



vRealize Network Insight 5.0 Release Notes

vRealize Network Insight 5.0 | 19 SEP 2019 | Build 1568279774

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 5.0:

VMware SD-WAN Support

- VMware SD-WAN™ by VeloCloud® support for end-end network/application monitoring, troubleshooting, analytics
- Uber Enterprise Dashboard with map view
- Site/Edge, App Dashboards and Analysis
- Site/Edge Topology for LAN and WAN visibility
- VMware SD-WAN Flow Analysis that includes traffic, latency and retransmit counts
- Top Performance Dashboards for VMware SD-WAN Infra and Apps
- End-to-End VM/IP to VM/IP Path visibility and hotspots

Public Cloud

- Azure support for security planning, flow analysis and single pane of glass visibility
 - Azure entities part of application discovery & security planning
 - Flow analysis: Intra and inter VNET flows, NSG-flow mapping, NSG recommendation
 - Azure entities first class citizen of search
 - Analytics: Top talkers, Elephant flows, Outliers (Application Tiers & ASG), Threshold (Azure VMs and Flows)
 - Dashboards: Azure Overview, Azure subscription, ASG, NSG, Subnet, VM, VNET

- APIs: Create, Update & Delete Azure data source
- Addition of VMware Cloud on AWS Bird's Eye View dashboard

Application Discovery and Visibility

- Support for Azure VMs in App Discovery and definitions
- 'Custom Search' support for Kubernetes entities when creating Application tiers
- Dashboard optimizations for improved responsiveness and load times

Kubernetes Environment

- Network path tracing for Kubernetes Services and pods

Third-Party Device Support

- Support Streaming Telemetry for Dell OS10 Switches (S5200, release 10.4/5.x of OS10)
 - Integrated Buffer Statistics and Tracking (BST)
 - Metrics supported: Peak buffer utilization (percentage) for per-port egress unicast queues (only for TOR downlink port)
 - Supported for application troubleshooting and VM-VM path topology

NSX-T

- VTEP-VTEP Latency metric support (for v2.5 and above) and display in Host and Transport Node dashboards
- PCI compliance Dashboard

Other Enhancements

- Updated the search query that appears below the search, based on the filters selected to refine the original search
- Ability to sort search results from the UI without updating the search query.
- Ability to search within the micro-segmentation donut
- Identify users who made the changes in NSX-T Manager and show in a timeline
- vRealize Suite Life Cycle Manager 2.1 Product Support Pack 4 supports the installation of vRealize Network Insight 5.0. See [VMware vRealize Suite Lifecycle Manager 2.1 Release Notes](#). For information about install and upgrade Network Insight by using vRealize Suite Lifecycle Manager, see the [vRealize Suite Lifecycle Manager Installation, Upgrade, and Management Guide](#).

Serviceability

- Health grid for monitoring and reporting key system parameters

Localization Support

- vRealize Network Insight 5.0 is available in the following languages:
 - English
 - French

- German
- Japanese
- Korean
- Spanish
- Simplified Chinese
- Traditional Chinese

Note: The following items are not considered for localization:

- The enumerated values used in the facets
- Search Queries
- The exported CSV and PDF report files
- The email subject and content
- Time controls for search
- Event tags
- The PCI Compliance Page

Product Upgrade

vRealize Network Insight 5.0 supports a direct upgrade from the 4.2, 4.1.1, and 4.1 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.

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](#)

Note: As you use the vRealize Network Insight documentation, we want you to know that we value inclusion at VMware. To foster this principle within our customer, partner, and internal community, we have updated some terminology in our documentation.

