

vMX

---

# vMX Getting Started Guide for AWS

Published  
2020-09-21

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*vMX vMX Getting Started Guide for AWS*

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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 the Documentation | v**

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

## **Overview**

### **vMX and AWS | 11**

vMX Limitations on AWS | 11

vMX Models | 12

2

## **Installing vMX in an AWS VPC**

### **Installing vMX in an AWS VPC | 14**

Creating an SSH Key Pair | 14

Creating a VPC | 15

Creating Network Interfaces | 16

Creating the vMX Instance | 17

Attaching Network Interfaces for WAN Ports | 18

### **Logging In to vMX on AWS | 19**

### **Changing the Interface Type to SR-IOV | 21**

### **Using cloud-init on AWS to Initialize vMX Instances | 22**

3

## **Configuring vMX Chassis-Level Features**

### **Configuring the Number of Active Ports on vMX | 27**

### **Naming the Interfaces | 27**

### **Configuring the Media MTU | 28**

### **Enabling Performance Mode or Lite Mode | 29**

**Tuning Performance Mode | 30**

**Managing vMX Licenses | 31**

Adding a License | 32

Deleting a License | 33

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

## Documentation Conventions

[Table 1 on page vi](#) defines notice icons used in this guide.

Table 1: Notice Icons







| Icon  | Meaning            | Description   |
|---|--------------------|---|
|  | Informational note | Indicates important features or instructions.                               |
|  | Caution            | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning            | Alerts you to the risk of personal injury or death.                         |
|  | Laser warning      | Alerts you to the risk of personal injury from a laser.                     |
|  | Tip                | Indicates helpful information.  |
|  | Best practice      | Alerts you to a recommended use or implementation.                          |

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

| Convention                   | Description   | Examples   |
|------------------------------|---|--|
| <b>Bold text like this</b>   | Represents text that you type.  | To enter configuration mode, type the <b>configure</b> command:<br><br>user@host> <b>configure</b>   |
| Fixed-width text like this   | Represents output that appears on the terminal screen.  | user@host> <b>show chassis alarms</b><br><br>No alarms currently active  |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul> | <ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul> |

Table 2: Text and Syntax Conventions (*continued*)

| Convention                     | Description  | Examples   |
|--------------------------------|--|--|
| <i>Italic text like this</i>   | Represents variables (options for which you substitute a value) in commands or configuration statements.   | Configure the machine's domain name:<br><br>[edit]<br>root@# <b>set system domain-name</b> <i>domain-name</i>  |
| <b>Text like this</b>          | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.              | <ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul> |
| < > (angle brackets)           | Encloses optional keywords or variables.   | <b>stub &lt;default-metric <i>metric</i>&gt;;</b>  |
| (pipe symbol)                  | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | <b>broadcast   multicast</b><br><br><i>(string1   string2   string3)</i>   |
| # (pound sign)                 | Indicates a comment specified on the same line as the configuration statement to which it applies.   | <b>rsvp { # Required for dynamic MPLS only</b>   |
| [ ] (square brackets)          | Encloses a variable for which you can substitute one or more values.   | <b>community name members [ <i>community-ids</i> ]</b>   |
| Indentation and braces ( { } ) | Identifies a level in the configuration hierarchy.   | [edit]<br>routing-options {<br>static {<br>route default {<br>nexthop <i>address</i> ;<br>retain;<br>}<br>}<br>}   |
| ;(semicolon)                   | Identifies a leaf statement at a configuration hierarchy level.  |  |

---

**GUI Conventions**


---

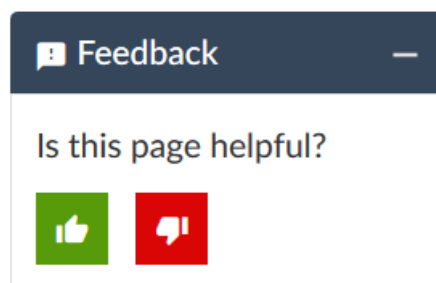
Table 2: Text and Syntax Conventions (*continued*)

| Convention                   | Description  | Examples  |
|------------------------------|--|---|
| <b>Bold text like this</b>   | Represents graphical user interface (GUI) items you click or select. | <ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul> |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections.                  | In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .  |

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are



covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

# 1

CHAPTER

## Overview

---

vMX and AWS | **11**

---

# vMX and AWS

vMX can be deployed in a virtual private cloud (VPC) in the Amazon Web Services (AWS) cloud. You can launch vMX as an Amazon Elastic Compute Cloud (EC2) instance in an Amazon VPC dedicated to a specific user account. vMX Amazon Machine Image (AMI) uses hardware virtual machine (HVM) virtualization.

vMX instances can be used to route between subnets in a VPC or to act as a gateway between a VPC and other VPCs or private networks outside of the AWS environment.

