Installing vRealize Network Insight

VMware vRealize Network Insight 3.9

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About vRealize Network Insight Installation Guide

The *vRealize Network Insight Installation Guide* is intended for administrators or specialists responsible for installing vRealize Network Insight.

Intended Audience

This information is intended for administrators or specialists responsible for installing vRealize Network Insight. The information is written for experienced virtual machine administrators who are familiar with enterprise management applications and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Preparing for Installation 1

Before you install vRealize Network Insight, prepare the deployment environment to meet the system requirements.

This chapter includes the following topics:

- System Recommendations and Requirements
- Supported Products and Versions

System Recommendations and Requirements

For optimum performance, the minimum recommendations for the deployment are as follows:

Recommendations for the Platform Deployment

For non-cluster deployment:

Table 1-1. Non-Cluster Deployment

Brick Size	CPU(Number of cores)	RAM	Disk	Number of VMs	Flows per Day	Total Flows	Flow Planning
Medium	8	32 GB	750 GB	4000	1 million	10 million	2 million
Large	12	48 GB	750 GB	6000	2 million	10 million	4 million

For cluster deployment:

Table 1-2. Cluster Deployment

Brick Size	Cluster Size (Number of nodes)	Total CPU (Number of cores)	Total RAM	Total Disk	Number of VMs	Flows per Day	Total Flows	Flow Planning
Large	3	36	144 GB	3 TB	10,000	2 million	10 million	4 million
Extra Large	3	48	192 GB	6 TB	18,000	6 million	10 million	4 million

Table 1-2. Cluster Deployment (Continued)

Brick Size	Cluster Size (Number of nodes)	Total CPU (Number of cores)	Total RAM	Total Disk	Number of VMs	Flows per Day	Total Flows	Flow Planning
Extra Large	5	80	320 GB	10 TB	30,000	10 million	10 million	4 million
Extra Large	10	160	640 GB	20 TB	60,000 **Note** For supporting 60,000 VMs on a 10-node cluster, contact VMware Support.	10 million	10 million	4 million

Note Each brick in the cluster configuration mentioned in the above table refers to the following recommendation.

Table 1-3.

Brick Size	CPU per Node (Number of Cores)	RAM per Node (GB)	Disk per Node (TB)
Large	12	48	1
Extra Large	16	64	2

Recommendation for the Collector Deployment

Table 1-4.

Collector Size	CPU (Number of Cores)	RAM	Disk	Number of VMs	Flows per Day
Medium	4	10 GB	150 GB	4000	2.5 million
Large	6	12 GB	150 GB	6000 **Note** For support on adding 10,000 VMs on a large collector, contact VMware Support.	5 million
Extra Large	6	36 GB	150 GB	6000 **Note** For extra large collector configuration and support for adding 10,000 VMs , contact VMware Support.	10 million

Other Requirements and Considerations

- The maximum time skew between the platform nodes has to be lesser than 30 seconds.
- The availability of the NTP service is critical to system operations. Ensure that you do not reboot the platform node or the collector node when the NTP service is not available.
- vRealize Network Insight services crashes and does not recover automatically when the existing compute resources are used up by the other processes on the platform. If the services fail to recover, reboot the platform node.

Supported Browser

- Google Chrome or Mozilla Firefox Web browser

Privileges

Privileges Required for Data Sources

- Privileges required to configure and use IPFIX
  - vCenter Server Credentials with privileges:
    - Distributed Switch: Modify
    - dvPort group: Modify

  - The predefined roles in the vCenter server must have the following privileges assigned at root level that need to be propagated to the children roles:
    - System.Anonymous
    - System.Read
    - System.View
    - global.settings
- Privileges required for NSX Manager Data Provider
  - NSX Manager Data Provider requires the **Enterprise** role.
  - If Central CLI is enabled, then the `system admin` credentials are required for NSX Manager Data Provider.
- User privileges required on Cisco switches for metrics collection
  - vRealize Network Insight is capable of collecting metric data via SNMP as well as configuration via SSH from Cisco Switches. Cisco Switches UCS platform requires the use of both SSH and API for collection.

Table 1-5.

Type of data	User Privileges
Configuration Data	Read-Only
Metric Data	SNMP read-only
	SNMPv2 read-only SNMP community
	SNMPv3 read-only

System Ports

The following tables list all the vRealize Network Insight inbound communication ports that need to be whitelisted for various setups:

Ports for the Platform Cluster Setup

Table 1-6.

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
SSH client	Platform	22	SSH	CLI or host access	No	Yes	User/Password or SSH key-based authentication
Client Web-Browser and vRNI Proxy	Platform	443	HTTPS	UI/API access and communication with vRNI Proxy	Yes	Yes	SSL channel encrypted with 2048b RSA key based SHA2 cert (or User configured custom cert). Proxy to Platform messages on this channel also encrypted further with HMAC.
Platform	Platform	2181	HTTP	Communication between zookeeper servers on other nodes (in case of cluster). And stores metdata information(znode data)	No	No	
Platform	Platform	2888	HTTP	Used to connect to zookeeper leader	No	No	
Platform	Platform	3000	HTTP	Used for email notifications	Yes	No	
Platform	Platform	3888	HTTP	Used for zookeeper leader election	Yes	No	

Table 1-6. (Continued)

