

# vRealize Network Insight 3.8 Release Notes

**Last Updated on:** 06 DECEMBER 2018

vRealize Network Insight 3.8 | 19 JUNE 2018 | Build 1528874037

Check regularly for additions and updates to these release notes.

**Alert!** Apply the [vRealize Network Insight Patch for Chrome 71 Support](#) on all the platforms that have vRealize Network Insight 3.8. For more information, see [KB 60368](#).

The release notes cover the following topics:

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

## What's New

Here are the key features and capabilities of vRealize Network Insight 3.8:

### Cisco ASA Series Support

You can add Cisco ASA series as a data source in vRealize Network Insight. In this release, vRealize Network Insight supports the following features for the Cisco ASA series:

- Cisco ASA-X series only
- Routed mode and L2 bridging mode only
- Cisco ASA operating system version 9.4 only

In this release, vRealize Network Insight does not support the following features for the Cisco ASA series:

- Clustered deployment of Cisco ASA
- High availability feature of Cisco ASA

### Integration of vRealize Network Insight and vRealize Log Insight

In the vRealize Network Insight-vRealize Log Insight integration, the alerts generated by vRealize Log Insight are consumed by vRealize Network Insight. The integration supports the CRUD-related alerts corresponding to the NSX security groups only. When the NSX security group is created or modified, the logs of NSX reflect these changes. When these logs are sent to vRealize Log Insight, it sends an alert to vRealize Network Insight, which further fetches the latest data for the changed security group from the NSX manager.

### Analytics for Outlier Detection

vRealize Network Insight offers analytics based on the flow based metrics defined over the VMs and physical IP addresses. Through outlier detection, vRealize Network Insight enables you to detect a particular

VM experiencing very different traffic pattern compared to other VMs/IPs in the group. For example, a VM sends or receives much higher/lower traffic compared to the rest of the group. Such a VM is categorized as an outlier.

## **User-Defined Preferences**

This feature enables an admin user to modify the idle session timeout duration on the UI.

## **NSX Edge Data Collection Changes**

When you add a NSX data source, you can enable the automatic edge data collection. In the previous releases, the edge data collection was done either by NSX Central CLI or Edge-SSH session. From this release onwards, the edge data collection is done by NSX Central CLI and no edge data providers are created under NSX Manager.

## **Enforcing Limits on the Number of Flows**

From this release onwards, vRealize Network Insight enforces the limits on the number of the flows processed for the platform as well as the collector. The limits are enforced by stopping the processing flow data. Also, visibility has been provided into the flow processing load in terms of flow count at the NetFlow reporter, datasource, platform, and collector level.

## **AWS Enhancements**

The support for the following properties of the AWS availability zones have been added:

- AWS Availability Zone property for AWS Instance and AWS VPC
- AWS Availability Zone in search queries, group by/ order by clauses
- AWS Availability Zone filter

The AWS instance or AWS VM has been renamed to AWS EC2.

The AWS manager has been renamed to AWS account.

## **Palo Alto Networks Panorama Enhancements**

- vRealize Network Insight captures the Palo Alto Networks Panorama policies to be displayed in VM to VM path when hierarchical device group is configured. At a given device group level, some policies are defined at the device group level and apart from that there are policies which are inherited from the ancestor device groups.
- Multiple service definitions are supported.

## **Recommended Firewall Rules**

The recommended firewall rules are separated into virtual and physical rules.

The following information for the recommended firewall rules has been added:

- Members (VM and non-VM IP Endpoints) of the source and the destination of a recommended rule
- Flows that are related to a recommended rule

## **Support for Online Upgrade of Cluster**

You can perform the online upgrade for clustered deployment in addition to the single node setup and air-gap collectors. Ensure that all the platform nodes are able to access the vRealize Network Insight upgrade server.

## **New and Improved Installation Workflow**

A new, secure, and improved installation workflow has been introduced for vRealize Network Insight. Refer [vRealize Network Installation Guide](#) for the workflow details.

## NSX Health Check

The following NSX health check has been added:

- VDR Port not set for Distributed Virtual Switch fault check

## Visibility of Health Information

A few configurational parameters have been added to the vRealize Network Insight health dashboards.

## Support for vRealize Suite LCM

You can also install vRealize Network Insight by using vRealize Suite Life Cycle Manager (LCM). For more information, see the [vRealize Suite Lifecycle Manager Installation, Upgrade, and Management](#) guide.

