SOFTWARE INSTALLATION GUIDE

Extreme Virtual TAP 2.0.0 Software Installation Guide

9035938-00
13 February 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
`Courier font`	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   NOTE
   You can modify your product selections or unsubscribe at any time.

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Started

Extreme Virtual TAP (vTAP) is a full-featured network visibility solution built for virtualized service provider and enterprise networks. It offers an end-to-end set of capabilities including traffic interception, filtering, load-balancing, and optimization for network monitoring and analytics tools. vTAP addresses the visibility challenge in virtual workloads.

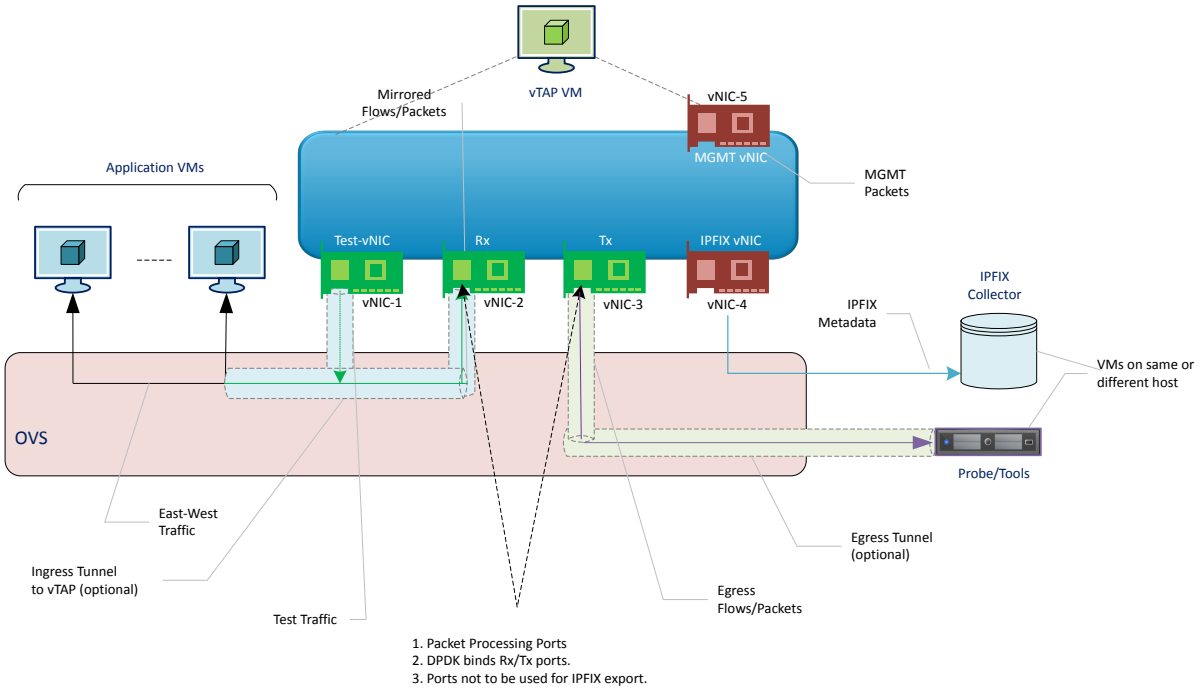
vTAP can perform various operations such as filtering (SMARTMatch), forwarding, VLAN tag insertion/deletion, header stripping, packet slicing, sampling and IPFIX export.

vTAP runs on a VM with KVM as the hypervisor host.

Deployment architecture

The image below shows a typical vTAP deployment on a KVM hypervisor:

FIGURE 1 Deployment architecture



vTAP is based on CentOS 7.2 and DPDK, and deployed using KVM-based qcow2 image. The vTAP qcow2 image is preconfigured with five vNICs: Rx (for receiving ingress packets), Tx (for sending packets post-processing), Test (for sending test packets), IPFIX Export (for exporting IPFIX metadata), and Management.