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
Platform	Platform	5432	jdbc	Storing VM configuration data and infra meta data	Yes	No	
Platform	Platform	8020	TCP/RPC	Communicate between other name node(s) and data nodes	Yes	No	
Platform	Platform	8025	HTTP	Node managers use this port to connect to resource manager	No	No	
Platform	Platform	8030	HTTP	Used by resource manager to schedule the tasks	No	No	
Platform	Platform	8032	HTTP	The address of the applications manager interface in the RM	No	No	
Platform	Platform	8033	HTTP	The address of the RM admin interface	No	No	
Platform	Platform	8042	HTTP	Node manager web app address	No	No	
Platform	Platform	8080	HTTP	Serves UI requests	Yes	No	
Platform	Platform	8088	HTTP	The HTTP address of the Resource Manager web application	No	No	
Platform	Platform	8480	TCP/RPC	JournalNode HTTP server	No	No	
Platform	Platform	8485	TCP/RPC	HDFS shared edits data dir	No	No	

Table 1-6. (Continued)

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
Platform	Platform	9090	HTTP	Serves requests from proxy and sends commands to proxy	Yes	Yes (protected via nginx)	
Platform	Platform	9092	Binary over TCP	Port on which other brokers communicate	Yes	No	
Platform	Platform	9200-9300	HTTP	Serves search requests. ES uses range of ports to listen, if 9200 is by it uses next port available.	Yes	No	
Platform	Platform	9300	HTTP	Serves search requests. ES uses range of ports to listen, if 9200 is by it uses next port available.	Yes	No	
Platform	Platform	30000:65535	TCP	Ephemeral ports range used by various processes to make the TCP connection with the other processes	No	No	
Platform	Platform	60000	IPC	Used for communication between other hbase masters and region servers	Yes	No	

Table 1-6. (Continued)

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
Platform	Platform	60010	HTTP	Used for hbase web UI	No	No	
Platform	Platform	60020	IPC	Communication between hbase master and region server	Yes	No	

Ports for the Single Platform Setup

Table 1-7.

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
SSH client	Platform	22	SSH	CLI or host access	No	Yes	User/Password or SSH key-based authentication
Client Web-Browser and vRNI Proxy	Platform	443	HTTPS	UI/API access and communication with vRNI Proxy	Yes	Yes	SSL channel encrypted with 2048b RSA key based SHA2 cert (or User configured custom cert). Proxy to Platform messages on this channel also encrypted further with HMAC.

Ports for the Proxy Server

Table 1-8.

Source	Target	Port	Protocol	Purpose	Sensitive	SSL	Authentication
SSH client	Proxy	22	SSH	CLI or host access	No	Yes	User/Password or SSH key-based authentication
vRNI Proxy	Platform	443	HTTPS	Primary communication channel with Platform	Yes	Yes	SSL channel encrypted with 2048b RSA key based SHA2 cert (or User configured custom cert). Proxy to Platform messages on this channel also encrypted further with HMAC.
Flow Forwarder	Proxy	UDP 2055	NetFlow/IPFIX	Flows from target are pushed to this port	Yes	No	

Network Communication Ports

The following table lists the ports and the protocols that are used for the network communication in vRealize Network Insight:

Table 1-9.

Purpose	From	To	Port	Protocol
Communication between the VMs of vRealize Network Insight	Collector	Platform	443	HTTPS
Services that require Internet access	Platform and Collector	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS

Table 1-9. (Continued)

Purpose	From	To	Port	Protocol
Communication for miscellaneous services configured	Platform	LDAP server	389, 636	LDAP and LDAPS
		SNMP server	Configurable	SNMP
	Platform and Collector	DNS server	53	UDP
		Syslog server	Configurable	
	ESXi Hosts	Collector	2055	
Communication with AWS as a data source	Collector	AWS(*.amazonaws.com)	443	HTTPS
Communication with other data sources within the data center	Collector	Arista switches	161 and 22	SNMP and SSH
		Brocade switches	161 and 22	SNMP and SSH
		Check Point firewall	443	HTTPS
		Cisco Nexus	161 and 22	SNMP and SSH
		Cisco UCS (Unified Computing System)	161, 22, and 443	SNMP, SSH, and HTTPS
		Cisco Catalyst switches	161 and 22	SNMP and SSH
		Dell switches	161 and 22	SNMP and SSH
		HP	22	SSH
		Juniper Switches	161 and 22	SNMP and SSH
		Palo Alto Networks	443	HTTPS
		VMware vSphere	443	HTTPS
		VMware NSX	22 and 443	SSH and HTTPS

Supported Products and Versions

vRealize Network Insight supports several products and versions.

Data Source	Version/Model	Connection Protocol	Permissions/Privileges
Amazon Web Services (Enterprise License Only)	Not Applicable	HTTPS	Refer the Adding an AWS Data Source section in the vRealize Network Insight User Guide.
Arista switches	7050TX, 7250QX, 7050QX-32S, 7280SE-72	SSH, SNMP	Read only user Read only SNMP user
Brocade Switches	VDX 6740, VDX 6940, MLX, MLXe	SSH, SNMP	Read only user Read only SNMP user

