

Add Flow Policy

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017. 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	Description	1
2	Procedure	1
2.1	Add Flow Policy	1



Add Flow Policy



1 Description

This instruction describes how to add a flow policy to an Abstract Load Balancer (ALB).

Flow policies are configured filters, which can segregate the incoming traffic into different flows. The flows can then be directed to different types of internal functions, which are associated with different application services.

The following two types of internal system mechanisms are used to abstract distributed internal functions associated with the application services:

- Target pools
- Socket groups

The target pools and socket groups are mutually exclusive attribute choices configured in a flow policy. A target pool or a socket group is a destination target for the segregated packet flows. For example, for an ALB with two VIP addresses and with two configured flow policies, traffic can be separated based on destination VIP addresses and directed to two different target pools.

For application services that are to be reached by TCP or UDP traffic, the attribute target pool is the relevant configuration choice, whereas socket groups are primarily used for SCTP traffic.

2 Procedure

2.1 Add Flow Policy

Prerequisites

- No documents are required.
- No tools are required.
- The following conditions must apply:
 - The ALB is known.
 - Either the target pool or the socket group to be used is known.
 - The criteria upon which the flow policy is to separate traffic is known.



- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



Attention!

Risk of data loss or data corruption.

Misconfiguration of flow policies can lead to black-holing of traffic and can cause a complete disruption of service.

Steps

1. Navigate to the `EvipFlowPolicies` Managed Object (MO), for example:

```
>dn ManagedElement=NODE06ST,Transport=1,Evip=1,EvipAlbs=1,EvipAlb=NetworkPartnerVPN_01,EvipFlowPolicies=1
```

2. Enter Config mode:

```
(EvipFlowPolicies=1)>configure
```

3. Create a `EvipFlowPolicy` MO, for example:

```
(config-EvipFlowPolicies=1)>EvipFlowPolicy=1
```

4. Set the mandatory attributes, for example:

```
(config-EvipFlowPolicy=1)>dest="10.1.1.4"
```

```
(config-EvipFlowPolicy=1)>protocol="tcp"
```

5. Set the appropriate optional attributes, for example:

```
(config-EvipFlowPolicy=1)>addressFamily="ipv4"
```

```
(config-EvipFlowPolicy=1)>targetPool="SIPTrafficPool"
```

```
(config-EvipFlowPolicy=1)>destport="5060"
```

The other optional attributes for the `EvipFlowPolicy` MO are `soGrp`, `src`, and `srcPort`.

6. Commit the settings:

```
(config-EvipFlowPolicy=1)>commit
```

7. Navigate to the `EvipFlowPolicies` MO:



```
(EvipVip=EvipFlowPolicy=1)>up
```

8. Verify the settings:

```
(EvipFlowPolicies=1)>show -r
```

The following is an example output:

```
EvipFlowPolicies=1
  EvipFlowPolicy=1
    addressFamily="ipv4"
    dest="10.1.1.4"
    destport="5060"
    evipFlowPolicyId="1"
    protocol="tcp"
    targetPool="SIPTrafficPool"
```

This example flow policy is called 1. It takes incoming IPv4 traffic with VIP address 10.1.1.4 to a target pool that is associated with the service called SIPTrafficPool, which listens to TCP port number 5060.