- Configure the OVS so that the traffic to be monitored is mirrored to vTAP.
- To monitor traffic from multiple switches, one instance of vTAP must be deployed per switch, since the Rx vNIC cannot be part of multiple switches at the same time. To avoid traffic flooding, ensure that the vTAP Rx vNIC and Tx vNIC are on separate OVS switches.
- If required, the mirrored traffic may be forwarded in a GRE, VXLAN, IPIP, or ERSPAN tunnel to vTAP with the Rx VNIC IP address as the destination address. vTAP terminates these tunnels and processes the flows/packets inside these tunnels.
- After processing the flows/packets, vTAP sends the packets to the configured probes/tools. vTAP can be configured to send out the egress packets with VLAN tags, or in a GRE/VxLAN tunnel.
- vTAP supports metadata export in IPFIX format based on the configuration. IPFIX export can be configured using the dedicated vNIC or the management vNIC.
- vTAP supports a Test vNIC for sending a test pcap to the Rx interface. The underlying switch must be appropriately configured such that the Test vNIC and Rx vNIC are on the same bridge.

System requirements

The table below shows the system specifications for vTAP qcow2 image. Ensure that the KVM hypervisor meets these requirements:

TABLE 1 System requirements

Entity	Specification	
vCPU	2	
RAM	4 GB	
HDD	16 GB	
vNIC	5	
Driver	e1000	
Hypervisor	qemu-kvm 1.5.3	
OS	**Release version**	**Kernel version**
	CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux	3.10.0-327.el7.x86_64

Downloading the distribution

Perform the following steps to download the distribution for Virtual TAP (vTAP) 2.0.0 from the Extreme Networks website:

1. Go to the Extreme Portal website and log in with your username and password.
2. If you are visiting Extreme Portal for the first time, click **Register Now** instead and follow the prompts to register.
   You may need to enter the access code/serial number you received in your order confirmation e-mail to view and download all files.
3. On the main page, click **Products** and then click **NetworkPacketBroker**.
4. On the **NetworkPacketBroker** page, click **Virtual TAP**.
   A list of products is displayed.

5. Go to:
   - **Software / Release Notes** > **Software & Downloads** > **2.0.0** for vTAP installation files.
   - **Software / Release Notes** > **Release Notes** for vTAP Release Notes.
   - **Documentation** > **2.0.0** for vTAP documentation.

   The table below provides information about all the files available for download:

TABLE 2 Virtual TAP files

Path	Filename	Description
Software / Release Notes > **Software & Downloads** > **2.0.0**	vtap-2.0.0-0-qcow.tar.gz	This tar archive includes the following files: • config_env.sh • preseed_config_kvm.xml • vtap-2.0.0-0.qcow2
Software / Release Notes > **Release Notes**	ExtremeVirtualTap2.0.0ReleaseNotes.pdf	Extreme Virtual TAP Release Notes
Documentation > **2.0.0**	ExtremeVirtualTap2.0.0SoftwareInstallation.pdf	Extreme Virtual TAP Software Installation Guide
	ExtremeVirtualTap2.0.0AdministrationGuide.pdf	Extreme Virtual TAP Administration Guide
	ExtremeVirtualTap2.0.0CommandReferenceGuide.pdf	Extreme Virtual TAP Command Reference Guide
	ExtremeVirtualTap2.0.0RESTAPIGuide.pdf	Extreme Virtual TAP REST API Guide

6. Click a file to download.
7. Save the file to a local directory on your system.

Extreme Virtual TAP installation

This chapter provides information about installing Extreme Virtual TAP (vTAP).

Prerequisites

Before deploying vTAP, ensure that the following are available:

- **Hypervisor**: QEMU-KVM

  vTAP is packaged in the QCow2 file format (defined by QEMU), and it must be deployed on a KVM hypervisor. KVM is an open-source hypervisor for Linux OS.

