Juniper Networks | Engineering Simplicity

How to Install and Set Up Virtual Juniper Advanced Threat Prevention

Published
2021-08-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

How to Install and Set Up Virtual Juniper Advanced Threat Prevention

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install and configure the basic parameters of the JATP virtual core and virtual email and traffic collectors. Refer to the JATP appliance software guides for configuration information.

1

CHAPTER

How to Install and Setup Virtual Juniper Advanced Threat Prevention

Installing the JATP Virtual Core OVA

IN THIS SECTION

Juniper's Advanced Threat Prevention extensible deployment options include a Virtual Core (vCore) detection engine product as an Open Virtual Appliance, or OVA, that runs as a virtual machine. Specifically, an OVA-packaged image is available for VMware Hypervisor for vSphere 6.5, 6.0, 5.5, and 5.0.

The OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the JATP virtual machine template and package (metadata for the OVF package and a JATP software image). The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).

Juniper generates an .ovf and a .vmdk file for every JATP build. Download both the OVF and the VMDK into the same directory. Then, from the vSphere client, click on File -> Deploy OVF Template. Choose the .ovf file and then complete the deployment of the ovf wizard. The configuration wizard prompts for collector/core properties such as IP address, hostname, device key. Log in to the CLI and configure each setting.

vCore Provisioning Requirements and Sizing Options

Table 1: Provisioning Requirements

VM vCenter Version Support	Recommended vCore ESXi Hardware	vCore CPUs	vCore Memory
VM vCenter Server Versions: 6.5, 6.0, 5.5, and 5.0 vSphere Client Versions: 6.5, 6.0, 5.5, and 5.0 ESXi version: 6.0, 5.5.1, and 5.5	Processor speed 2.3-3.3 GHz As many physical CORES as virtual CPUs Hyperthreading: either enable or disable	CPU Reservation: Default CPU Limit: Unlimited Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	Memory Reservation: Default Memory Limit: Unlimited

Table 2: Sizing Options

Model	Number of vCPUs	Memory	Disk Storage
v500M	8	32 GB	Disk 1: 512 G Disk 2: 1 TB
v1G	24	96 GB	Disk 1: 512 G Disk 2: 2 TB

Install the JATP OVA to a VM

NOTE: Starting in release 5.0.5, Windows 10 sandbox is supported (in addition to Windows 7) for behavior analysis. Windows 10 sandbox requires “nested hypervisor support” or “guest VM

hypervisor support" enabled from vSphere. See instructions for "Enable Nested Virtualization for Windows 10 Sandboxing" at the end of this page.

1. Download the JATP OVA file from the location specified by your JATP support representative to a desktop system that can access VMware vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page.
5. Accept the EULA and click Next to view the Name and Location page.
6. A default name is automatically created. Optionally, enter a new name for the Virtual Core.
7. Choose the Data Center on which the vCore will be deployed, then click Next to view the Host/ Cluster page.
8. Choose the host/cluster on which the vCore will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCore virtual machine files, then click Next to view the Disk Format page. The default is THICK PROVISION LAZY ZEROED which requires 512GB of free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported.

   Click Next to view the Network Mapping page.
10. Set up the vCore interface:
    - Management (Administrative): This interface is used for management and to communicate with the JATP Traffic Collectors. Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
    - Click Next to view the JATP Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
    - IP Address: Assign the Management Network IP Address for the vCore.
    - Netmask: Assign the netmask for the vCore.
    - Gateway: Assign the gateway for the vCore.
    - DNS Address 1: Assign the primary DNS address for the vCore.
    - DNS Address 2: Assign the secondary DNS address for the vCore.
12. Enter the Search Domain and Hostname for the vCore.
13. Complete the JATP vCore Settings:

- New JATP CLI Admin Password: this is the password for accessing the vCore from the CLI.
- JATP Central Manager IP Address: If the virtual core is stand-alone (no clustering enabled) or Primary (clustering is enabled), the IP address is 127.0.0.1. If the virtual core is a Secondary, the Central Manager IP address will be the IP address of the Primary.
- JATP Device Name: Enter a unique device name for the vCore.
- JATP Device Description: Enter a description for the vCore.
- JATP Device Key Passphrase: Enter the passphrase for the vCore; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.