Data Source	Version/Model	Connection Protocol	Permissions/Privileges
Check Point Firewall	Check Point R80	HTTPS	Administrator with `Read Write` permissions The Check Point Management Server should accept API access from the Collector IP address. It can be set up from **Manage & Settings > Blades > Management API > Advanced Settings**.
Cisco ASA	X Series with OS 9.4	SSH, SNMP	The user should have rights to switch to the enable mode. The user's password should be same as the one used for the enable mode of Cisco ASA.
Cisco Catalyst	3000, 3750, 4500, 6000, 6500	SSH, SNMP	Read only SNMP user with default privilege level 15
Cisco Nexus	3000, 5000, 7000, 9000, VSM N1000	SSH, SNMP	Read only user Read only SNMP user
Cisco UCS (Unified Computing System)	Series B blade servers, Series C rack servers, Chassis, Fabric interconnect	UCS Manager: HTTPS UCS Fabric: SSH, SNMP	Read only user Read only SNMP user
Dell switches	FORCE10 MXL 10, FORCE10 S6000, S4048, Z9100, S4810, PowerConnect 8024	SSH, SNMP	Read only user Read only SNMP user
HP	HP Virtual Connect Manager 4.41, HP OneView 3.0	HP OneView 3.0: HTTPS HP Virtual Connect Manager 4.41: SSH	Read only user
Infoblox	Infoblox NIOS version 8.0, 8.1, 8.2	HTTPS	Read only user with API Interface access Read-only permissions for DNS object types as follows: ■ Permission Type - DNS ■ Resource - A Records, DNS Zones, DNS Views
Juniper Switches	EX3300, QFX 51xx Series (JunOS v12 & v15, without QFabric)	Netconf, SSH, SNMP	Read only user Read only SNMP user
Palo Alto Networks	Panorama 7.0.x, 7.1, 8.0	HTTPS	Read only user `Admin role` profile is required for an administrator.
VMware NSX-V	Supported Versions	SSH, HTTPS	NSX Manager Data Provider requires the Enterprise role. For 6.2.x & 6.3.x if Central CLI is used, then provide `system admin` credentials.

Data Source	Version/Model	Connection Protocol	Permissions/Privileges
VMware NSX-T	Supported Versions	HTTPS	Read only user
VMware vRealize Log Insight	Supported Versions	HTTPS	API user with permissions to install, configure, and manage the content pack

VMware vSphere	Supported Versions
	For IPFIX, VMware ESXi version needed:
	- 5.5 Update 2 (Build 2068190) and above
	- 6.0 Update 1b (Build 3380124) and above
	- VMware VDS 5.5 and above
	Note Vmware tools should be installed on all the VMs in the data center to identify the VM to VM path.
		HTTPS	Read only user
			Privileges required to configure and use IPFIX
			vCenter Server Credentials with privileges:
			`Distributed Switch: Modify`
			`dvPort group: Modify`
			The predefined roles in the vCenter server must have the following privileges assigned at root level that need to be propagated to the children roles:
			`System.Anonymous`
			`System.Read`
			`System.View`
			`global.settings`

Installing vRealize Network Insight

2

You can deploy vRealize Network Insight using vSphere Web client or vSphere Windows native client.

Note After you successfully deploy vRealize Network Insight Platform OVA, verify whether the given static IP is set on vCenter Server.

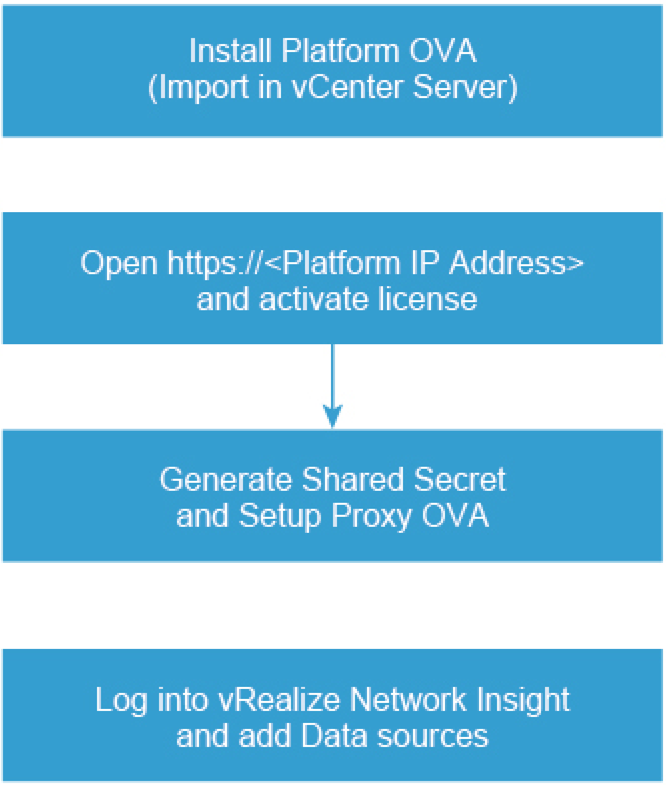
You can also install vRealize Network Insight by using vRealize Suite Life Cycle Manager (LCM). For more information, see the *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management* guide.

This chapter includes the following topics:

Installation Workflow

To install vRealize Network Insight, you install the platform OVA, activate the license, generate shared secret, and setup proxy OVA.

Note The terms **Proxy** and **Collector** are used interchangeably in the documentation.



Deploying vRealize Network Insight Platform OVA

You can import the vRealize Network Insight Platform OVA to your vCenter Server.

Deployment using vSphere Web Client

You can deploy vRealize Network Insight using vSphere Web Client.

Procedure

1. Right-click the **Datacenter** where you want to install the appliance and select **Deploy OVF Template**.
2. Enter the URL to download and install the OVA package or browse to select the source location of the OVA package.
3. Enter the OVA name. Select the destination folder for deployment.
4. Select a host or a cluster or a resource pool where you want to run the deployed template.
5. Verify the OVF template details.
6. Read the End User License Agreement and click **Accept**.
7. Select a deployment configuration. Click **Next**.