- **Virtual network**: Open vSwitch (OVS) bridge

  Two mandatory OVS bridges must be created: One for management and another for ingress (Rx) interface. In addition, as per your setup, configure another OVS bridge for egress (Tx) interface.

  CAUTION
  Ensure that ingress (Rx) and egress (Tx) interfaces are not configured on the same OVS bridge.

- **IP address**: One IP address for the management port, so that you can remotely access the vTAP VM using the management port.

  In addition, as per your setup, one IP address for ingress (Rx) and another for egress (Tx).

- **X11 Forwarding through SSH**:
  - An X Window Server for Windows OS, such as xming or VNC.
  - An SSH Client, such as PUTTY: When setting up PUTTY connection, enable X11 Forwarding.

Deploying Virtual TAP using qcow2 image

NOTE
Before deploying Virtual TAP (vTAP), configure OVS and the underlying network such that:

- vTAP's Rx vNIC correctly receives the ingress packets
- The egress packets are correctly routed to the destination through the Tx vNIC

Perform the following steps to deploy vTAP using qcow2 image:

1. Use SSH to log in to the KVM hypervisor as the root user.
2. Download the tar archive `vtap-2.0.0-0-qcow.tar.gz` to your KVM hypervisor-based server.

   NOTE
   For information about downloading the tar archive, see the section Downloading the distribution on page 10.

3. Run the following command to extract the contents of the downloaded tar archive `vtap-2.0.0-0-qcow2.tar.gz` to a location of your choice:

   ```
   tar -xvzf vtap-2.0.0-0-qcow2.tar.gz
   ```

   The tar archive includes the following files:

   - config_env.sh
   - preseed_config_kvm.xml
   - vtap-2.0.0-0.qcow2

4. Backup the `preseed_config_kvm.xml` file, as this file is overwritten during installation.
5. Run the following commands to provide execute permissions for the files `config_env.sh` and `vtap-2.0.0-0.qcow2`.

   ```
   chmod 755 config_env.sh
   chmod 755 vtap-2.0.0-0.qcow2
   ```

6. Run the following command:

   `./config_env.sh -n <vm_name> -p <path_to_qcow2>`

   - **vm_name**: Provide a meaningful name for the vTAP VM.
   - **path_to_qcow2**: This is the absolute path to the vTAP qcow2 image you downloaded.

   Example

   ```
   ./config_env.sh -n myvm1 -p /root/vtap_image/vtap_qcow2
   ```

7. Run the following virsh command to define the QEMU domain (myvm1) from the `preseed_config_kvm.xml` file:

   ```
   virsh define preseed_config_kvm.xml
   ```

   Example

   ```
   [root@localhost]# virsh define preseed_config_kvm.xml
   Domain myvm1 defined from preseed_config_kvm.xml
   ```

8. Run the following command to start virt-manager. The tool virt-manager enables you to use a graphical interface (such as Xming) to interact with KVM.

   ```
   virt-manager
   ```

   This launches the X Window System (such as Xming), which is used for managing virtual machines, including the vTAP VM.

9. Create the appropriate bridges as per your setup and attach the eth interfaces in OVS.

   NOTE
   Two mandatory OvS bridges must be created: One for management and another for ingress (Rx).

   For recommended OvS configuration, see Recommended Open vSwitch configuration on page 25.

10. Power on the vTAP VM.

    vTAP installation is now complete.

    NOTE

    When you run the vTAP VM, the following error message might be displayed:

    `Error starting domain: Cannot access storage file '/root/<installation_directory>/vtap-2.0.0/: Permission denied.`

    To fix this issue, perform the following steps:

    1. Open the file `/etc/libvirt/qemu.conf`.
    2. Search for **`user = "<username>"`** and **`group = "<username>"`**, where `usename` is the KVM hypervisor user.