14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the vCore model--either 500Mbps, or 1Gbps. Note that it is important to reserve CPU and memory for any virtual deployment.
15. To configure the number of vCPUs and memory:
    a. Power off the virtual collector.
    b. Right click on the virtual collector -> Edit Settings
    c. Select Memory in the hardware tab. Enter the required memory in the Memory Size combination box on the right.
    d. Select CPU in the hardware tab. Enter the required number of virtual CPUs combination box on the right. Click OK to set.
16. To configure CPU and memory reservation:
    a. For CPU reservation: Right click on vCore-> Edit settings:
    b. Select Resources tab, then select CPU.
    c. Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs *processor speed.
    d. For Memory Reservation: Right click on vCore -> Edit settings.
    e. In the Resources tab, select Memory.
    f. Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.
17. If Hyperthreading is enabled, perform the following selections:
    a. Right click on the vCore -> Edit settings.
    b. In the Resources tab, select HT Sharing: None for Advanced CPU.
18. Power on the Virtual Core (vCore).

19. Log into the CLI and use the server mode “show uuid” command to obtain the UUID; send to Juniper to receive your license. Refer to the Operator’s Guide for licensing instructions.

> **NOTE**: When an OVA is cloned to a create another virtual Secondary Core, the value for column "id" in the Central Manager table is the same by default. Admins must reset the UUID to make it unique. A new Virtual Core CLI command “set id” is available to reset the UUID on a cloned Virtual Core from the CLI’s core mode. Refer to the Juniper ATP Appliance CLI Command Reference to review the Core mode "set id" and "show id" commands. Special characters used in CLI parameters must be enclosed in double quotation marks.

Enable Nested Virtualization for Windows 10 Sandboxing

Before You Begin

- The VM should be upgraded to ESXi 6 and later (VMWare version 11).
- Shut down the vJATP VM.

To enable nested virtualization, the “hardware-assisted virtualization” capabilities need to be exposed to the VM, in this case vJATP.

1. Once the VM is powered off, use the vSphere web client to navigate to the **Compatibility** option and select **Upgrade VM Compatibility**.
2. Once the VM compatibility upgrade finishes, use the vSphere web client to navigate to the **Processor Settings** screen. Select the check box next to **Expose hardware-assisted virtualization to the guest operating system**.
3. Click **OK**.

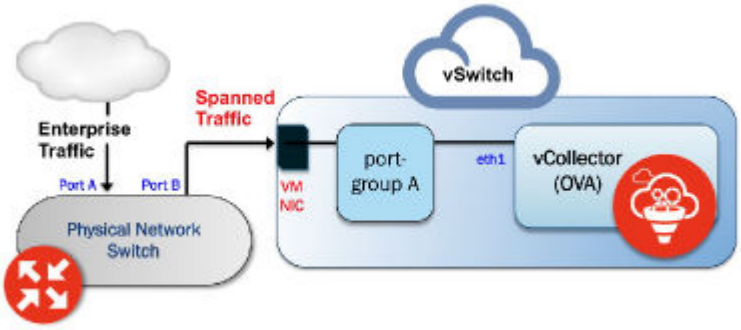
Installing the JATP Virtual Collector OVA

IN THIS SECTION

JATP's extensible deployment options include a Virtual Collector (vCollector) product, as an Open Virtual Appliance, or OVA, that runs in virtual machines. Specifically, a JATP OVA-packaged image is available for VMware Hypervisor for vSphere 6.5, 6.0, 5.5 and 5.0. Virtual Collector models supporting 25 Mbps, 100 Mbps, 500 Mbps and a 1.0 Gbps are available.

An OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the JATP virtual machine template and package: metadata for the OVF package, and a JATP software image. The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).

Figure 1: Both the vSwitch and the port-group are in promiscuous mode



Virtual Collector Deployment Options

Two types of vCollector deployments are supported for a network switch SPAN/TAP:

1. Traffic that is spanned to a vCollector from a physical switch. In this case, traffic is spanned from portA to portB. ESXi containing the JATP vCollector OVA is connected to portB. This deployment scenario is shown in the figure above.

2. Traffic from a virtual machine that is on the same vSwitch as the vCollector. In this deployment scenario, because the vSwitch containing the vCollector is in promiscuous mode, by default all port-groups created will also be in promiscuous mode. Therefore, 2 port groups are recommended wherein port-groupA (vCollector) in promiscuous mode is associated with the vCollector, and port-groupB (vTraffic) represents traffic that is not in promiscuous mode.