8 Select the location to store the files for the deployed template. Select **Thin Provision** as the Virtual Disk format. Select the datastore or the datastore clusters where you want to store the files. Click **Next**.

9 Select the network that the deployed VM will use.

The selected network should allow the appliance to reach out to Internet for support and upgrade.

10 To customize the template for the deployment, you will have to manually configure the appliance using the VM console. Click **Next**.

11 Verify the configuration details and click **Finish**.

12 Once the platform is installed, start the VM and launch the console.

13 Log in with the given console credentials. Run the `setup` command.

14 Create the password for the `support` login. Change the password for the `consoleuser`.

15 Enter the following details to configure the network:

a **IPv4 Address**: Second reserved static IP address

b **Netmask**: Subnet mask for the above static IP

c **Default Gateway**: Default gateway of your network

d **DNS** : DNS server of your environment

Note For multiple DNS servers, ensure that they are separated by space.

e **Domain Search List** : The domain that needs to be appended for dns lookups

f Enter `y` to save the configuration.

16 Enter the NTP Sever and ensure that it can reached from the VM. The services will fail to start if NTP time is out of sync.

Note For multiple NTP servers, ensure that they are separated by commas.

17 To configure Web proxy, enter `y`. This is an optional configuration.

18 To configure Health Telemetry, enter `y`. This is an optional configuration.

19 All the services are verified.

Deployment Using vSphere Windows Native Client

You can deploy vRealize Network Insight using vSphere Windows native client.

Procedure

1 Click **File > Deploy OVF Template**.

2 Enter the URL to download and install the OVA package from the internet or browse to select the source location of the OVA package on your computer.

3 Click **Next** and verify the OVF template details.

4 Read the End-User License Agreement and click **Accept**.

5 Provide a name and specify the location for the deployed template. Click **Next**.

6 Select the **Deployment Configuration**.

7 Select a **Host/Cluster** where you want to run the deployed template.

8 Select the **Resource Pool** in which you want to deploy this template.

9 Select a destination storage for the VM files. Click **Next**.

10 Specify the format in which you want to store the virtual disks. Select **Thin Provision** as the virtual disk format. Click **Next**.

11 Specify the network that the deployed template should use. Map the network from OVA to your inventory.

12 Customize the template for the deployment. Provide the shared secret that was generated on the onboarding page. You will have to manually configure the appliance using the VM console. Click **Next**.

13 Verify all the configuration data. Check **Power on after deployment**. Click **Finish**.

14 Once the Collector OVA is installed, start the VM and launch the console.

15 Log in with the given console credentials. Run the `setup` command.

16 Create the password for the `support` login. Change the password for the `consoleuser`.

17 Enter the following details to configure the network:

   a **IPv4 Address**: Second reserved static IP address

   b **Netmask**: Subnet mask for the above static IP

   c **Default Gateway**: Default gateway of your network

   d **DNS** : DNS server of your environment

   Note For multiple DNS servers, ensure that they are separated by space.

   e **Domain Search List** : The domain that needs to be appended for `dns lookup`.

   f Enter y to save the configuration.

18 Enter the NTP Sever and ensure that it can reached from the VM. The services will fail to start if NTP time is out of sync.

Note For multiple NTP servers, ensure that they are separated by commas.

19 To configure Web proxy, enter `y`. This is an optional configuration.

20 To configure Health Telemetry, enter `y`. This is an optional configuration.

21 All the services are verified.

Activating the License

After installing the vRealize Network Insight Platform OVA, open *https://<vRealize Network Insight Platform IP address>* in the Chrome Web browser.

Procedure

1 Enter the license key received in the welcome email.

2 For UI admin (`admin@local`) user name, set the password. If you are a support user or a CLI user, refer Default Login Credentialsfor the password.

3 Click **Activate**.

4 Add the vRealize Network Insight Collector after activating the license.

Generating Shared Secret

You can generate and import the vRealize Network Insight proxy virtual appliance.

Generate a shared secret and import the vRealize Network Insight proxy virtual appliance:

Procedure

1 Generate a shared secret after activating the license on the **Setup Proxy Virtual Appliance** page.

2 Copy the shared secret.

You will require this during the deployment of vRealize Network Insight Proxy OVA.

Setting up Network Insight Collector (OVA)

You can set up vRealize Network Insight collector by importing OVA to your vCenter server.

Follow the steps below to import the vRealize Network Insight collector OVA to your vCenter Server.

Deployment Using vSphere Web Client

You can import the vRealize Network Insight Collector OVA using vSphere Web Client.

Procedure

1 Right-click the **Datacenter** where you want to install the appliance and select **Deploy OVF Template**.

2 Enter the URL to download and install the OVA package from the internet or browse to select the source location of OVA from your computer.

3 Provide a name and specify the location for the deployed template. Click **Next**.

4 Select a resource (host or a cluster) where you want to run the deployed template. Click **Next**.

5 Verify all the details of the template. Click **Next**.

6 Read the End-User License Agreement and click **Accept**. Click **Next**.

7 Select a deployment configuration. Click **Next**.

8 Select the location where you want to store the files for the deployed template. Specify the format in which you want to store the virtual disks. Select **Thin Provision** as the virtual disk format. Select the Datastore in which you want to install the files. Click **Next**.