       For example: **`user = "root"`** and **`group = "root"`**
    3. Uncomment these lines, and save file and exit.
    4. Run the following command to restart libvirtd:

       ```
       systemctl restart libvirtd
       ```

    5. Run the following command to start virt-manager:

       ```
       virt-manager
       ```

Uninstalling/reinstalling Virtual TAP

Perform the following steps to uninstall/reinstall Virtual TAP (vTAP):

1. Go to the directory where the tar archive `vtap-2.0.0-0-qcow2.tar.gz` was extracted and delete the following files:
   - config_env.sh
   - preseed_config_kvm.xml
   - vtap-2.0.0-0.qcow2
2. Install vTAP again by performing all the steps in the section Deploying Virtual TAP using qcow2 image on page 13.

Extreme Virtual TAP configuration

This chapter provides information about configuring Virtual TAP (vTAP).

Configuring vTAP

NOTE

Before performing the steps below, configure OVS and the underlying network such that:

- vTAP's Rx vNIC correctly receives the ingress packets
- The egress packets are correctly routed to the destination through the Tx vNIC
- All five vTAP vNICs are configured to use e1000 driver.

  Run `ifconfig` command to view vTAP interface names. Run `ethtool -i <interface_name>` command to view vNIC driver information.

When you login to the vTAP VM for the very first time, it displays a startup script, enables you to configure various settings for vTAP.

You can exit the startup script at any point by pressing **CTRL+C**. However, it is highly recommended that you complete all the steps using the startup script.

Perform the following steps to configure vTAP settings:

1. Log on to the vTAP VM with the following credentials:
   - **localhost login**: root
   - **Password**: password
2. The following screen is displayed. Press **Enter** to begin:

```
================================================================
Extreme Networks - vTAP
- Welcome to the vTAP Setup
================================================================
Typically a default value is displayed in brackets.
Pressing the [enter] key without entering a new value will use the
bracketed value and proceed to the next item.

If a default value cannot be provided, the prompt will indicate that the item
is either (Required) or (Optional). The [enter] key may be pressed without
entering data for (Optional) items. A value must be entered for (Required) items
================================================================
Press [enter] to begin setup or CTRL-C to exit:
```

3. **Root Password Configuration**

   The following screen is displayed:

```
================================================================
Root Password Configuration
================================================================
There is currently no password set in the system administrator account (root).
It is recommended that you set one so that it is active the first
time the machine is rebooted.
================================================================
Would you like to set a root password (y/n) [y]?
```

   This configures the same password for both the root user and vTAP (SSH/Telnet):

   a) The default password is `password`. Enter **Y** to set a new password.

      NOTE

      Enter **N** to continue without changing the default password.

   b) Enter the new password and press **Enter**.

   c) Re-enter the same password and press **Enter**.

      NOTE

      Ignore the following message:

```
BAD PASSWORD: The password fails the dictionary check - it is based on a
dictionary word.
```

4. **Host Name Configuration**

   The following screen is displayed:

```
================================================================================
Host Name Configuration
================================================================================

Please enter new hostname for vTAP [localhost.localdomain]:
```

   This configures a new hostname for vTAP.

   - The default hostname is `vTAP`. To continue without changing the default hostname, press **Enter**.
   - To change the hostname, enter a new hostname and press **Enter**.

5. **Interface Configuration**

   The following screen is displayed:

```
Select the interface for configuration
1) Egress
2) Ingress
3) Management
4) Flow Exporter
5) Test Interface
6) None
Please choose option:
```

   This configures the following interfaces:

   - **Egress**: For sending packets post-processing
   - **Ingress**: For receiving ingress packets
   - **Management (mgmt)**: For management
   - **IPFIX (flowexporter)**: For exporting IPFIX metadata
   - **Test interface (testintf)**: For sending a test pcap to the Rx interface

   a) Enter **1**, **2**, **3**, **4**, or **5** to configure a specific interface.