NOTE: Traffic from a virtual machine that is not on the same vSwitch as the vCollector is not supported. Also, a dedicated NIC adapter is required for the vCollector deployment; attach the NIC to a virtual switch in promiscuous mode (to collect all traffic). If a vSwitch is in promiscuous mode, by default all port-groups are put in promiscuous mode and that means other regular VMs are also receiving unnecessary traffic. A workaround for that is to create a different port-group for the other VMs and configure without promiscuous mode.

Table 3: Provisioning Requirements for Traffic and Email Collector

VM vCenter Version Support	Recommended vCollector ESXi Hardware	vCollector CPUs	vCollector Memory
VM vCenter Server Version: 6.5, 6.0, 5.5 and 5.0. vSphere Client Version: 6.5, 6.0, 5.5 and 5.0. ESXi version: 5.5.0 and 5.5.1	Processor speed 2.3-3.3 GHz As many physical CORES as virtual CPUs Hyperthreading: either enable or disable	Reservation: Default CPU Limit: Unlimited Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	Memory Reservation: Default Memory Limit: Unlimited

Table 4: Sizing Options for Traffic Collector

Model	Performanc e	Number of vCPUs	Memory	Disk Storage
vC--v500M	500 Mbps	4	16 GB	512 GB
vC--v1G	1 Gbps	8	32 GB	512 GB
vC-v2.5G	2.5 Gbps	24	64 GB	512 GB

Table 5: Sizing Options for Email Collector

Model	Performance	Number of vCPUs	Memory	Disk Storage	Emails/Day
vC--v500M	500 Mbps	8	16 GB	512 GB	720 thousand
vC--v1G	1 Gbps	16	16 GB	512 GB	1.4 million
vC-v2.5G	2.5 Gbps	24	32 GB	512 GB	2.4 million

NOTE: VDS and DVS are not supported in this release.

OVA Deployment vSwitch Setup

1. Identify the physical network adapter from which the spanned traffic is received, then create a new VMware Virtual Switch and associate it with the physical network adapter.
2. Click on Virtual Switch Properties. On the Ports tab, select vSwitch and click on the Edit button.
3. Select the Security tab and change Promiscuous Mode to accept, then click OK. Click OK again to exit.
4. Create a new port-group “vtraffic” in the Virtual Switch. This new port-group will be assigned to your vCollector later. See **vSwitch Tip** below for information about troubleshooting this setup.

To install the Traffic Collector JATP OVA to a VM

1. Download the JATP OVA file to a desktop system that can access VMware vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page.
5. Accept the EULA and click Next to view the Name and Location page.
6. A default name is created for the Virtual Collector. If desired, enter a new name.

7. Choose the Data Center on which the vCollector will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCollector will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCollector virtual machine files, then click Next to view the Disk Format page. The default is THIN PROVISION LAZY ZEROED which requires 512GB of free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported.

   Click Next to view the Network Mapping page.
10. Set up the two vCollector interfaces:
    - Management (Administrative): This interface is used to communicate with the JATP Central Manager (CM). Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
    - Monitoring: This interface is used to inspect and collect network traffic. Assign the destination network to a port-group that is receiving mirrored traffic; this is the port-group "vtraffic" configured in the requirements section above. Click Next to view the JATP Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
    - IP Address: Assign the Management Network IP Address for the Virtual Collector; it should be in the same subnet as the management IP address for the JATP Central Manager.
    - Netmask: Assign the netmask for the Virtual Collector.
    - Gateway: Assign the gateway for the Virtual Collector.
    - DNS Address 1: Assign the primary DNS address for the Virtual Collector.
    - DNS Address 2: Assign the secondary DNS address for the Virtual Collector.
12. Enter the Search Domain and Hostname for the Virtual Collector.
13. Complete the JATP vCollector Settings:
    - New JATP CLI Admin Password: this is the password for accessing the Virtual Collector from the CLI.
    - JATP Central Manager IP Address: Enter the management network IP Address configured for the Central Manager. This IP Address should be reachable by the Virtual Collector Management IP Address.
    - JATP Device Name: Enter a unique device name for the Virtual Collector.
    - JATP Device Description: Enter a description for the Virtual Collector.

- JATP Device Key Passphrase: Enter the passphrase for the Virtual Collector; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.

