

# vRealize Network Insight 4.2 Release Notes

vRealize Network Insight 4.2 | 18 JUL 2019 | Build 1562947515

Check for additions and updates to these release notes.

## What's in the Release Notes

The release notes cover the following topics:

- [What's New](#)
- [Product Upgrade](#)
- [Documentation](#)
- [VMware Product Compatibility](#)
- [VMware MIB Files](#)
- [Resolved Issues](#)
- [Known Issues](#)

## What's New

Here are the key features and capabilities of vRealize Network Insight 4.2:

### Application Discovery and Visibility

- Application Discovery
  - REGEX Builder to detect patterns, Save/Edit templates of the discovery configurations, Bulk-Save of discovered applications.
- Application Dashboard
  - Zoom-In to visualize more members (VMs, Physical IPs, and Kubernetes Services) and connections between them.
  - Visualize tiers by type: vCenter, Kubernetes, VMware Cloud on AWS.
  - View and filter unprotected flows .
  - 'What's New' section to identify changes to this application in the last 24 Hrs.

### VMware NSX Data Center

- NSX-V
  - Support for Flow Round Trip Time (RTT) and Virtual Infrastructure Latency (vNIC-pNIC, pNIC-vNIC, vNIC-vNIC and VTEP-VTEP)
  - Edge Load Balancer (LB) support
    - LB configuration and metrics
    - VM/IP to VM path with LB
- NSX-T
  - Identify users who made the changes (CREATE, UPDATE) and show on the timeline
  - Policy Manager: Link Policy Info to NSGroup, IPSet, L2 Network, Firewall Rule
- VM-VM underlay topology improvements
  - Simplified numbering , details on entity click

Number tooltip on entity hover, group numbering when entity numbers are grouped, and a path through PNIC context

- Complete VM-VM path when NSX Edge configured with trunk interface.

## Third-Party Device Support

- Fortinet Firewall support through FortiManager.
- User Assisted Network Information Framework (UANI) SDK: UANI allows the addition of third-party devices which are not supported natively in vRealize Network Insight.

## Container Visibility and Security

- Support for Red Hat OpenShift version 3.11 and below
- Support for defining applications using Kubernetes constructs such as Kubernetes Service Name and Namespace

## Public Cloud - AWS, VMware Cloud on AWS

- Support for AWS instance type, EC2 subnets, and region property
- AWS Security Group change tracking
- UX/UI enhancements for VMware Cloud on AWS data source page

## Other Enhancements

- Pinboards: More intuitive and readily noticeable **Edit** and **Share** options. Easy pin, drag and move option with a prominent visual indicator, inline edit for the title and description field.
- Analytics:
  - Detect abnormal flows using Flow RTT in the 'Flow Insights' dashboard
  - Auto-enable 'Dynamic Baseline' analytics during Application Definition
  - New scope of Applications in the Threshold Configuration page
- Plan Security Micro-segmentation:
  - Guidance to identify flow links between wedges
  - IPset/IP address included when recommended Firewall rules are exported .csv format
- One-click support bundle creation.

## Product Upgrade

vRealize Network Insight 4.2 supports a direct upgrade from the 4.1.1, 4.1 and 4.0 versions.

Refer to the [Upgrading vRealize Network Insight](#) section for more information on upgrade options.

The upgrade path is available at

[https://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php#upgrade&solution=285](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#upgrade&solution=285).

## Documentation

For additional information about new features, see the vRealize Network Insight documentation.

- [Installing vRealize Network Insight](#)
- [Using vRealize Network Insight](#)
- [vRealize Network Insight FAQs](#)
- [vRealize Network Insight Command Line Interface Guide](#)
- [vRealize Network Insight API Guide](#)

## VMware Product Compatibility

The [VMware Product Interoperability Matrix](#) provides details about the compatibility of vRealize Network Insight with other VMware products.

## VMware MIB Files

For MIB information, see [Determining the MIB module listing, name, and type of an SNMP OID](#). You can download the SNMP MIB module file from the [1013445 KB](#) article.