      The following screen is displayed:

```
Configure the interface using static IP or DHCP:
1) Static
2) DHCP
3) Quit
Please choose option:
```

      NOTE

      It is recommended that you configure the Management (mgmt) interface for remote access to vTAP.

   b) Enter **1** to configure the selected interface with a static IP address and enter the following information:

```
Please enter the IP address for 'mgmt' (Required): 10.1.1.1
Enter the IPv4 subnet prefix for 'mgmt' (Required): 20
Enter the gateway address (Optional): 10.1.1.2
```

      or

   c) Enter **2** for DHCP. vTAP automatically acquires DHCP server information.

      or

   d) Enter **6** to continue with default configuration for all interfaces. This, however, is not recommended.

6. **DNS Configuration**

   The following screen is displayed:

```
New configuration will overwrite existing DNS configuration
Do you want to configure DNS:(Y/N)
```

   Enter **y** to configure a DNS server.

```
Enter primary DNS Domain Name[nameserver]: Primary
Please enter the IP address for Primary (Required): 10.1.1.1
Inter the secondary DNS name server (Optional):
```

   a) Primary DNS Domain Name[nameserver]:

   b) **IP address for Primary (Required)**: Enter the IP address of the name server.

   c) Secondary DNS name server (Optional):

7. **Date and Time Configuration**

   The following screen is displayed:

```
================================================================
Configure Date And Time Settings
================================================================
The engine date and time can be set manually or using an external
Network Time Protocol (NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5
server IP addresses may be entered if NTP is used.
================================================================
Do you want to use NTP (y/n) [n]?
```

   a) Enter **y** to use an external Network Time Protocol (NTP) server and enter the NTP server IP address(es).

      NOTE

      Enter **n** to configure the date and time manually and proceed to the next step.

      NTP Server

```
Please enter an NTP Server IP address: 10.37.138.181

Would you like to add another server (y/n) [y]?
```

      In the NTP Servers validate selection screen, enter **0** to accept the current settings and proceed to the Set Time Zone screen.

```
================================================================================
NTP Servers
================================================================================
These are the currently specified NTP Servers:

10.37.138.181

Enter 0 or any key other than a valid selection to complete NTP configuration and
continue.
If you need to make a change, enter the appropriate number from the
choices listed below.

0. Accept the current settings and continue
1. Restart NTP server selection
2. Set date and time manually
================================================================================
Enter selection [0]:
```

   b) If you answered no to using an NTP server to set date and time, set the date and time in the Set Date and Time screen:

```
Set Date And Time

The current system date and time is: Sun 06 Jan 2019 08:25:02 AM UTC
Please enter the values for date and time as directed where input is expected in
the following format:

MM   - 2 digit month of year
ID   - 2 digit day of month
YYYY - 4 digit year
hh   - 2 digit hour of day using a 24 hour clock
mm   - 2 digit minute of hour
ss   - 2 digit seconds

Please enter the month [01]:
```

```
Please enter the day of the month [06]:
Please enter the year [2019]:
Please enter the hour of the day [11]:
Please enter the minutes [14]:
Please enter the seconds [14]:
```

c) In the Use UTC screen, select whether you want the system clock to be set to use UTC.

```
================================================================================
Use UTC
================================================================================
The system clock can be set to use UTC. Specifying no for using UTC
sets the hardware clock using localtime.
================================================================================
Do you want to set the clock using UTC (y/n) [n]:
```

In the Set Time Zone screen, type the number that corresponds to the appropriate time zone and press **Enter**.

```
================================================================
Set Time Zone
================================================================
You will now be asked to enter the time zone information for this system.
Available time zones are stored in files in the /usr/share/zoneinfo directory.
Please select from one of the following example time zones:
1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
================================================================
Enter selection [1]:
```