When deploying vMX as a VPC gateway, you might set up your vMX instance as follows:

- Management interface (fxp0) on one subnet
- Each WAN interface (ge-0/0/x) on independent subnets

These interfaces use an Elastic IP address to provide external connectivity by mapping a private IP address to a public IP address. vMX instances use private IP addresses for configuration. AWS transparently handles the mapping between private and public IP addresses using NAT.

## vMX Limitations on AWS

vMX has the following limitations on AWS:

- Maximum number of interfaces for supported instance types is 8.
- Minimum of 4 vCPUs is required and 15 GB memory for lite mode.
- Minimum of 8 vCPUs is required and 15 GB memory for performance mode.

vMX does not support these features on AWS:

- Layer 2 features, and any features or protocols dependent on Layer 2 features
- Attachment or detachment of interfaces while a vMX instance is running
- VLAN tagging
- Jumbo frames (MTU greater than 1500)

## vMX Models

vMX can be deployed using one of these models on AWS:

- Bring Your Own License (BYOL)—Licenses are required to use vMX features with this model. You must order licenses from Juniper Networks and add the license key.
- Pay As You Go (PAYG)—No licenses are required. You can use all vMX features for the available capacity. The selected EC2 instance type determines the available bandwidth.

Some Junos OS software features require a license to activate the feature. To understand more about vMX Licenses, see, *vMX Licenses for AWS*. Please refer to the *Licensing Guide* for general information about License Management. Please refer to the product [Data Sheets](#) for further details, or contact your Juniper Account Team or Juniper Partner.

### RELATED DOCUMENTATION

[vMX Overview](#)

---

[Installing vMX in an AWS VPC | 14](#)

---

[Logging In to vMX on AWS | 19](#)

# 2

CHAPTER

## Installing vMX in an AWS VPC

---

[Installing vMX in an AWS VPC | 14](#)

[Logging In to vMX on AWS | 19](#)

[Changing the Interface Type to SR-IOV | 21](#)

[Using cloud-init on AWS to Initialize vMX Instances | 22](#)

---

# Installing vMX in an AWS VPC

## IN THIS SECTION

- [Creating an SSH Key Pair | 14](#)
- [Creating a VPC | 15](#)
- [Creating Network Interfaces | 16](#)
- [Creating the vMX Instance | 17](#)
- [Attaching Network Interfaces for WAN Ports | 18](#)

This procedure requires you to have an AWS account. Sign in to your AWS account to perform these tasks to install vMX in an AWS VPC.

## Creating an SSH Key Pair

An SSH key pair is required to remotely access a vMX instance in AWS. You can create a new key pair in the EC2 Management Console or import a key pair created by another tool.

To create an SSH key pair:

1. In the AWS Management Console, click **EC2** under Compute to display the EC2 Management Console.
2. In the left navigation pane, click **Key Pairs**. Verify that the region name shown in the toolbar is the same as the region where you created the VPC.
3. Click **Create Key Pair**, specify a key pair name, and click **Create**.
4. Download the private key, where the filename is based on the key pair name you specified (**key-pair-name.pem**), and save it to a secure location.
5. To use an SSH client on a Mac or Linux computer to connect to the vMX instance, use the following command to set the permissions of the private key file so that only you can read it:

```
chmod 400 key-pair-name.pem
```

## Creating a VPC

**NOTE:** You do not have to create a VPC. You can use an existing VPC that is in the same region as your EC2 instance.

To create a VPC, you configure private IP addresses for the network and private IP addresses for the subnet in the VPC, attach an Internet gateway to the VPC, and configure a route table to connect the subnet to the Internet gateway.

