

Disable Promiscuous mode and Forget Transmits at Security Policy Attributes

Ericsson Service-Aware Policy Controller

Operating Instructions

Copyright

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document [Trademark Information](#).



Contents

| | | |
|----------|---|----------|
| 1 | Disable Promiscuous Mode and Forget Transmits Introduction | 1 |
| 1.1 | Prerequisites | 1 |
| 2 | Disable Promiscuous Mode and Forget Transmits Procedure | 2 |
| 2.1 | General Procedure | 2 |
| 2.1.1 | Perform a System Backup | 2 |
| 2.1.2 | Configure eVIP for the Use of IPVLAN | 2 |
| 2.1.3 | Check Promiscuous Mode and Forget Transmits on the VMware vCenter | 2 |
| 2.1.4 | SAPC Reboot | 3 |
| 2.1.5 | Disable Promiscuous Mode and Forget Transmits on the VMware vCenter | 3 |
| 2.1.6 | Final Checks | 3 |
| 2.1.7 | Perform a System Backup | 3 |





1 Disable Promiscuous Mode and Forget Transmits Introduction

This instruction is applicable to a VMware environment with an already deployed SAPC.

The upgrade to the eVIP 3.5 included in SAPC 1.1.1 allows the operator to disable "Promiscuous Mode" and "Forget Transmits" security policy attributes on the Virtual Interfaces where it was mandatorily enabled on previous versions.

1.1 Prerequisites

This section provides the prerequisites, which must be addressed before using the procedure.

Conditions

The following conditions must apply:

- The operator must be familiar with VMware virtualization and cloud environments.
- The SAPC accessible. The OAM virtual IP address (VIP_OAM) to access the SAPC and the password for **sapcadmin** and **root** users are known.
- A [Health Check](#) procedure has been executed and shows no errors.



2 Disable Promiscuous Mode and Forget Transmits Procedure

2.1 General Procedure

To disable these attributes, follow these steps.

2.1.1 Perform a System Backup

Follow [Create Backup Operational Instruction](#) and perform a System Backup.

2.1.2 Configure eVIP for the Use of IPVLAN

The new settings for these security policy attributes are only compatible with eVIP working mode named IPVLAN; therefore, this mode must be activated. The eVIP working mode can be checked with the following command:

```
SC-<X>:~ > lsmod | grep vlan
```

To change from MACVLAN to IPVLAN, proceed as follows:

Steps

1. Log on to the system:

```
External Machine> ssh root@<OAM VIP>
```

2. SC-<X>:~ # **mkdir -p /home/evip**

3. SC-<X>:~ # **echo "export EVIP_LAN=ipvlan" > /home/evip/evip.source**

2.1.3 Check Promiscuous Mode and Forget Transmits on the VMware vCenter

Verify the current security policy attributes of all Port Groups associated to the SAPC, refer to [Define the SAPC Port Groups](#) section of [SAPC VNF Deployment Instruction for VMware](#)



Attention!

To avoid communication disturbances, the actual change of attributes from previous value `Accept` to new value `Reject` **must** be performed immediately after the disconnection of the SAPC as a consequence of the reboot ordered in next section.

2.1.4 SAPC Reboot

Order a reboot of the whole cluster as shown in chapter "SAPC Reboot" on document [SAPC Troubleshooting Guide](#).

2.1.5 Disable Promiscuous Mode and Forget Transmits on the VMware vCenter

Right after the "Connection closed" message received from SAPC, change the values from `Accept` to `Reject`.

2.1.6 Final Checks

Wait a few minutes before executing these steps.

Steps

1. Log on to the SAPC:
`External Machine> ssh sapcadmin@<OAM VIP>`
2. Confirm the use of IPVLAN mode: `SC-<X>:~ > lsmod | grep vlan`
3. Run Health Check:
`SC-<X>:~ > sudo sapcHealthCheck`
4. Check that there are not errors. If errors are found, run `sudo sapcHealthCheck` command after suitable time. If error condition persists, contact your next support level.

2.1.7 Perform a System Backup

Follow [Create Backup Operational Instruction](#) and perform a System Backup.