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

- 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.
- The pods that are deleted in the Kubernetes cluster might be visible in vRealize Network Insight.
- NSX-T security group does not display the direct rules and its count.
- The data retention (Config Store Maintenance) service is unhealthy even after running the java query for cleaning flows.
- When you attempt to export flow data to CSV format, Realize Network Insight displays the HTTP 500 Internal Server Error .
- You see a huge flow count and network traffic rates and also incorrect source and Destination details on vRealize Network Insight.
- You see an empty rule ID under Applied Firewall Rules for NSX T flows.
- You see the Platform Health: Data Source Failed error regularly for NSX-T.
- When you attempt to edit a collector setting, you see Error: Selected Collector VM is not responding. Collector VM should be running and reachable from Platform.
- When you click the information icons on the VM Topology page to view the additional information, you see a blank space.
- You see an incorrect data about BGP state and remote AS in vRealize Network Insight.
- You could not add Arista switches to vRealize Network Insight.
- vRealize Network Insight fails during the cipher scan.
- Flows are not closed in vRealize Network Insight.
- The flow processor stops responding periodically.
- The Check Point access rule collection is limited to 50 per access layer. So, when you search for Check Point Access Rule , you do not see the complete list of access rules in vRealize Network Insight.

Known Issues

- **[NEW]** If you are using NSX-V versions 6.4.5 or 6.4.6, do not enable Virtual Infrastructure Latency on the NSX Manager data source. The NSX-V prepared ESX hosts may observe Purple Screen of Death (**PSOD**) in certain conditions. For more information, see

the [75224 KB article](#).

Note: There is no impact to NSX-T versions.

- **[NEW]** When the Online Upgrade UI notification is available, you could not perform the Offline upgrade.
- **[NEW]** vRealize Network Insight 5.0 supports the addition of following switches in the hmac-sha1-96, hmac-sha1, hmac-md5-96, hmac-md5 SSH authentication modes only.
 - Nexus 5k
 - Dell Z9100, Dell OS10 and Dell Force10 S6k
 - Cisco ASA and Cisco ASR/ISR
 - Catalyst 4500
 - Arista
 - Huawei
 - Brocade MLX series
- **[NEW]** vRealize Network Insight does not collect the route information of the Check Point data source, which results in missing VM paths details.
- **[NEW]** In a cluster setup, when you search for the NSX Firewall Rules with the Firewall Rule Masked Event, vRealize Network Insight incorrectly lists the Distributed firewall rule masked by preceding rule event in the search result.
- **[NEW]** The Path Topology does not display the DFW firewall for Kubernetes entities.
- **[NEW]** If you have upgraded the collector from 4.2 to 5.0, the VMware SD-WAN flow processing does not trigger automatically.

Add a vCenter on the same collector before you send the VMware SD-WAN flows.

Note: You can remove the vCenter later.

- **[NEW]** The facet filter does not work in non-English language.
- **[NEW]** The event severity icons are not displayed in non-English language.
- **[NEW]** The edit event by non-English user permanently changes the event title and the severity for all users
- **[NEW]** AWS primary link account might not work in non-English locale.
- **[NEW]** VMware Cloud on AWS 1.9 is not supported in vRealize Network Insight 5.0. If you have upgraded VMware Cloud on AWS from 1.8 to 1.9 version, you might see the flows twice on the UI.
- **[NEW]** The Dell switch running version 9.14.2.0 crashes when vRealize Network Insight runs the show interfaces command on it to collect configuration information.

Workaround: Disable data collection on Dell switches running 9.14.2.0 and upgrade it to 9.14.2.1 and resume the data collection.

- Though you delete the application, you see the protection status of the application on the map view.
- In the VM-VM path, NSX-T Edge firewall drop rule is not populated under the T0 router.
- When you re-enable the IPFIX on NSX-T, the firewall IPFIX profile is not created.
- When you search for Kubernetes Nodes in vRealize Network Insight, the search result displays the list of primary nodes for the native Kubernetes cluster and not for VMware PKS.
- 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

- 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.
- 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 the events search where sometimes facet counts are incorrect upon selection and no events are shown.
- 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.

- 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.
- 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 auto-refresh counter restarts and keeps showing incorrect data even though auto-refresh is paused.
- 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.