## Documentation

The following documentation is available at [vRealize Network Insight Information Center](#):

- [vRealize Network Installation Guide](#)
- [vRealize Network Insight User Guide](#)
- [vRealize Network Insight Command-Line Interface Reference Guide](#)
- [vRealize Network Insight Frequently Asked Questions](#)
- [vRealize Network API Documentation](#)

## Product Upgrade

vRealize Network Insight 3.8 supports direct upgrade from the 3.7 and 3.6 versions.

Refer to the [Upgrading vRealize Network Insight](#) section to get 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).

## Resolved Issues

The resolved issues for vRealize Network Insight 3.8 are as follows:

- The CPU usage is high on the NSX Controller after creating more than 250 logical switches.
- The **ClusterBasedJobCoordinator** service does not run alerts in a 3-node cluster setup in vRealize Network Insight.
- The upload of the upgrade bundle may fail due to timeout during extraction because of heavy compute load on the platform node.
- The **Security Group Membership Change** and the **Firewall Membership Change** events do not work.
- On the Home page, when you click **All Security Groups**, a search page comes up with the **security groups by translated vm count** query.
- The **appliedTo** field of the firewall rule does not support DVPG.

# Known Issues

The known issues and limitations for vRealize Network Insight 3.8 are as follows:

- **[New]** The UI of vRealize Network Insight 3.8 is not accessible from Chrome version 71. Apply the [vRealize Network Insight Patch for Chrome 71 Support](#) on all the platforms that have vRealize Network Insight 3.8. For more information, see [KB 60368](#).
- **[New]** vRealize Network Insight 3.8 may cause NSX controller nodes to run out of memory leading to VM connectivity loss. See [KB 57311](#) for symptoms and workaround. Download the vRealize Network Insight patch file `vRealizeNetworkInsight-3.8.0-P4-201808101430.bundle` from the [VMware vRealize Network Insight 3.8.0](#) download page.
- The disk may run out of space for the vRealize Network Insight Platform VM. In large environments, the partition `/var` may become full and additional storage may be needed. See <https://kb.vmware.com/s/article/53550> for instructions on how to increase disk space.
- The vRealize Network UI is not available when the partition `/var` is more than 85% full in the Platform VM. For validation and fix, contact VMware support.
- An unwanted default rule is applied to certain NSX IPFIX flows. This is because sometimes, NSX IPFIX reports 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 CSV feature for the flow data takes more than 30 minutes for 180,000 flows when all the fields are selected.
- The Export to PDF feature for the PCI dashboard has the following known issues:
  - The order of events in the dashboard is different than the order in the PDF.
  - 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 actually selected in that widget.
  - The unicode characters are not getting exported correctly to the PDF.
  - 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.
- If issues such as upload failure or UI failure come up while performing the centralized upgrade, please contact VMware support.
- The Plan Security page for the last 2 days takes around 3 minutes to load. A higher response time is seen while executing queries for about 24 hours after migration of a datasource 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.
- Sometimes, the Export to CSV feature fails with the 502 error in the browser. The workaround is to retry the operation.
- vRealize Network Insight does not support rollback or product downgrade. It is recommended that you take a backup.
- The datastore metrics of a VM are not shown on vRealize Network Insight if it is hosted on vSAN Datastore.
- If the vCenter and the associated NSX manager data sources are not attached to the same proxy server, you will not see the denied flows (when NSX IPFIX is enabled) and the **Applied Firewall Rule** will be missing in some flows.
- The NAT rules on the NSX Edge version 5.5 or the previous versions are not supported.
- The firewall rule section of the PCI Compliance dashboard may 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 sub-interfaces on VRF for Cisco Nexus 7000/9000 are not supported.
- In the **Applied To grouping** criteria, the NSX edge is not supported.
- The platform cluster does not support the high availability configuration. All the platform nodes need to be up and running for the cluster to work at optimal performance levels.
- The recommended firewall rules support only global rules creation. The creation of universal rules is not supported.
- 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 as CSV** option is not supported for advanced searches that use **group by**, **sum**, **max**, and **min** functionality.
- Some events such as **Host network control plane mismatch** are not raised if the datacenter is not at the top level and is located inside a folder in vCenter.
- The product update notifications are supported only for the single-platform node deployment that is connected to Internet.
- 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.
- vRealize Network Insight shows the older version after the upgrade. Once the product upgrade is complete, refresh the browser after clearing the browser cache.
- Upon the expiry of the Evaluation license, the data providers are disabled and they stop collecting data. After renewing the license, the data providers must be enabled again from the UI to start data collection.
- To use Gmail® server as the choice of mail server, additional configuration settings as listed on <https://support.google.com/accounts/answer/6010255?hl=en> are required.
- After you remove a data source from the system, you can add the same data provider back only after two or more hours.
- The support bundle creation on a medium sized system can take in excess of fifteen minutes.

## 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.