To configure the VPC on AWS:

1. In the AWS Management Console, click **VPC** under Networking to display the VPC Management Console.
2. In the left navigation pane, click **Your VPCs** to list configured VPCs. A default VPC that is automatically created is listed.
3. Click **Create VPC**, specify a name and CIDR block of private IP addresses for a new VPC, and click **Yes, Create**.
4. In the left navigation pane, click **Subnets** to list configured subnets.
5. Click **Create Subnet**, specify a name for the subnet, select the VPC, specify the subnet CIDR block within the VPC CIDR, and click **Yes, Create**.

One subnet is created for the management port (fxp0) and a subnet is created for each WAN port on the vMX. These values must be customized depending on your deployment scenario.

6. In the left navigation pane, click **Internet Gateways** to list configured gateways. The Internet gateway routes traffic between the VPC and the Internet. The gateway is required for communications outside of the AWS network.
7. Click **Create Internet Gateway**, specify a name for the gateway, and click **Yes, Create**.
8. Select the gateway, click **Attach to VPC**, select the VPC from the drop-down list to associate the gateway with the VPC, and click **Yes, Attach**.

9. In the left navigation pane, click **Route Tables** to list configured route tables. Select the route table associated with the VPC.
10. Select the **Routes** tab in the bottom section and click **Edit** to add a default route pointing to the Internet gateway. Specify **0.0.0.0/0** as the destination, select the Internet gateway as the target, and click **Save**.

## Creating Network Interfaces

**NOTE:** Make sure the VPC and EC2 instance are in the same region.

To configure the EC2 instance on AWS:

1. In the AWS Management Console, click **EC2** under Compute to display the EC2 Management Console.
2. In the left navigation pane, click **Network Interfaces** to list configured network interfaces.
3. Click **Create Network Interface**, specify a description (used as the Name field), select a subnet, provide an IP address (optional), select a security group to be associated with the network interface, and click **Yes, Create**.

Create one network interface for the management port and one network interface for each WAN port. Copy the description into the Name field for ease of use.

**NOTE:** You can only associate two interfaces when creating the EC2 instance using the Web interface. You must have at least one WAN interface.

4. For each network interface associated with a WAN port, disable the source and destination check.  
Select the network interface, click **Actions**, click **Change Source/Dest. Check**, select **Disabled**, and click **Save**.



**NOTE:** You must disable the source and destination check for each network interface associated with a WAN port.

5. For each network interface connected to vMX, create Elastic IP addresses for external access from the Internet.

In the left navigation pane, click **Elastic IPs**, and click **Allocate New Address**. Select the Elastic IP address, click **Actions > Associate Address**, select the network interface in the Associate Address dialog box, and click **Associate**.

## Creating the vMX Instance

You can create following types of instances on AWS:

- m4.4xlarge
- C4.2xlarge
- C5.2xlarge and C5.4xlarge (from Junos OS Release 19.4R1 onwards)

To configure the vMX instance on AWS:

1. In the AWS Management Console, click **EC2** under Compute to display the EC2 Management Console.
2. In the left navigation pane, click **AMIs** to list available AMIs.
3. Select the vMX AMI and click **Launch**.
4. Choose the instance type and click **Next: Configure Instance Details**.
5. Configure the instance.
  - a. Select the VPC for the Network field, select the management subnet in the Subnet field, and enable Auto-assign Public IP.
  - b. In the Network Interfaces section, select the management interface for the eth0 device as the network interface. Click **Add Device** to add the eth1 device and select the WAN interface as the network interface.

You can configure the instances for the WAN interfaces later.

- c. (Optional, starting with Junos OS Release 17.2R1) In the User data section on the Configure Instance Details page, select **As File** and attach the user-data file. The selected file is used for the initial launch of the instance. See [“Using cloud-init on AWS to Initialize vMX Instances” on page 22](#) for information about how to create the user-data file.

**NOTE:** The Junos OS configuration that is passed as user data is only imported at initial launch. If the instance is stopped and restarted, the user-data file is not imported again.

- d. Click **Next: Add Storage**.
6. You do not need to change any values. Click **Next: Tag Instance**.
7. Specify the vMX instance name as the value for the Name key and then click **Next: Configure Security Group**.
8. Configure the security group with a rule to allow all required protocol traffic to reach the instance. You can create a new security group or select an existing security group.
9. Click **Review and Launch** to review the instance settings, and click **Launch**.
10. Select the SSH key pair you created, select the acknowledgment check box, and click **Launch Instance**.
11. In the left navigation pane, click **Instances** to list the instances.