## Resolved Issues

- When the count of VMs associated to a firewall rule's source or destination gets updated from a non-zero value to zero, and if you run firewall rule query with source VM or destination VM as a filter, it might give an incorrect result.
- vRealize Network Insight does not detach the NSX-T logical ports from the unhealthy pods or nodes.
- If OpenID Connect (OIDC) authenticator is used for PKS, then contact VMware Support. OIDC is supported for PKS in vRealize Network Insight 4.2.
- You can not edit or delete an empty application.
- **vRealize Network Insight incorrectly applied firewall rules including NSX DFW orphaned rules.**
  - Though the `Applied To` field does not exist for a firewall rule (for example, logical port), the rule is still shown as applied to VMs on the same NSX-T Manager.
  - The VM dashboard does not consider the owning NSX Manager or the `Applied To` fields and does not display the actual applied rules.
- **Unable to add F5 as a data source using AD authentication.**

You see the following messages:

  - `No access to shell. Please use tmsh or advanced shell`
  - `Data Source is not reachable from Proxy VM`
- After upgrade, you see the following error message:

```
Indexer Service - Recent data is not being indexed due to null. Search results can be inaccurate
```
- `crontab` is not set with the `source` argument in the web proxy code.
- Though Edge Services Gateway (ESG) has an uplink interface, you see the following message:

```
NSX DLR deployed without an uplink interface
```
- The CPU utilization is high on platform VMs.
- The fabric extenders (*FEX*) that were removed are still visible on switches in vRealize Network Insight.
- `EsRejectedExceptions` appears in indexer logs on a [LARGE] brick single node setups.
- In a multiple container setup, elastic search restarts frequently and results in the out of memory error.
- The VM snapshot count in vRealize Network Insight does not match the count in vCenter Server.
- After you delete the LDAP auth source for the users, you cannot add the vIDM auth source.

# Known Issues

- **[NEW]** If you update the NSX-T password after you add it as a data source in vRealize Network Insight, you see the `Invalid credentials` error.

Update the password after 15 minutes of disabling the NSX-T data source.

- **[NEW]** Though you delete the application, you see the protection status of the application on the map view.
- **[NEW]** The pods that are deleted in the Kubernetes cluster might be visible in vRealize Network Insight.
- **[NEW]** In the VM-VM path, NSX-T Edge firewall drop rule is not populated under T0 router.
- **[NEW]** When you re-enable the IPFIX on NSX-T, the firewall IPFIX profile is not created.
- **[NEW]** NSX-T security group does not display the direct rules and its count.
- When you search for Kubernetes Nodes in vRealize Network Insight, the search result displays the list of Master Nodes for native Kubernetes cluster and not for VMware PKS.
- In the absence of a firewall rule on a VM, default connectivity strategy applies to a VM in VMC. In such cases, the firewall icon is not present in the VM-VM path on the VMC side as we do not get enough information about the realization of the default rule from the VMC SDDC.
- When you attempt to export a pinboard in which the pinboard name contains a Non-ASCII character, vRealize Network Insight shows the incorrect filename on the Export to PDF window.
- When you add a filter in the query result, the count shown in the filter is approximate.
- If the Native Kubernetes cluster uses kubeconfig that does not contain static service account tokens, then the addition of Kubernetes data source fails.

Contact VMware Support.

- When you set the home page from **My Preferences**, it requires a page refresh to reflect that information in UI.
- When you attempt to add a Cisco ASA data source, you see a message to contact support with the following error:

```
Message missing required fields: vendorId
```

- The auto-refresh counter restarts and keeps showing incorrect data even though auto-refresh is paused.
- An unwanted default rule is applied to certain NSX IPFIX flows because sometimes, NSX IPFIX reports a reverse packet in which client and server are flipped and the firewall rule is applied as per the flipped source and destination IP.
- The Export to PDF feature for the PCI dashboard has the following known issues:
  - The changes that you make in the NetFlow flow diagram dashboard are not visible in the PDF.
  - For a particular widget, the number of properties that are exported as PDF is more than the number of properties that are selected in that widget.

- The non-ASCII characters are not being exported correctly to the PDF. The workaround for this issue is to run the `sudo apt-get install fonts-wqy-zenhei` command on the vRealize Network Insight server to install the additional fonts.
- The metric properties are not exported in the PDF.
  
- When you create a logical subnet or logical router, a new edge VM is dynamically created to serve this request. The events for this kind of VM are shown.
  
- The Plan Security page for the last two days takes around 3 minutes to load. A higher response time is seen while running the queries for about 24 hours after migration of a data source between collectors. This is because the same flows are reported, opened, and closed from two different collectors within a span of 24 hours. It leads to multiple versions created for the same flows.
  
- The firewall rule section of the PCI Compliance dashboard can show incorrect rules if the selected scope is a nested security group in NSX or an application when multiple NSX managers are added as a data source.
  
- The plan topology widget has options to select all flows, all protected flows, and so on. The flows that are solely captured from VDS and not from NSX IPFIX only show up when the **all flows** option is selected because their protection status is classified as unknown not as protected or unprotected.
  
- Some events such as **Host network control plane mismatch** are not raised if the data center is not at the top level and is located inside a folder in vCenter.
  
- There is a known issue in the list view for events search where sometimes facet counts are incorrect upon selection and no events are shown.