8. **SNMP Configuration**

   The following screen is displayed:

```
SNMP Configuration

 The following information will be used to configure SNMP management of this device.
 The SNMP information entered here must be used to contact this device
 with remote management applications

SNMP Configuration.

Please enter rocommunity [public]: test1
Please enter rwcommunity [private]: test2
Please enter trapcommunity [vTAP]: test3
Please enter username[testuser1]: testuser
Please enter authentication pass-phrase[authpass]: passwordl
Please enter encryption pass-phrase[encryptpassl: passwordl
Please enter the IP address of the SNMP Manager[127.0.0.1]:

Do you want to configure another Manager:(Y/N)
```

   This configures SNMP agent.

   a) Enter the following to configure the SNMP agent:
      - **rocommunity**: Specifies the read-only community string.
      - **rwcommunity**: Specifies the read-write community string.
      - **trapcommunity**: Specifies the community string for the traps.
      - **username**: Specifies a username for SNMPv3 user.
      - **authentication pass-phrase**: Specifies passphrase for authentication for the SNMPv3 user.
      - **encryption pass-phrase**: Specifies passphrase for encryption for the SNMPv3 user.
      - **IP address of the SNMP Manager**: Specifies the IP address of the SNMP manager.

9. **vTAP Settings**

   The following screen is displayed:

```
================================================================
vTAP Settings
================================================================

Enter 0 to accept the current settings and continue.
If you need to make a change, enter the appropriate number.

0. Accept settings and continue
1. Access interface IP setting:
2. SNMP User:
3. Modify all settings
================================================================

Enter selection [0]:
```

   a) Enter **0** to accept the settings and continue.

      or

   b) Enter **1**, **2** or **3** to edit settings.

vTAP configuration is now complete. vTAP starts automatically.

Re-running startup script

To restart the startup script again after exiting, run the following command:

```
/etc/extvsiblity/scripts/startup.sh -r
```

This stops the vTAP service and starts the startup script.

> NOTE
> Restarting the startup script overwrites all previously configured settings.

Appendix

Recommended Open vSwitch configuration

CAUTION
Ensure that ingress (Rx) and egress (Tx) are not configured on the same OVS bridge.