**NOTE:** The initial boot after installation might take up to 25 minutes. Subsequent boot times might take several minutes.

## Attaching Network Interfaces for WAN Ports

To attach the network interfaces for WAN ports on AWS:

1. In the AWS Management Console, click **EC2** under Compute to display the EC2 Management Console.
2. In the left navigation pane, click **Instances** to list available instances.

3. Select the vMX instance, click **Actions**, select **Networking > Attach Network Interfaces**, and select the network interface to be attached.

For each network interface associated with a WAN port, repeat this step to attach to the vMX instance.

4. To use the attached interfaces, restart the vMX instance.

SEE ALSO

[vMX and AWS | 11](#)

[Logging In to vMX on AWS | 19](#)

## Logging In to vMX on AWS

To log in to vMX or the VCP on AWS, use the SSH protocol to log in to the management interface (fxp0) with username **jnpr** and SSH key pair. The SSH key pair is the same key used when creating the vMX instance. You must set a root password for Junos OS configuration; otherwise, the **commit check** command fails for configuration.

**NOTE:** If you are using the BYOL model and Junos OS Release 15.1F6, log in to the management interface (fxp0) with username **root** and SSH key pair. Starting in Junos OS Release 15.1F6, if you are using the PAYG model or later releases, log in to the management interface (fxp0) with username **jnpr** and SSH key pair.

At a minimum, you must perform these initial Junos OS configuration tasks after logging in to vMX:

1. Start the CLI.

```
root# cli
```

2. Enter configuration mode.

```
root> configure
```

```
[edit]
```

```
root#
```

- Configure the root password.

```
[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

- Configure the WAN interfaces with the same private IP address associated with the AWS network interface.

```
[edit]
root# set interfaces interface-name unit 0 family inet address address
```

For example:

```
[edit]
root# set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.10/24
```

- Commit the configuration.

```
[edit]
root# commit
```

**NOTE:** Starting in Junos OS Release 19.4R1, on AWS management console, system boot-messages are displayed when you boot the VMX instance. You can use these log messages to know the status of the VMX during the booting stage.

### Release History Table

| Release                | Description  |
|------------------------|--|
| <a href="#">15.1F6</a> | Starting in Junos OS Release 15.1F6, if you are using the PAYG model or later releases, log in to the management interface (fxp0) with username jnpr and SSH key pair. |

### RELATED DOCUMENTATION

[vMX and AWS | 11](#)

[Installing vMX in an AWS VPC | 14](#)

[Changing the Interface Type to SR-IOV | 21](#)

[Using cloud-init on AWS to Initialize vMX Instances | 22](#)

## Changing the Interface Type to SR-IOV

For instance types that support Enhanced Networking, you can change the interface type from Xen-PV to SR-IOV. The interface type applies to all interfaces for this instance.

**NOTE:** After you set the interface type to SR-IOV, you cannot change the instance back to the Xen-PV interface type.

To change the interface type, you use CLI tools installed on a separate host. The CLI tools cannot be on the same host as the instance being modified.

To change the interface type to SR-IOV:

1. Shut down the instance being modified.
2. Execute the following commands on a Ubuntu host.

```
$ sudo apt-get install ec2-api-tools
$ export AWS_ACCESS_KEY=access-key
$ export AWS_SECRET_KEY=secret-key
$ export EC2_URL=ec2-url
$ ec2-describe-instance-attribute instance-id --sriov
$ ec2-modify-instance-attribute instance-id --sriov simple
```

For example:

```
$ sudo apt-get install ec2-api-tools
$ export AWS_ACCESS_KEY=ABC123EXAMPLE
$ export AWS_SECRET_KEY=abc123EXAMPLEKEY
$ export EC2_URL=https://ec2.us-west-1.amazonaws.com
$ ec2-describe-instance-attribute i-0abc9cde12f345 --sriov
sriovNetSupport i-0abc9cde12f345
```

