<th>Rule Count</th>
<th>RuleSets Type</th>
<th>Rules</th>
<th>Serial</th>
<th>Spoofguard</th>
<th>Status</th>
<th>Source</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Want to do more with VMware networking?

Try a quick introduction to VMware Aria Operations for Networks – Lightening Lab

Save time.
Collaborate more.
Find answers faster.

VMware Aria Operations for Networks