9 Specify the destination network for the source network. Click **Next**.

10 Customize the template for the deployment. Provide the shared secret that was generated from the UI. You will have to manually configure the appliance using the VM console. Click **Next**.

11 Verify all the configuration data. Click **Finish**.

12 Once the Collector OVA is installed, start the VM and launch the console.

13 Log in with the given console credentials. Run the `setup` command.

14 Create the password for the `support` login. Change the password for the `consoleuser`.

15 Enter the following details to configure the network:

a **IPv4 Address**: Second reserved static IP address

b **Netmask**: Subnet mask for the above static IP

c **Default Gateway**: Default gateway of your network

d **DNS** : DNS server of your environment

Note For multiple DNS servers, ensure that they are separated by space.

e **Domain Search List** : The domain that needs to be appended for dns lookups

f Enter `y` to save the configuration.

16 Enter the NTP Sever and ensure that it can reached from the VM. The services will fail to start if NTP time is out of sync.

Note For multiple NTP servers, ensure that they are separated by commas.

17 A check is made to see if the shared secret key has been configured. The proxy is paired with the corresponding platform. This may take few minutes.

18 To configure Web proxy, enter `y`. This is an optional configuration.

19 To configure Health Telemetry, enter `y`. This is an optional configuration.

20 All the services are verified.

21 Click **Finish**, once **Proxy Detected!** message is displayed on the onboarding page. It will redirect to the Login Page.

Deployment using vSphere Windows Native Client

You can import the vRealize Network Insight Collector OVA using vSphere Windows native client.

Procedure

1. Click **File > Deploy OVF Template**.
2. Enter the URL to download and install the OVA package from the internet or browse to select the source location of the OVA package on your computer.
3. Verify the OVF template details. Click **Next**.
4. Read the End-User License Agreement and click **Accept**. Click **Next**.
5. Provide a name and specify the location for the deployed template. Click **Next**.
6. Select a **Deployment Configuration**. Click **Next**.
7. Select a **Host/Cluster** where you want to run the deployed template. Click **Next**.
8. Select the **Resource Pool** in which you want to deploy this template. Click **Next**.
9. Select a destination storage for the VM files. Click **Next**.
10. Specify the format in which you want to store the virtual disks. the Select **Thin Provision** as the virtual disk format. Click **Next**.
11. Specify the network that the deployed template should use. Map the network from OVA to your inventory.
12. Customize the template for the deployment. Provide the shared secret that was generated on the onboarding page. You will have to manually configure the appliance using the VM console. Click **Next**.
13. Verify all the configuration data. Check **Power on after deployment**. Click **Finish**.
14. Once the Collector OVA is installed, start the VM and launch the console.
15. Log in with the given console credentials. Run the `setup` command.
16. Create the password for the `support` login. Change the password for the `consoleuser`.
17. Enter the following details to configure the network:

    a. **IPv4 Address**: Second reserved static IP address

    b. **Netmask**: Subnet mask for the above static IP

    c. **Default Gateway**: Default gateway of your network

    d. **DNS** : DNS server of your environment

    Note For multiple DNS servers, ensure that they are separated by space.

e **Domain Search List** : The domain that needs to be appended for `dns lookup`.

f Enter `y` to save the configuration.

18 Enter the NTP Sever and ensure that it can reached from the VM. The services will fail to start if NTP time is out of sync.

Note For multiple NTP servers, ensure that they are separated by commas.

19 A check is made to see if the shared secret key has been configured. The proxy is paired with the corresponding platform. This may take few minutes.

20 To configure Web proxy, enter `y`. This is an optional configuration.

21 To configure Health Telemetry, enter `y`. This is an optional configuration.

22 All the services are verified.

23 Click **Finish**, once **Proxy Detected!** message is displayed on the onboarding page. It will redirect to the Login Page.

Deploy Additional Proxy to an Existing Setup

You can add additional vRealize Network Insight proxy to an existing setup.

Procedure

1 Log into the vRealize Network Insight UI. Navigate to **Settings > Install and Support**.

2 Click **Add Proxy VM**.

3 Copy the shared secret from the dialog that is displayed.

4 Follow the steps in section Setting up Network Insight Collector (OVA) in step 3.

Default Login Credentials

vRealize Network Insight has three types of users. The login credentials for these users are as follows:

Note Use Google Chrome to log in to vRealize Network Insight.

Table 2-1.

Types of Users	User name	Password
Admin UI	`admin@local`	Set this password in the Activate License window during installation.
SSH User	`support`	Set this password during installation.
CLI User	`consoleuser`	Set this password during installation.

Procedure

1. Navigate to *https://<vRealize Network Insight Platform IP address>*.
2. Log in to the product UI with the corresponding user name and password.

NSX Assessment Mode for Evaluation License

vRealize Network Insight starts in the NSX assessment mode when you use the evaluation license.

You can add a data source to vRealize Network Insight, analyze traffic flow, and generate reports.

Note To switch to the Full Product mode, click **Switch to Full Product Evaluation** located in the bottom right corner.

Add vCenter Server

You can add vCenter Servers as data source to vRealize Network Insight.

Multiple vCenter Servers can be added to vRealize Network Insight to start monitoring data.

Procedure

1. Click **Add vCenter**.
2. Click **Add new source** and customize the options.

Option	Action
Source Type	Select the vCenter Server system from the drop-down menu.
IP Address/FQDN	Enter the IP address or fully qualified domain name of the vCenter Server.
Username	Enter the user name, with the following privileges: ■ **Distributed Switch**: Modify ■ **dvPort group**: Modify
Password	Enter the password for vRealize Network Insight software to access the vCenter Server system.