```
$ ec2-modify-instance-attribute i-0abc9cde12f345 --sriov simple  
sriovNetSupport i-abc9cde12f345 simple
```

3. Start the instance with SR-IOV network interfaces.

## RELATED DOCUMENTATION

[Installing vMX in an AWS VPC | 14](#)

[Logging In to vMX on AWS | 19](#)

[Using cloud-init on AWS to Initialize vMX Instances | 22](#)

# Using cloud-init on AWS to Initialize vMX Instances

Starting with Junos OS Release 17.2R1, when you create the vMX instance, you can use **cloud-init** services on AWS to pass a valid Junos OS configuration file as user data to initialize the vMX instance. The user-data file uses the standard Junos OS syntax to define all the configuration details for your vMX instance. The user-data file cannot exceed 16 KB. If your user-data file exceeds this limit, you must compress the file using gzip and use the compressed file. For example, the **gzip junos.conf** command results in the **junos.conf.gz** file.

The configuration must be validated and include details for the fxp0 interface, login, and authentication. It must also have a default route for traffic on fxp0. This information must match the details of the AWS VPC and subnet into which the instance is launched. If any of this information is missing or incorrect, the instance is inaccessible and you must launch a new one.

**NOTE:** The Junos OS configuration that is passed as user data is only imported at initial launch. If the instance is stopped and restarted, the user-data file is not imported again.

To create the user-data file:

1. Create a file in plaintext with the Junos OS syntax and save it.

**NOTE:** The string **#junos-config** must be the first line of the user-data file before the Junos OS configuration.

2. (Optional) You can use special tags in the configuration. The following special tags are case-sensitive and are replaced by the corresponding information at run-time.

| Tag      | Replaced With                                  |
|----------|--|
| FXPOADDR | IP address/mask of the first network interface |
| GATEWAY  | IP address of the default gateway              |
| SSHRSKEY | SSH public key specified during launch         |
| HOSTNAME | Hostname assigned by DHCP to the instance      |

3. To specify the user-data file for configuring the vMX instance, select **As File** in the User data section on the Configure Instance Details page and attach the file. The selected configuration file is used for the initial launch of the instance.

This sample user-data file is the default file that is used when you do not specify a file. It uses the special tags in the configuration.

```
#junos-config
groups {
  global {
    system {
      host-name HOSTNAME;
      services {
        ssh {
          root-login deny-password;
        }
      }
      login {
        user jnpr {
          uid 2000;
          class super-user;
          authentication {
            ssh-rsa "SSHRSKEY"; ## SECRET-DATA
          }
        }
      }
    }
    syslog {
      user * {
        any emergency;
      }
    }
  }
}
```





Logging In to vMX on AWS | 19

---

Changing the Interface Type to SR-IOV | 21

---

Using cloud-init on AWS to Initialize vMX Instances | 22

# 3

CHAPTER

## Configuring vMX Chassis-Level Features

---

Configuring the Number of Active Ports on vMX | 27

Naming the Interfaces | 27

Configuring the Media MTU | 28

Enabling Performance Mode or Lite Mode | 29

Tuning Performance Mode | 30

Managing vMX Licenses | 31

---

# Configuring the Number of Active Ports on vMX

You can specify the number of active ports for vMX. The default number of ports is 10, but you can specify any value in the range of 1 through 23. You can change this number if you want to limit the number of Ethernet interfaces in the VCP VM to match the number of NICs added to the VFP VM.

**NOTE:** If you are running virtio interfaces in lite mode, you can use up to 96 ports.

Other configurations running in performance mode support up to 23 ports.

To specify the number of active ports, configure the number of ports at the `[edit chassis fpc 0 pic 0]` hierarchy level.

```
[edit]
```

```
user@vmx# set chassis fpc 0 pic 0 number-of-ports
```

## RELATED DOCUMENTATION

---

[Naming the Interfaces | 27](#)

---

[Configuring the Media MTU | 28](#)

---

[Enabling Performance Mode or Lite Mode](#)

---

[Tuning Performance Mode | 30](#)

## Naming the Interfaces

vMX supports the following interface types:

- Gigabit Ethernet (ge)
- 10-Gigabit Ethernet (xe)
- 100-Gigabit Ethernet (et)

By default, the interfaces come up as ge interfaces with 1 Gbps bandwidth in the Junos OS configuration. The default port speed values for the interface types are 1 Gbps (ge), 10 Gbps (xe), and 100 Gbps (et). If you do not enable schedulers, the speed is only for display purposes and is not enforced. If you enable

schedulers, the transmit rate of the port is limited to the speed unless it is overridden by the shaping rate in the CoS configuration.

To specify the interface types, configure the interface type at the `[edit chassis fpc 0 pic 0]` hierarchy level.

