

VMware vRealize Network Insight 3.4 Release Notes

vRealize Network Insight 3.4 | 01 JUNE 2017 | Build 1495004044

Check regularly for additions and updates to these release notes.

Last updated on 17 JULY 2017

The release notes cover the following topics:

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

What's New

The new and enhanced features in this release are as follows:

- **AWS Public Cloud Support**
vRealize Network Insight now provides visibility into native AWS constructs such as VPC, VM, Security Group, and Firewall rules. Traffic flows are also analyzed to provide security and micro-segmentation view of cloud workloads (Enterprise edition only).
- **Configurable Data Retention**
vRealize Network Insight provides ability to modify the data retention periods for problem events, configuration changes, and metrics (Enterprise edition only).
- **Support for Physical Devices in Application Modeling**
vRealize Network Insight now allows the inclusion of physical servers in application tier definition and micro-segmentation planning.
- **New NSX Operation Events**
Additional NSX operations alerts have been introduced in this release.
- **Customization of Alerts**
The customization is done through global macro settings as well as at individual alerts level.
- **Support of vCenter Tags and Annotations**
It is an additional way to group virtual machines into security and application groups.
- **Visibility of Physical Layer-2 Network**
From this release onwards, the layer-2 networks are visible in the VM-to-VM path dashboard.
- **Addition of Syslog Messages**
vRealize Network Insight supports syslog messages for sending the events generated by the system to external log management products (including Log Insight).

Documentation

vRealize Network Insight 3.4 includes the following product documentation.

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

Product Upgrade

The upgrade to vRealize Network Insight 3.4 is allowed only from version 3.3.

Refer to KB article at <https://kb.vmware.com/kb/2150310> to get information on upgrade options.

NOTE: The access to the following URLs and ports need to be allowed from this release:

Service	URL	Port
Upgrade Service/Metric Service	svc.ni.vmware.com	443
Log Service	log.ni.vmware.com	443
Support Tunnel Service	support2.ni.vmware.com	443
Registration Service	reg.ni.vmware.com	443

Resolved Issues

- The patch at <https://kb.vmware.com/kb/2150738> provides resolution to the following issues:
 - The export of the firewall rules to CSV does not contain proper service fields.
 - The VM underlay topology does not load when VM to IP path query is executed.
- The password for UI local users can be changed by using the `modify-password` CLI.
- The offline upgrade and patch bundles can be directly copied to the appliance VMs by using secure copy utility (`scp/pscp`).
- The patch bundles can be directly downloaded from URL on the appliance VMs by using CLI.
- Sometimes, the online product update would hang or freeze. This issue has been resolved.

Known Issues

The known issues and limitations for vRealize Network Insight 3.4 are as follows:

- The universal IPsets are not correctly annotated on the VMs and physical IPs in the flows of VMs associated with the secondary NSX manager.
- vRealize Network Insight 3.4 does not support the rollback or product downgrade. It is recommended that you take a snapshot.
- The NAT rules on NSX Edge version 5.5 or the previous versions are not supported.
- 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 high availability (HA) configuration. All the platform nodes need to be up and running for the cluster to work at optimal performance levels.
- The LDAP feature does not support restricting group access based on the Active Directory Primary Group.
- The recommended firewall rules support only global rules creation. The universal rules creation is

not supported.

- The export as CSV 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 NSX Manager data provider requires **Enterprise** role. If the central CLI is enabled, then the system admin user credentials are required for the NSX Manager data provider.
- You must enable the NSX central CLI in the **Settings** page to get visibility into NSX NAT settings.
- The product update notifications are supported only for single-platform node deployment that is connected to internet.
- There is a known issue in events search list view where sometimes facet counts are incorrect upon selection and no events are shown.
- vRealize Network Insight shows the older version after the upgrade. The browser needs to be refreshed after clearing the browser cache once the product upgrade is complete.
- Upon Evaluation license expiry, the data providers are disabled and stop collecting data. After renewing 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.
- The export to CSV feature can export a maximum of 20,000 rows.
- Once a data provider is removed from the system, the same data provider can be added back only after two or more hours.
- The support bundle creation on a medium sized system can take in excess of fifteen minutes.
- When the number of distinct 4-tuple flows exceeds 3 million within 24 hours, the processing of flow data on Proxy VM is paused. It resumes only when number of active flows in the system are less than this limit. To reduce the number of flows, remove some of the vCenter data sources or disable IPFIX on some of the DVSSs.

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 at <http://kb.vmware.com/kb/1013445>.

[Top of Page](#)