3. Click **Validate**.
4. Select **Enable Netflow (IPFIX) on this vCenter** to enable IPFIX.
5. Add advanced data collection sources to your vCenter Server system.
6. (Optional) Click **Submit** to add the vCenter Server system. The vCenter Server systems appear on the homepage.

Analyze Traffic Flows

You can use vRealize Network Insight to analyze flows in your datacenter.

Prerequisites

At least two hours of data collection must occur before starting the flow analysis.

Procedure

1 Specify the scope of the analysis. For example, if you are interested in flows of all virtual machines in a **Cluster**, select Cluster from the dropdown menu. You can alternately select all virtual machines connected to a VLAN or VXLAN.

2 Select the entity name for which you want to analyze the flows.

3 Select the duration and click **Analyze**.

Generate a Report

You can generate a report of the flow assessment.

Prerequisites

Analyze traffic flows in the datacenter. For comprehensive reports, collect 24 hours of data before the analysis.

Procedure

1 In the **EVAL NSX Assessment Mode**, click **Generate Report** in the Analyze Flows page.

2 In the **Non EVAL Mode**, on the **Microsegmentation** page, click **Traffic Distribution > More Options > Assesment Report**.

Adding Data Sources

After you log in, add the various data sources to vRealize Network Insight for the software to monitor your data center.

The product will start showing the data from your environment after two hours of data collection.

Procedure

1 Select **Profile > Settings**.

2 Click the **Add new source** button.

3 Select the **Source Type**.

4 Enter the required details and click **Submit** to add the Data source.

5 Repeat the above steps to add all the required data sources from your environment.

Scaling up of a Platform or Collector Appliance

3

The process of scaling up of a platform or a proxy appliance implies changing its brick size from MEDIUM to LARGE.

If a platform is of LARGE brick size, then you have to scale up by adding more platform nodes such as creating a platform cluster. After a proxy is of LARGE brick size, then you have to add more proxies.

The steps to scale up vRealize Network Insight Virtual Appliance from MEDIUM brick to LARGE brick are as follows:

1 Log in to vCenter.

2 Increase the RAM of the VM to at least match the LARGE brick size requirements.

3 Increase the vCPU count of the VM to at least match the LARGE brick size requirements.

4 Refer to the brick size in the Privileges section.

5 Restart the VM.

Planning to Scale up the Platform Cluster

4

Three or more LARGE platform bricks can be connected together to form a platform cluster.

Note Ensure that you take a backup of the Platform1 node before you create clusters. Refer to VMware best practices to take the backup of virtual machines (like VMware VDP using VADP). Restore the Platform1 node from backup if there is an unrecoverable error while creating the cluster. It is recommended that you use cleanly deployed platform nodes while creating clusters. Redeploy the new platform nodes (p2-pn) before restarting cluster creation process if there is an unrecoverable error.

To decide the required number of platform bricks:

```
Number of bricks needed = Round off to next Integer ((Total number of managed VMs) /
(Capacity of LARGE Platform brick in table above))
```

Scaling up Scenarios for the Platform Cluster

- Scenario 1

  a Assume that on January 1st (today), the datacenter has 2000 VMs (with flows) across many vCenters.

  b Assume that in March, the number of VMs grows to 3100.

  c Assume that in June, the number of VMs grows to 6100 which could be because of the additions of few more vCenters or the expansion of the existing vCenters.

  d Assume that in December, the number of VMs grows to 18100 (with flows).

  The deployment model for this scenario is as follows:

  a On January 1, deploy a single platform node with the MEDIUM brick size.

  b In March, scale up the platform node to the LARGE brick size.

  c In June, scale out the platform, convert to a three node platform cluster by adding new Platform nodes to the existing Platform.

  d In December, the user needs a four node platform cluster.

- Scenario 2

  a Assume that on January 1st (today), the datacenter has 7000 VMs (with flows) across many vCenters.

b Assume that in June, the number of VMs grows to 15000 (with flows).

c Assume that in December, the number of VMs grows to 24000 (with flows).

The deployment model for this scenario is as follows:

a On January 1, deploy a three node platform cluster.

b In June or later, as the environment size gets closer to exceeding 18000, the user needs a four node platform cluster.

c In December, as the environment size gets closer to exceeding 24000, the user needs a five node platform cluster.

Planning to Scale up the Proxy Server 5

The scaling up of the proxy node is independent of the platform nodes in the cluster. Typically, the users install one or more proxy VMs per site. Within a site, the number of proxy VMs needed is a simple function of total number of VMs for which it has to collect data. Refer to the capacity of proxy VMs in the brick size table in the System Requirements section.

You can add a data source (maybe a vCenter or a switch) to exactly one proxy VM.

Scaling up Scenarios for the Proxy Server

- Scenario1: Suppose there are 2000 VMs in a vCenter.

  Install one medium proxy VM. Assign the vCenter to this proxy using the product UI.

- Scenario 2: 1000 VMs in vCenter1 and 2000 VMs in vCenter2 (all of them are in one data center)

  Install one medium Proxy VM. Assign both vCenters to this proxy using the product UI.

- Scenario 3: 1000 VMs in vCenter 1 and 2000 VMs in vCenter2 (all of them are in the same data center)

  Install one medium Proxy VM. Assign both vCenters to this proxy using the product UI.

