Installing vRealize Network Insight

VMware vRealize Network Insight 3.5

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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 Requirements

Ensure that the system meets the minimum hardware configurations to install vRealize Network Insight.

Minimum Resource Requirements

- vRealize Network Insight Platform OVA
  - 800 GB - HDD, Thin provisioned
  - Medium Brick Requirement
    - 8 cores - Reservation 4096 Mhz
    - 32 GB RAM - Reservation - 16GB
  - Large Brick Requirement
    - 12 cores - Reservation 6144 Mhz
    - 48 GB RAM - Reservation - 24GB
- vRealize Network Insight Proxy OVA
  - 150 GB - HDD, Thin provisioned
  - Medium Brick Requirement
    - 4 cores - Reservation 2048 Mhz
    - 10 GB RAM - Reservation - 5GB
  - Large Brick Requirement
    - 6 cores - Reservation 3072 Mhz
    - 12 GB RAM - Reservation - 6GB

Software Requirements

- Google Chrome or Mozilla Firefox Web browser

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 1-1.

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

Brick Sizes

The hardware requirements of various brick sizes for a single platform and a single proxy VM are as follows:

Table 1-2.

Type	Brick Size	Capacity (Number of Managed VMs)	Flows (# of 4-Tuples)	Flow Records/l PFIX	vCPU Cores	RAM	Disk (Thin provision ed)	IOPS
Platform (With flows)	LARGE	6K	2M		12	48 GB	750GB	250
Platform Without flows)	LARGE	10K			12	48 GB	750GB	250
Platform (With flows)	MEDIUM	3K	1M		8	32 GB	750GB	150
Platform (Without flows)	MEDIUM	5K			8	32 GB	750GB	150
Proxy (With flows)	LARGE	6K		100k/s	6	12 GB	150 GB	75
Proxy (Without flows)	LARGE	10K			6	12 GB	150 GB	75
Proxy (With flows)	MEDIUM	3K		50k/s	4	10 GB	150 GB	50
Proxy (Without flows)	MEDIUM	5K			4	10 GB	150 GB	50

Supported Products and Versions

vRealize Network Insight support several products and versions.

Data Source	Version/Model	Description
Amazon Web Services (Enterprise License Only)	Not Applicable	The data source connects to Amazon Web Services over HTTPS.
Arista switches	7050TX, 7250QX	The data provider connects to Arista switches over SSH v2 and SNMP.
Brocade Switches	VDX 6740, VDX 6940, MLX, MLXe	The data provider connects to Brocade switches over SSH v2 and SNMP.
Check Point Firewall	Check Point R80	The data provider connects Check Point Firewall over HTTPS.
Cisco Nexus	5000, 7000, 9000, VSM N1000	The data provider connects Cisco Nexus switches over SSH v2 and SNMP.

Data Source	Version/Model	Description
Cisco UCS (Unified Computing System)	Series B blade servers, Series C rack servers, Chassis, Fabric interconnect	The data provider connects to UCS Manager over HTTPS and UCS Fabric Interconnect over SSH to fetch information. It also connects to the SNMP service on UCS.
Cisco Catalyst switches	3000, 3750, 4500, 6000, 6500	The data provider Cisco Catalyst switches connects to device over SSH and SNMP.
Dell switches	FORCE10 MXL 10, FORCE10 S6000, S4048, Z9100, S4810, PowerConnect 8024	The data provider connects to Dell switches over SSH v2 and SNMP.
HP	HP Virtual Connect Manager 4.41, HP OneView 3.0	The data provider connects to HP Virtual Connect Manager over SSH v2.
Juniper Switches	EX3300	The data provider connects to Juniper switches over SSH v2 and SNMP.
Palo Alto Networks	Panorama 7.0.x, Panorama 7.1	The data provider connects to Palo Alto Panorama appliance HTTPS.
VMware vSphere	■ vSphere 5.5 (up to U3) ■ vSphere 6.0 (up to U3) ■ vSphere 6.5 (up to U1) 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** vmtools should be installed on all the Virtual Machines in the data center to identify the VM to VM path.	Data provider connects to VMware vCenter over HTTPS to fetch virtual environment information.
VMware NSX	■ 6.3 (up to 6.3.3) ■ 6.2 (up to 6.2.8) ■ 6.1 (up to 6.1.7) ■ 6.0	The data provider connects: ■ VMware NSX Manager over HTTPS ■ VMware NSX Controller over SSH ■ VMware NSX Edge over SSH or Central CLI depending on customer preference

Prerequisites

- The connectivity to the following services requires Internet access to the specific URL and the port. If the vRealize Network Insight platform is behind an Internet proxy, ensure that you whitelist the following domain names and ports:

  Table 1-3.

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

- 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.