```
[edit]
```

```
user@vmx# set chassis fpc 0 pic 0 interface-type (ge | xe | et)
```

## RELATED DOCUMENTATION

---

[Configuring the Number of Active Ports on vMX | 27](#)

---

[Configuring the Media MTU | 28](#)

---

*Enabling Performance Mode or Lite Mode*

---

[Tuning Performance Mode | 30](#)

# Configuring the Media MTU

For vMX, you can configure the media MTU in the range 256 through 9500.

**NOTE:** For VMware, the maximum value is 9000. For AWS, the maximum value is 1514.

You configure the MTU by including the `mtu` statement at the `[edit interface interface-name]` hierarchy level.

```
[edit]
```

```
user@vmx# set interface ge-0/0/0 mtu bytes
```

## RELATED DOCUMENTATION

---

[Configuring the Number of Active Ports on vMX | 27](#)

---

[Naming the Interfaces | 27](#)

---

*Enabling Performance Mode or Lite Mode*

---

[Tuning Performance Mode | 30](#)

## Enabling Performance Mode or Lite Mode

vMX can be configured to run in two modes depending on the use case.

- Lite mode—Needs fewer resources in terms of CPU and memory to run at lower bandwidth.
- Performance mode—Needs higher resources in terms of CPU and memory to run at higher bandwidth.

**NOTE:** Performance mode is enabled implicitly by default.

When you enable performance mode, make sure you have configured the proper number of vCPUs and memory for your VMs based on your use case.

To calculate the minimum number of vCPUs needed by VFP for performance mode:  $(4 * \text{number-of-ports}) + 4$ .

You can explicitly enable performance mode by including the **performance-mode** statement at the **[edit chassis fpc 0]** hierarchy level.

```
[edit]
```

```
user@vmx# set chassis fpc 0 performance-mode
```

If you are using paravirtualized network interfaces such as virtio (for KVM) or VMXNET3 (for VMware) for lab simulation use cases, you can disable performance mode by including the **lite-mode** statement at the **[edit chassis fpc 0]** hierarchy level.

```
[edit]
```

```
user@vmx# set chassis fpc 0 lite-mode
```

[Table 3 on page 29](#) highlights some of the challenging features which are supported in the Fast Path and some which are not supported. Features which are not supported in the Fast Path still work but they get less than 100K PPS per worker vCPU.

**Table 3: Features Support in Fast Path**

| Features  | Support in Fast Path |
|---|----------------------|
| Pseudowire Headend Termination (PWHT) (Layer 2 VPN) | Not Supported        |

Table 3: Features Support in Fast Path (continued)

| Features  | Support in Fast Path |
|---|----------------------|
| L2 circuit  | Not Supported        |
| Ethernet VPN (EVPN)   | Not Supported        |
| Virtual Extensible LAN protocol (VXLAN)                     | Not Supported        |
| MPLS-over-UDP (MPLSoUDP)                                    | Not Supported        |
| Inline J-flow   | Supported            |
| Pseudowire Headend Termination (PWHT) (Layer 3 VPN and IP ) | Supported            |
| GRE   | Supported            |
| logical tunnel interfaces (lt)                              | Supported            |

## RELATED DOCUMENTATION

[Tuning Performance Mode](#) | 30

# Tuning Performance Mode

To tune performance mode for the traffic, you can specify the number of Workers dedicated to processing multicast and control traffic. You can specify any value in the range of 0 through 15. The default of 0 specifies that all available Workers are used to process all traffic.

The number of dedicated Workers specified in relation to the number of available Workers results in the following behavior:

- If the number of dedicated Workers is greater than or equal to the number of available Workers, then all available Workers are used to process all traffic.
- If the number of dedicated Workers is less than the number of available Workers, then the first set of available Workers (equal to the specified number of dedicated Workers) is used to process multicast and control traffic while the remaining available Workers are used to process flow cache traffic.

To specify the number of dedicated Workers for processing multicast and control traffic, configure the number of Workers at the [edit chassis fpc 0 performance-mode] hierarchy level.