- Scenario 4: 1000 VMs in vCenter1 (data center1) and 2000 VMs in vCenter2 (data center2)

  Install one medium Proxy VM in each data center. Assign vCenter1 to proxy VM in same data center using Product UI. Assign vCenter2 to Proxy VM in its data center using the product UI.

- Scenario 5: 9,000 VMs in vCenter1 without flows (data center1)

  Install one large proxy brick. Assign this vCenter to this proxy using the product UI.

- Scenario 6: 11,000 VMs in vCenter1 with flows (data center1)

  This scenario is not supported. Maximum number of VMs that can be managed by one proxy VM is 10,000 without flows OR 6,000 with flows. And one vCenter can be added to only one proxy at a time.

- Scenario 7: vCenter1 with 2000 VMs in January, vCenter2 with 5000 VMs in June

  Install one medium Proxy VM in January and assign vCenter1 to it. Install the second large proxy VM in June and assign vCenter2 to it.

Proxy VMs with a Platform Cluster

The number of proxy VMs does not depend on the number of VMs in a platform cluster. All proxy VMs communicate only to the first platform VM (`platform1` in the following example) in a platform cluster. A few example deployment models that are supported are as follows:

- Case 1: A proxy VM connects to a platform cluster.

  The proxy connects to `platform1`.

- Case 2: Many Proxy VMs connect to a platform cluster

  All the proxies are connected to `platform1`. And then `platform1` VM load balances both proxy requests and the data processing to other platform VMs in this cluster internally automatically.

- Case 3: A proxy VM connects to the single platform node deployment
- Case 4: Many proxy VMs connect to one platform node deployment

Expanding a Cluster 6

The cluster expansion feature enables you to add the platform nodes to any existing old and new cluster without incurring any data loss.

Note Ensure that you take a backup of all the Platform nodes before you create clusters. Refer to the VMware best practices to take the backup of virtual machines (like VMware VDP using VADP). Restore the Platform nodes from the backup if there is an unrecoverable error.

For example, if you have an existing cluster with three nodes, you can add 4 more nodes to it without any data loss.

Procedure

1 On the **Install and Support** page, click **Expand Cluster** for **Platform VMs**.

2 The IP addresses of the VMs that are part of the cluster already are listed on the Expand Cluster page. To add one or more nodes to the existing cluster, provide the IP address of the node and the support user password.

   Note

   - Currently, vRealize Network Insight supports 10 nodes in an existing cluster. Once the limit is reached, the **Add more** button is disabled.
   - Ensure that all the new nodes are non-provisioned and are reachable through SSH.
   - Ensure that you have taken a backup of the existing platform VMs before you go ahead with the cluster expansion.

3 Click **Submit**.

   The step-by-step progress is displayed.

4 Once the cluster expansion link is completed, a message indicating success is displayed.

   While the cluster expansion is in progress, the application cannot be used for any other operation.

Upgrading vRealize Network Insight

7

You can upgrade your current vRealize Network Insight environment to the latest version.

In vRealize Network Insight, you can upgrade to 3.9 version from the 3.8 version and the 3.7 version from the same upgrade bundle.

```
3.7->3.9
```

```
3.8->3.9
```

The supported upgrade path is:

`3.0->3.1->3.2->3.3->3.4->3.5->3.6->3.7->3.8->3.9`

From Release 3.5 onwards, jump upgrades are supported. For example:

`3.0->3.1->3.2->3.3->3.4->3.5->3.7->3.9`

From Release 3.8 onwards, you can perform the cluster upgrade online. vRealize Network Insight provides the following three modes of upgrade:

This chapter includes the following topics:

- Online Upgrade
- Single-Click Offline Upgrade
- Offline Upgrade

Online Upgrade

Whenever there is a new version of vRealize Network Insight available, you receive a notification.

Prerequisites

Ensure that the following disk space requirements are met before going ahead with the upgrade:

- The following requirements are for both platform and proxy server:
  - `/tmp` - 6 GB
  - `/home` - 2 GB

- /- 6 GB (Only for the Platform1 node)

  Note This requirement is only for the platform.

If the bandwidth is insufficient to download the upgrade bundle from the server, then the upgrade fails. The minimum bandwidth required is 500 KB/s. The **Install and the Support** page throws an error if the download bandwidth check fails.

Note The download bandwidth check is not applicable when upgrading from 3.8 to 3.9. But from 3.9 to all future upgrades this will be applicable.

Procedure

1. To enable online upgrade, you have to contact the VMware support. Verify the upgraded version from the product UI under **Settings** page to be one that is mentioned in the update.

   Note

   - If the update notification is not available, verify that both vRealize Network Insight Platform and Proxy VMs have connectivity to `svc.ni.vmware.com` on port 443 and `reg.ni.vmware.com` on port 443 by running the `show-connectivity-status` command. If this connectivity requires `http proxy`, configure it on each VM using the `set-web-proxy` command. Ensure that the output contains upgrade connectivity status as `Passed`.
   - File a support ticket and provide the service tag from the product UI. The service tag is shown under **Settings**.
   - Provide a screenshot of the `show-connectivity-status` command output from each vRealize Network Insight Platform and Proxy VMs.

2. Check if the update notification is available on the **Install and Support** page under **Settings**.
3. Click **View details** to view details of update.
4. Click **Install Now** on the details page to download and upgrade the vRealize Network Insight deployment.

   Note

   - Ensure that all the nodes are online before beginning the upgrade. If any node is inactive before the upgrade begins, you will not be allowed to trigger the upgrade.
   - Once the upgrade begins, if a node becomes inactive, the upgrade process does not continue. The upgrade will not resume until the node becomes active again.
   - The Platform1 becomes the upgrade server here. If Platform1 is offline, then no other node is upgraded.