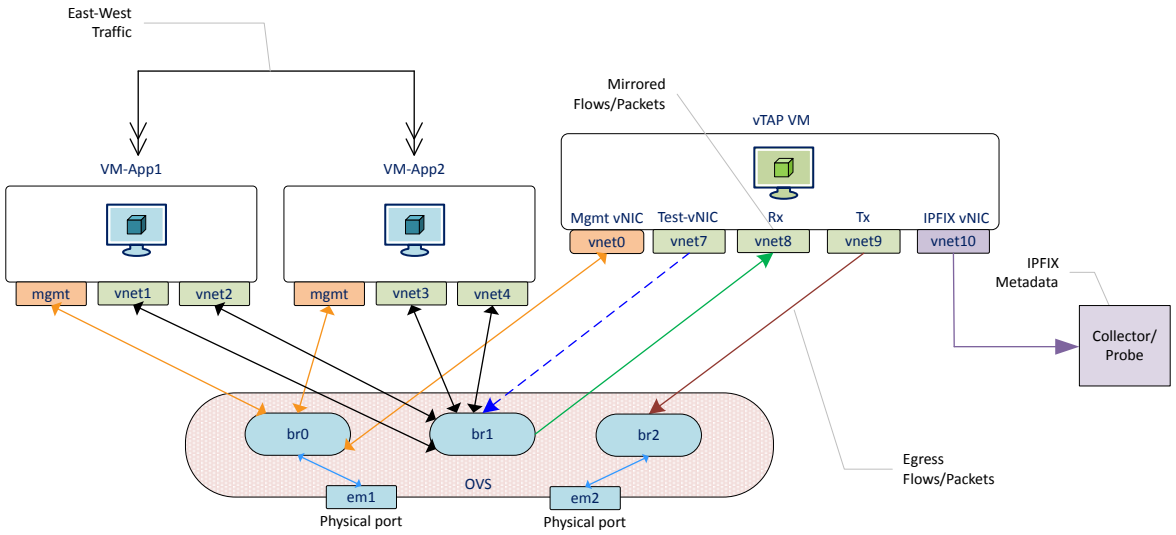
TABLE 3 Recommended OVS configuration

Interface	Bridge/description
Management	Mandatory OVS bridge 1.
Ingress (Rx)	Mandatory OVS bridge 2.
Egress (Tx)	Configure an OVS bridge based on your setup.
IPFIX	The IPFIX export cannot use the virtual interfaces that is used for packet processing. The virtual interface required for the IPFIX export must be configured on the VM. The IP address for the IPFIX interface must be configured using the startup script. For more information, see the section Configuring vTAP on page 17. Optionally, the management virtual interface may be used for IPFIX export.
Test interface	Configure the Test interface and the Rx interface to be on the same bridge.

Sample Open vSwitch configuration for vTAP

This section provides information about a sample Open vSwitch (OVS) configuration for vTAP.

FIGURE 2 Topology



In the above topology image, east-west traffic flows between VM App1 and VM App2 through two NIC cards, vnet1 and vnet2.

- **Management**
  - **OVS-br0**: This is the OVS bridge created for management access for all VMs. Hence all management vNICs (bound with respective VM IP) and one physical port (that connects to the external network for SSH access of VMs and host machine) are bound to OVS-br0 bridge.
  - Management port is connected to the outer network using OVS-br0 bridge through the physical port em1.
- **Ingress**
  - **OVS-br1**: This is the OVS bridge created for east-west traffic between VM App1 and VM App2 through two NIC cards, vnet1 and vnet2 (black line in the image above). This traffic is mirrored to vTAP.
  - **Port Mirroring**: This is done on the OVS-br1 bridge. Mirrored traffic is sent to the vTAP Rx port (vnet8).
  - **East-West traffic**: This is the traffic between VM App1 and VM App2 using vNIC port (vnet1, vnet2, vnet3, vnet4) and OVS-br1 bridge.
- **Egress**: **OVS-br2** is the OVS bridge that vTAP uses as egress for forwarding packets.

Create the appropriate OVS bridges and attach the eth interfaces:

- Use the following commands to create the bridges and add ports:

```
ovs-vsctl add-br <bridgeName>
ovs-vsctl add-port <bridgeName> <portName>
```

Example

```
ovs-vsctl add-br ovsbr0
ovs-vsctl add-port ovsbr0 vnet0
ovs-vsctl add-br ovsbr1
ovs-vsctl add-port ovsbr1 vnet1
ovs-vsctl add-port ovsbr1 vnet2
ovs-vsctl add-port ovsbr1 vnet3
ovs-vsctl add-port ovsbr1 vnet4
ovs-vsctl add-br ovsbr2
```

- The following command displays the interfaces and bridges associated with them:

```
ovs-vsctl show
fd04df5b-cea8-48f2-b074-642eaa1baa8b
    Bridge "ovsbr0"
        Port "ovsbr0"
            Interface "ovsbr0"
                type: internal
        Port "vnet0"
            Interface "vnet0"
        Port "vnet1"
            Interface "vnet1"
        Port "em1"
            Interface "em1"
    Bridge "ovsbr1"
        Port "vnet3"
            Interface "vnet3"
        Port "vnet2"
            Interface "vnet2"
        Port "vnet4"
            Interface "vnet4"
        Port "ovsbr1"
            Interface "ovsbr1"
                type: internal
    ovs_version: "2.8.1"
```

Configuring OVS-br1 for port mirroring

Following is the OVS rule to mirror east-west traffic and forward the traffic to the vTAP Rx port:

```
ovs-ofctl dump-flows ovs-br1

ovs-ofctl add-flow ovs-br1 in_port=11,action=output:18

ovs-ofctl add-flow ovs-br1 in_port=12,action=output:18
```

NOTE

- `output:18` is the Rx port of vnet8 for vTAP.
- `in_port=11` is vnet1 in VM App1.
- `in_port=12` is vnet3 in VM App2.