```
[edit]
```

```
user@vmx# set chassis fpc 0 performance-mode number-of-ucode-workers number-workers
```

**NOTE:** Changing the number of Workers reboots the FPC.

## RELATED DOCUMENTATION

*Enabling Performance Mode or Lite Mode*

*performance-mode*

# Managing vMX Licenses

## IN THIS SECTION

- [Adding a License | 32](#)
- [Deleting a License | 33](#)

You must add a license to use vMX features. The licensed features are enforced based on the license you purchased.

Starting in Junos OS Release 17.4 for AWS, you must add a license if you are using vMX in the Bring Your Own License (BYOL) model.

If you upgrade from a BASE package license to an ADVANCE or PREMIUM package license or if you downgrade from an ADVANCE or PREMIUM package license to a BASE package license, you must restart the routing protocol process (**restart routing**). If your configuration has logical systems, you must restart the routing protocol process for all logical systems (**restart routing logical-system *logical-system-name***).

If you need to move your vMX installation to another host, you must remove vMX from the current host before installing vMX and adding the license on the new host.

## Adding a License

To add a license key to the vMX:

1. Copy the license activation key file to the VCP and add the license key by specifying the filename.

```
user@vmx> request system license add filename
```

Or, you can copy and paste the license activation key directly to add the license key. For example:

```
user@vmx> request system license add terminal
XXXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX
          XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX
          XXXXXXX XXXXXXX
```

2. Verify that the license is installed. VMX-BANDWIDTH indicates the licensed bandwidth (in Mbps) and VMX-SCALE indicates the application package. (VMX-SCALE 1 is the BASE package, VMX-SCALE 2 is the ADVANCE package, and VMX-SCALE 3 is the PREMIUM package.) This information is also listed as Features in the Licenses installed section. For example, this output indicates that the 40G perpetual license for the PREMIUM application package is installed.

```
user@vmx> show system license
```

```
License usage:

```

| Feature name     | Licenses used | Licenses installed | Licenses needed | Expiry    |
|------------------|---------------|--------------------|-----------------|-----------|
| scale-subscriber | 0             | 1000               | 0               | permanent |
| scale-l2tp       | 0             | 1000               | 0               | permanent |
| scale-mobile-ip  | 0             | 1000               | 0               | permanent |
| VMX-BANDWIDTH    | 40000         | 40000              | 0               | permanent |
| VMX-SCALE        | 3             | 3                  | 0               | permanent |

```
Licenses installed:
License identifier: JUNOS640113
License version: 4
Software Serial Number: XXXXXXXX
Customer ID: vMX-Juniper
Features:
```



```

vmx-bandwidth-40g - vmx-bandwidth-40g
    permanent
vmx-feature-premium - vmx-feature-premium
    permanent

```

3. Verify the configured bandwidth for PFE traffic matches the licensed bandwidth (VMX-BANDWIDTH). The current and average bandwidth are also displayed.

```
user@vmx> show pfe statistics traffic bandwidth
```

```

Configured Bandwidth      : 40000000000 bps
Bandwidth                  : 0 bps
Average Bandwidth         : 0 bps

```

## Deleting a License

To delete a vMX license:

1. Display the installed licenses.

```
user@vmx> show system license installed
```

```

License identifier: JUNOS640113
License version: 4
Features:
  vmx-bandwidth-40g - vmx-bandwidth-40g
    permanent
  vmx-feature-premium - vmx-feature-premium
    permanent

```

2. Delete the license.

```
user@vmx> request system license delete license-identifier
```

For example:

```
user@vmx> request system license delete JUNOS640113
```

3. Verify that the license is deleted.

```
user@vmx> show system license
```

```
License usage:

Feature name          Licenses used   Licenses installed Licenses needed  Expiry
scale-subscriber      0              1000             0               permanent
scale-l2tp            0              1000             0               permanent
scale-mobile-ip       0              1000             0               permanent

Licenses installed: none
```

### Release History Table

| Release              | Description  |
|----------------------|--|
| <a href="#">17.4</a> | Starting in Junos OS Release 17.4 for AWS, you must add a license if you are using vMX in the Bring Your Own License (BYOL) model. |