14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the Virtual Collector model--either 100Mbps, 500Mbps, or 1Gbps. It is important to reserve CPU and memory for any virtual deployment.
15. To configure the number of vCPUs and memory:
    a. Power off the virtual collector.
    b. Right click on the virtual collector -> Edit Settings
    c. Select Memory in the hardware tab. Enter the required memory in the Memory Size combination box on the right.
    d. Select CPU in the hardware tab. Enter the required number of virtual CPUs combination box on the right. Click OK to set.
16. To configure CPU and memory reservation:
    - For CPU reservation: Right click on vCollector-> Edit settings:
    - Select Resources tab, then select CPU.
    - Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs *processor speed.
    - For Memory Reservation: Right click on vCollector -> Edit settings.
    - In the Resources tab, select Memory.
    - Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.
17. If Hyperthreading is enabled, perform the following selections:
    - Right click on the virtual collector -> Edit settings.
    - In the Resources tab, select HT Sharing: None for Advanced CPU.
18. Power on the Virtual Collector.

TIP: **vSwitch** Setup Troubleshooting: If your Virtual Collector is not seeing traffic, (1) confirm your environment setup [ESXi installation with OVA installation of a Juniper ATP Appliance vCollector; your vNIC for traffic collection is connected to a tap-aggregation switch]. (2) Verify symptoms [ESXi host-level interface monitoring shows expected tap traffic levels; TCPdump packet capture shows only spanning-tree traffic and no data; basic system configuration conforms to documentation. Probable Solution: If the switch port preserves

VLAN tags (trunking), set the VMkernel adapter to just look at ALL (4095) VLANs and not only at default VLAN (0) as shown in Settings below:

Figure 2: vSwitch VLAN Troubleshooting Config in port-groups

TIP: Juniper generates an .ovf and a .vmdk file for every release. The .ovf and .vmdk are bundled into a .tar file that you download and expand. For customers who do not want to use vCenter for the virtual collector deployment: download the .tar file and expand both the OVF and the VMDK into the same directory. Then, from the vSphere client, click on File -> Deploy OVF Template. Choose the .ovf file and then complete the deployment of the ovf wizard. The configuration wizard prompts for collector/core properties such as IP address, hostname, device key. Log in to the CLI and configure each setting.

To install the Email Collector JATP OVA to a VM

1. Download the JATP OVA file to a desktop system that can access VMware vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page
5. Accept the EULA and click Next to view the Name and Location page
6. a default name is created for the Virtual Email Collector. If desired, enter a new name.
7. Choose the Data Center on which the vCollector will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCollector will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCollector virtual machine files, then click Next to view the Disk Format page. The default is THIN PROVISION LAZY ZEROED which requires 512GB of

free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported.

Click Next to view the Network Mapping page.

10. Set up the Virtual Email Collector management interface: This interface is used to communicate with the JATP Central Manager (CM). Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
    - IP Address: Assign the Management Network IP Address for the Virtual Collector; it should be in the same subnet as the management IP address for the JATP Central Manager.
    - Netmask: Assign the netmask for the Virtual Collector.
    - Gateway: Assign the gateway for the Virtual Collector.
    - DNS Address 1: Assign the primary DNS address for the Virtual Collector.
    - DNS Address 2: Assign the secondary DNS address for the Virtual Collector.
12. Enter the Search Domain and Hostname for the Virtual Collector.
13. Complete the JATP vCollector Settings:
    - New JATP CLI Admin Password: this is the password for accessing the Virtual Collector from the CLI.
    - JATP Central Manager IP Address: Enter the management network IP Address configured for the Central Manager. This IP Address should be reachable by the Virtual Collector Management IP Address.
    - JATP Device Name: Enter a unique device name for the Virtual Collector.
    - JATP Device Description: Enter a description for the Virtual Collector.
    - JATP Device Key Passphrase: Enter the passphrase for the Virtual Collector; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.
14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the sizing options available). It is important to reserve CPU and memory for any virtual deployment.
15. To configure CPU and memory reservation:
    - For CPU reservation: Right click on vCollector-> Edit settings:
    - Select Resources tab, then select CPU.

- Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs processor speed.
- For Memory Reservation: Right click on vCollector -> Edit settings.
- In the Resources tab, select Memory.
- Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.

16. If Hyperthreading is enabled, perform the followings elections:
    - Right click on the virtual collector -> Edit settings.
    - In the Resources tab, select HT Sharing: None for Advanced CPU.
17. Power on the Virtual Email Collector.