Single-Click Offline Upgrade

vRealize Network Insight supports the single-click offline upgrade of the product from Release 3.7 to the future releases such as 3.7->3.8, 3.7->3.9, 3.8->3.9, and so on.

Ensure that the following disk space requirements are met before going ahead with the upgrade:

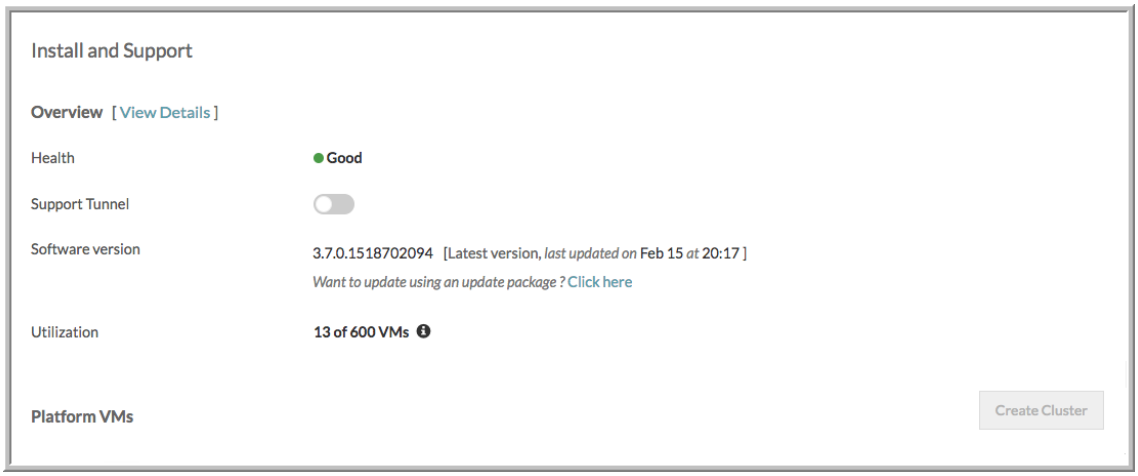
- The following requirements are for both platform and proxy server:
  - `/tmp` - 6 GB
  - `/home` - 2 GB
- `/`- 12 GB (Only for the Platform1 node)

Note This requirement is only for the platform.

Procedure

1 Ensure that you have saved the update package to your local disk so that you can upload it on this page. Click **Browse** to select the file and click **Upload**.

2 On the **Install and Support** page, under **Software version**, click **Click here**.



Install and Support

Overview [View Details]

Health ● Good

Support Tunnel

Software version 3.7.0.1518702094 [Latest version, *last updated on* Feb 15 *at* 20:17]
Want to update using an update package ? Click here

Utilization 13 of 600 VMs

Platform VMs

3 After the upload is complete, a dialog box with the basic upgrade instructions appears before the upgrade begins. To proceed further, click **Install Now**.

4 Once the upgrade process begins, a pop-up window appears. This pop-up window provides the status of each node.

Note

- Ensure that all the nodes are online before beginning the upgrade. If any node is inactive before the upgrade begins, the upgrade is not triggered.
- Once the upgrade begins, if a node becomes inactive, the upgrade process does not continue. The upgrade will not resume until the node becomes active again.
- Until the upload of the package happens, the user should take care that the session is not closed. If the session ends, the user has to restart the upload process.
- The Platform 1 becomes the upgrade server here. If Platform1 is offline, then no other node is upgraded.

5 Upon the completion of upgrade process, all platforms and the collectors nodes are upgraded.

Offline Upgrade

Consider offline upgrade only if both online upgrade or single-click offline upgrade don't work. Use this option when both vRealize Network Insight Platform and Proxy VMs do not have access to the internet. You must upgrade Platform VMs before Proxy VMs.

Prerequisites

In case of the cluster upgrade, `platform1` must be upgraded first. To confirm platform1 IP address, run the `ping platform1` command from any platform node.

Procedure

1 Download the required upgrade bundle file from My VMware.

2 Copy the upgrade bundle to all vRealize Network Insight Platform and Proxy VMs by using either of the following options:

   a To copy the file from Linux VM to vRealize Network Insight VM, run this command:

   ```
   scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/
   ```

   To copy file from Windows VM to vRealize Network Insight VM, run this command:

   Note Use the `pscp` utility from https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe.

   ```
    pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/
   ```

   b Log in to the vRealize Network Insight Platform CLI using `consoleuser` and run this command:

   Note This command uses SCP to download the bundle from the host where the bundle is downloaded. So the SCP server is required to be running on the host.

   ```
   package-installer copy --host <ip address> --user johndoe --
   path /path/to/<filename>.upgrade.bundle
   ```

3 Upgrade each node starting with Platform1 node using the `package-installer upgrade` command. For the 3.5 version, run the command as follows:

   ```
   package-installer upgrade --name VMWare-vRealize-Network-Insight-<version_number>.upgrade.bundle
   ```

   For 3.4 and the preceding versions, run the command as follows:

   ```
   package-installer upgrade
   ```

4 Verify the upgraded version using the `show–version` command.

Note

- Ensure that you verify the checksums for the upgrade bundle as specified.
- You can upgrade the cluster only in the offline mode.
- After a successful upgrade, you do not have to reboot the virtual machine.