Installing vRealize Network Insight 2

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

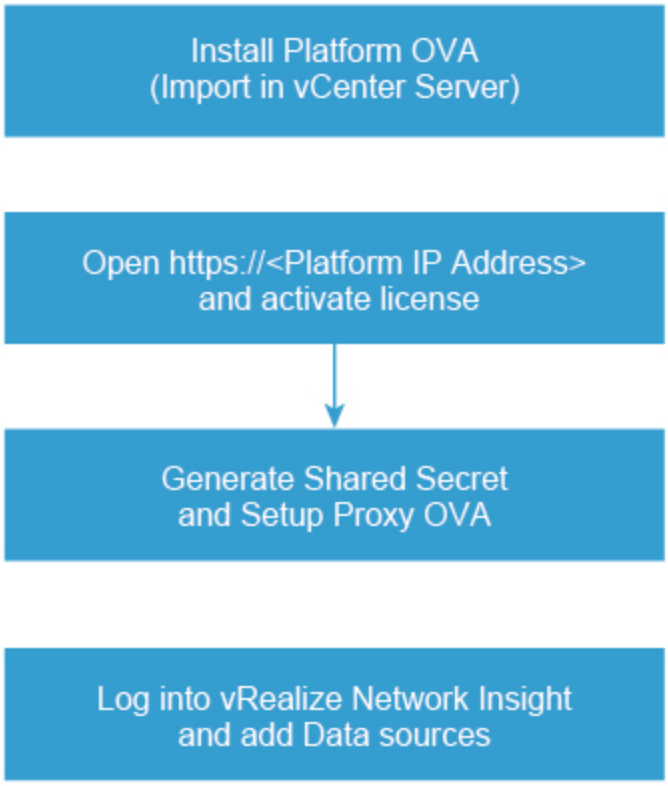
Note After you successfully deploy vRealize Network Insight Platform OVA, verify whether the given static IP is set on vCenter Server.

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 on the **Datacenter** where you want to install the appliance and select **Deploy OVF Template**.
2. Browse to select the source location of the appliance OVA.
3. Verify the OVF template details.
4. Read the End User License Agreement and click **Accept**.
5. Select the destination folder in which you want to create the VM and give a desired name to the VM.
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 the **Datastore** where you want to store the files.
10. Select **Thin Provision** as the Virtual Disk format.

11 Select the **Network** that the deployed VM will use.

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

12 Customize the template as mentioned below:

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

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

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

d **DNS Server List**: DNS servers of your environment

e (Optional) **DNS Server List**: DNS servers of your environment

f Domain Search List: Determines which domain to be appended for dns lookups.

g (Optional) **NTP Server List**: Enter the list of NTP servers and ensure that NTP Server can be reached from the VM. The services will fail to start if NTP time is out of sync.

h (Optional) **Web Proxy IP/FQDN and Web Proxy Port**: For accessing the Internet using a proxy

i (Optional) **Syslog server IP** : Syslog server IP [Optional]: IP address of the syslog server where you want to send the syslog messages

j Uncheck the **Log Push Enable** checkbox if you do not want to send diagnostic and troubleshooting data to VMware.

13 Review the details and select the **Power on after deployment checkbox**, then click **Finish**.

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 Browse to select the source location of the OVA.

3 Click **Next** and Verify OVF template details.

4 Ensure that the desired folder is selected and give a name to the VM.

5 Select the **Deployment Configuration**.

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

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

8 Select the **Datastore** where you want to store the files.

9 Select **Thin Provision** as the Virtual Disk format.

10 Map the **Network** from OVA to your inventory

11 Customize the template as mentioned below:

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

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

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

d **DNS Server List**: DNS servers of your environment

e (Optional) **DNS Server List**: DNS servers of your environment

f **Domain Search List:** Determines which domain to be appended for dns lookups.

g (Optional) **NTP Server List**: Enter the list of NTP servers and ensure that the NTP Server can be reached from the VM. The services will fail to start if NTP time is out of sync.

h (Optional) **HTTP Proxy IP/FQDN** and **HTTP Proxy Port**: For accessing the Internet using a proxy

i (Optional) **Syslog server IP** : IP address of the syslog server where you want to send the syslog messages

j Uncheck the **Log Push Enable** checkbox if you do not want to send diagnostic and troubleshooting data to VMware.

k Select the **Health Telemetry Enable** checkbox to improve the product by sending anonymous data about product performance.

12 Review the details and select the **Power on after deployment checkbox**, then click **Finish**.

Generating the Support Tunnel Certificate

Perform this step only if you are offline or have restricted access to Internet.

To generate the support tunnel certificate:

1 Log on to the console user CLI and run the `offline-registration` command.

2 The CLI generates a token. After you supply this token to VMware Support, an entry is created in the registration server and a certificate is given to you.

3 Install this certificate by using the `offline-registration` command.

Activating the License

Before the deployment, activate and install the vRealize Network Insight virtual appliance.

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 Credentials," on page 19for 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 vRealize Network Insight Proxy Virtual Appliance (OVA)

You can set up vRealize Network Insight proxy virtual appliance by importing OVA to your vCenter server.

Follow the steps below to import the vRealize Network InsightProxy OVA to your vCenter Server

Deployment using vSphere Web Client

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

Procedure

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

2 Browse to select the source location of the appliance OVA.

3 Verify the OVF template details.

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

5 Select the destination folder in which you want to create the VM and give a desired name to the VM.

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 the Datastore where you want to store the files.

