vRealize Network Insight 5.1 Release Notes

vRealize Network Insight 5.1 | 14 JAN 2020 | Build 1578493419

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

Here are the key features and capabilities of vRealize Network Insight 5.1:

VMware SD-WAN by VeloCloud®

- Analytics support for VMware SD-WAN: Support Threshold-based Analytics for various metrics for VMware SD-WAN entities including Edge, Link, and Edge-Application.
- Pre-SD-WAN assessment report:
  - WAN Uplink/downlink assessment of non-SD-WAN (Cisco ASR/ISR) deployment.
  - Generate a report (as pdf) which includes ROI computation, savings, and recommendations if a customer decides to deploy the VeloCloud SD-WAN solution.
  - The report also includes traffic visibility of the current WAN deployments.

Application Discovery and Troubleshooting

- Discover applications using a new 'Advanced' mode, that supports NSX Security Tag and Security Groups. Also, you can combine multiple discovery methods, using the **Advanced** tab. For example, use name convention for the application name and use the tag for tier name.
- Summary Panel: View a summary of key application-related information (events, flow count, health, incoming/outgoing traffic, countries accessing the application, member

count, etc.) at the top of the application dashboard.
- Troubleshoot Application: Filter and troubleshoot
  - Degraded Flows: Flows experiencing abnormal latencies.
  - Unprotected Flows: Flows that are not protected by any NSX firewall rules.

VMware NSX-T™

- NSX-T Manager topology and dashboard to give you quick insights into your NSX-T deployment
- Support for new out of the box NSX-T events. SeeNSX-T Events and System Events.
- Monitor BGP status on your NSX-T deployments

VMware Cloud™ on AWS

- VMware Cloud on AWS dashboard enhancements
  - VMware Cloud on AWS SDDC object introduced as a part of vRealize Network Insight search and VMware Cloud on AWS dashboard
  - VMware Cloud on AWS SDDC list view with enriched metadata
  - New entities added to VMware Cloud on AWS SDDC dashboard - VMware Cloud on AWS SDDC overview, Network Traffic and Events, Top Talkers, VM, and Host limit-based alerts
- VMware Cloud on AWS Edge Gateway Firewall rule visibility
- Proactive alerting in VMware Cloud on AWS
  - Maximum number of VMs in SDDC
  - Maximum number of Hosts in SDDC

Containers

- Kubernetes Service topology and dashboard to give you quick insights into your Kubernetes Services
- New out of the box Kubernetes events

Other Enhancements

- 3rd Party: Support for Arista HW VTEP in VM-VM path
- 3rd Party: Support for VM-VM Path topologies using L3 NAT (with Fortinet)
- Support for up to 4 SNMP trap targets.
- Operate in an air-gapped network without Internet connectivity
- Patch vRealize Network Insight from UI
- To distribute configuration data across datastores in the cluster, vRealize Network Insight 5.1 replaces PostgreSQL with Foundation DB for storing the configuration data. For additional benefits, see Upgrading vRealize Network Insight. Note that the migration happens as a part of vRealize Network Insight upgrade process. So, the upgrade time might be longer. You can see the tentative upgrade time on the UI when you start the upgrade process. For more information, see Upgrading vRealize Network Insight.
- Simplified *support* and *consoleuser* default password.
- vRealize Suite Lifecycle Manager 8.0.1 Patch 1 supports the installation of vRealize Network Insight 5.1. See VMware vRealize Suite Lifecycle Manager 8.0.1 Patch 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.

Product Upgrade

vRealize Network Insight 5.1 supports a direct upgrade from the 5.0 and 4.2 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

- In the VM-VM path, NSX-T Edge firewall drop rule is not populated under the T0 router.
- 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.
- The Path Topology does not display the DFW firewall for Kubernetes entities.
- The event severity icons are not displayed in non-English language.

- The edit event by non-English user permanently changes the event title and the severity for all users
- AWS primary link account might not work in non-English locale.
- When you run a query without **where** condition to return the flow count over 4 days, vRealize Network Insight displays the correct result, instead of an error message even if the count exceeds 10M.
- The Nexus5K page shows information about the port 1/1 only. You cannot see any traffic in that port or traffic through the switch.and you cannot see these switches in the VM-VM L2 path.
- vRealize Network Insight network operations agent (netopa) collector is crashing due to memory overflow with 4k tunnels on each host.
- After upgrading to vRealize Network Insight 5.0, you see the data source error on the UI: Something went wrong. Please contact support.
- After you upgrade NSXT 2.4 to NSX-T 2.5, vRealize Network Insight proxy is unable to communicate with the NSX-T. You see the following error message: Data Source is not reachable from Proxy VM.
- While adding the PAN 9.x data source into vRealize Network Insight 5.0, you see the Insufficient Credentials error.
- CLI tool is vulnerable to Command Injection.
- When you use double quotes in the Pinboard Name field, you see the 500 error.
- When logging in to vRealize Network Insight through SSH as a `consoleuser` user, the Python script does not sufficiently validate user input, which accepts certain unsupported strings and encounters an error to terminate prematurely.
- The columns are reversed when you export data in the CSV format without a template.
- When you use a too large search criteria and attempt to export the flow details in the CSV format, the option is not accessible.
- The VAPI health status is going to YELLOW repeatedly with the following endpoint warning:

  HTTP response with status code 429
- Unexpected positive alerts appear on vRealize Network Insight.
- Even after the flow processing is complete, vRealize Network Insight does not display the expected flow information.
- vRealize Network Insight does not display NSX-T VIB data of certain ESXi hosts.
- vRealize Network Insight shows that the communication with F5 is failing while adding the

datasource.

- The denorm objects are not created or deleted for F5 and VMware NSX® Manager™.
- Though there is no issue in the data center, certain events (for example,Logical switch table mismatched between host and NSX Controller) are not closed automatically.

Known Issues

- **[NEW]** The **Path to internet** fails to populate when you use VMware Cloud on AWS 1.12 with vRealize Network Insight.

  To avoid or fix the issue, see the 80359 KB article.

- **[NEW]** If the PKS data source password contains special characters like&,(,),|,<,>,`, then vRealize Network Insight does not fetch Kubernetes clusters.
- **[NEW]** During license calculation, vRealize Network Insight incorrectly considers the vSAN Witness Appliances and HCX Mobility Agent as hosts.
- **[NEW]** With the release of vSphere 7.0 and NSX-T 3.0, some vRealize Network Insight features might stop to work in the 5.1 and 5.2 versions due to WCP (Workload Control Plane) and C-VDS. For more information, see the 78492 KB article.

  Workaround:

- When upgrading from 4.2 version, if the Online Upgrade UI notification is available, you could not perform the Offline upgrade.
- **[NEW]** The NSX-V prepared ESX hosts might observe the Purple Screen of Death (**PSOD**) in certain conditions. So, the Virtual Infrastructure Latency collection is disabled for NSX-V data source in vRealize Network Insight 5.1.0. For more information, see the 75224 KB article.

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

- **[NEW]** The HostPrep FeatureUnhealthy event is not closed even when the feature status is Green.
- **[NEW]** Validation fails for AWS access key users having restricted access to the regions.
- **[NEW]** vRealize Network Insight not processing flows correctly after moving from NSX-V to NSX-T.

  When you search for flows between two VMs, you do not see any results; however, you see the flow results when you search between the VM's IP addresses.

- **[NEW]** The Dell switch running version 9.14.2.0 stops responding when vRealize Network Insight runs the show interfaces command on it to collect the configuration information.

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

- **[NEW]** If the AWS VPC logs are published at a delay of 20 minutes at source, the AWS flow data might not show on the Threshold dashboard.
- **[NEW]** If the flow-based threshold configured application has overlapping members (IP endpoints, VMs, or Kubernetes entities) across tiers of different applications, then tiers from other applications will appear on the dashboard of that threshold configuration.
- **[NEW]** The violation region might not be seen on the Threshold Dashboard when the region is outside the preview scale window.
- **[NEW]** When the application has Kubernetes entities, the thresholds with scope as flows do not show flow data when you use Source Application or Destination Application filters.

  Select scope as flows and use the following query:

Scope Query	Aggregation Type
flow type = 'Internet' and generic source application = 'abc’	source Tier
flow type = 'Internet' and generic destination application = 'abc’	destination tier
generic source application = 'abc’	source Tier
generic destination application = ‘abc’	destination tier
application = ‘abc’	source/destination Tier

- **[NEW]** The changes to LDAP or VIDM configuration (newly created or updated) might not reflect on some platform nodes in a cluster deployment, which may result in login failures.

  To fix the issue, run following commands from Platform1:

  ubuntu@platform1:~$ ./run_all.sh sudo service restapilayer-service stop

  ubuntu@platform1:~$ ./run_all.sh sudo service restapilayer-service start

- **[NEW]** If you export the VeloCloud Enterprise dashboard, or any pinboard containing the SD-WAN Deployments widget, you see a blank PDF. However, you can generate the PDF by selecting any widgets of your choice other than the SD-WAN Deployments widget.
- vRealize Network Insight 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

- vRealize Network Insight does not collect the route information of the Check Point data source, which results in missing VM paths details.
- If you have upgraded the collector from 4.2, 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.
- The facet filter does not work in non-English language.
- Though you delete the application, you see the protection status of the application on the map view.
- 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, the default connectivity strategy applies to a VM in VMware Cloud on AWS.
  In such cases, the firewall icon is not present in the VM-VM path on the VMware Cloud on AWS side as we do not get enough information about the realization of the default rule from the VMware Cloud on AWS SDDC.