10 Select **Thin Provision** as the Virtual Disk format.

11 Select the **Network** that the deployed VM will use.

12 Customize the template as mentioned below:

   a **Shared Secret for vRealize Network Insight Proxy**: The shared secret generated on the onboarding page

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

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

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

   e **DNS Server List**: DNS servers of your environment

   f (Optional) **Domain Search List** : Determines which domain to be appended for dns lookups

   g **NTP Server List**: Enter the list of NTP servers and ensure that the NTP Server can be reached from the VM. The services will fail to start if NTP time is out of sync.

   h (Optional) **Web Proxy IP/FQDN**and **Web Proxy Port**: For accessing the Internet using a proxy

   i (Optional) **Syslog server IP** : IP address of the syslog server where you want to send the syslog messages

   j Uncheck the **Log Push Enable** checkbox if you do not want to send diagnostic and troubleshooting data to VMware.

   k Select the **Health Telemetry Enable** checkbox, to improve the product by sending anonymous data about product performance.

13 Review the details and select the **Power on after deployment** checkbox then click Finish.

Deployment using vSphere Windows Native Client

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

Procedure

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

2 Browse to select the source location of OVA.

3 Verify the OVF template details.

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

5 Ensure the desired folder is selected and give a name to the VM.

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 the **Datastore** where you want to store the files.

10 Select **Thin Provision** as the Virtual Disk format.

11 Select the **Network** that the deployed VM will use.

12 Map the network from OVA to your inventory.

13 Customize the template as mentioned below:

   a **Shared Secret for vRealize Network Insight Proxy**: The shared secret generated on the onboarding page

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

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

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

   e **DNS Server List**: DNS servers of your environment

   f (Optional) **Domain Search List** : Determines which domain to be appended for dns lookups

   g **NTP Server List**: Enter the list of NTP servers and ensure that the NTP Server can be reached from the VM. The services will fail to start if NTP time is out of sync.

   h (Optional) **HTTP Proxy IP/FQDN** and **HTTP Proxy Port**: For accessing the Internet using a proxy

   i (Optional) **Syslog server IP** : IP address of the syslog server where you want to send the syslog messages

   j Uncheck the **Log Push Enable** checkbox if you do not want to send diagnostic and troubleshooting data to VMware.

   k Select the **Health Telemetry Enable** checkbox, to improve the product by sending anonymous data about product performance.

14 Review the details and select the **Power on after deployment** checkbox then click **Finish**.

Note After the vRealize Network Insight Proxy OVA is deployed and running, you must verify whether the given static IP is set on vCenter Server.

15 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 vRealize Network Insight Proxy Virtual Appliance (OVA)," on page 16 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	Username	Password
Admin UI	`admin@local`	Set this password in Activate License screen during installation
SSH User	`support`	`ark1nc0113ct0r`
CLI User	`consoleuser`	`ark1nc0ns0l3`

Procedure

1 Open *https://<vRealize Network Insight Platform IP address>*.

2 Log in to the product UI with the corresponding username 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 Add advanced data collection sources to your vCenter Server system.

5 (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 Proxy 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 out 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 a Log in to vCenter.

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

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

d Refer to the brick size in the "System Requirements," on page 7 section.

e Restart the VM.

Planning to Scale Up the Platform Cluster

4

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

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 VM's (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 MEDIUM brick size.
  b. In March, scale up the platform node to LARGE brick size.
  c. In June, scale out the platform, convert to a 3-node platform cluster by adding new Platform nodes to the existing Platform.
  d. In December, the user needs a 4-node platform cluster. vRealize Network Insight does not support extension of cluster.
- Scenario 2
  a. Assume that on January 1st (today), the datacenter has 7000 VM's (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 3-node platform cluster.
  b. In June or later, as the environment size gets closer to exceeding 18000, the user needs a 4-node platform cluster. vRealize Network Insight does not support extension of cluster.

c In December, as the environment size gets closer to exceeding 24000, the user needs a 5-node platform cluster. vRealize Network Insight does not support extension of cluster..

Planning to Scale up the Proxy Cluster

5

The scaling out of the proxy node is independent of the platform nodes in the cluster

Typically, 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. A data source (maybe a vCenter or a switch) can be added to exactly one proxy VM.

Scaling up Scenarios for the Proxy Cluster

- Scenario1: 2000 VMs in one vCenter

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

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

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

- Scenario 3: 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 Product UI.

- Scenario 4: 9,000 VMs in vCenter1 without flows (data center1)

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

- Scenario 5: 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 6: 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 in a platform cluster. A few example deployment models are as follows

- Case1: One Proxy VM connecting to a platform cluster

  Supported. Proxy connects to platform1.

- Case2: Many Proxy VMs connecting to a platform cluster

Supported. All 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.

- Case3: One proxy connecting to single platform node deployment

  Supported.

- Case4: Many proxy VMs connecting to One platform node deployment

  Supported.

:

Index