

eVIP, IPSEC Tunnel Fault

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2015. 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	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
2.1	Analyzing Alarm	3
2.2	Actions for Clearing Alarm	3





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is raised when an IP Security (IPsec) tunnel goes down ungracefully between an Evolved Virtual IP (eVIP)-enabled cluster and a peer.

The possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Faulty peer	The peer is faulty	Faulty peer	Peer	The peer cannot communicate with the IKE daemon on the eVIP side. IPsec key negotiation fails.
Faulty connection between the peer and the eVIP cluster	The connection between the peer and the eVIP cluster is faulty	Faulty connection between the peer and the eVIP cluster	Connection between the peer and the eVIP cluster	There is a networking issue between the eVIP cluster and the peer. IPsec key negotiation fails.
Faulty configuration	The configuration is faulty	Faulty configuration	Faulty configuration in the Managed Element	The IPsec tunnel goes down

Note: The alarm can appear after a cluster or a node restart.

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2129526787



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Source	ipsecPolicyId=<policy_name>, Evip_IpsecipsecTunnelId=<ikev2_tunnel_name>, Evip_HosthostId=eVIP_ALB_<alb_name> or Evip_Ipsec_Ikev1phase2PolicyId=<policy_name>, Evip_IpsecipsecTunnelId=<ikev1_tunnel_name>, Evip_HosthostId=eVIP_ALB_<alb_name>
Specific Problem	eVIP, IPSEC Tunnel Fault
Event Type	communicationsAlarm (2)
Probable Cause	x736UnspecifiedReason (418)
Additional Text	Problem with IPSEC Tunnel
Perceived Severity	major (4)

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

This instruction references the following document:

- *Data Collection Guideline*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- An eVIP, IPSEC Tunnel Fault alarm is raised.
- The user has knowledge in basic UNIX® commands.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



2 Procedure

This section describes the procedure to follow when this alarm is received.

2.1 Analyzing Alarm

To clear the alarm, the possible error causes must be investigated. The causes can be the following:

- Faulty configuration
- Network connectivity issue

Configuration mismatch can be a primary suspect if the IPsec tunnel configuration has been added or changed on the local side or the remote side, or both.

Note: On a system with properly configured tunnels, the alarm is cleared automatically when the nodes are successfully restarted.

2.2 Actions for Clearing Alarm

Validate Configuration

Do the following:

1. Identify the tunnel instance, shown in alarm attribute `source`, for example, `ipsecPolicyId=1,Evip_IpsecipsecTunnelId=1min,Evip_HosthostId=eVIP_ALB_alb_1`.
2. View the configuration parameters for the *IPsecTunnel* Managed Object (MO), for example:

```
>show -r ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,IpsecTunnel=1min
```

The following is an example output:



```
IpsecTunnel=1min
  localAddressStr="10.0.20.101"
  remoteAddressStr="10.128.171.101"
  Ikev2Session=1
    ikev2PolicyProfile="ManagedElement=1,Transport=1,⇒
Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min"
  IpsecPolicy=1
    ipsecProposalProfile="ManagedElement=1,Transport=1,⇒
Host=eVIP_ALB_alb_1,IpsecProposalProfile=1min"
    localTrafficSelector
      addressRange="10.0.20.1/32"
    remoteTrafficSelector
      addressRange="10.128.171.1/32"
```

3. View the referenced profiles, for example:

- a. **>show -r ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min**

The following is an example output:

```
Ikev2PolicyProfile=1min
[...]
  ikev2Proposal
    diffieHellmanGroup
      MODP_2048_GROUP_14
    encryptionAlgorithm
      ENCR_AES_CBC_128
    integrityAlgorithm
      AUTH_HMAC_SHA1_96
[...]
```

- b. **>show -r ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,IpsecProposalProfile=1min**

The following is an example output:

```
IpsecProposalProfile=1min
  childSaLifetime
    timeLimit=200
  ipsecProposal
    diffieHellmanGroup
      MODP_2048_GROUP_14
    encryptionAlgorithm
      ENCR_AES_CBC_256
    integrityAlgorithm
      AUTH_HMAC_SHA1_96
```

4. Is there any mismatch between the configurations shown in Step 2 and Step 3, and the configuration on the peer?



Yes: Determine if the configuration has been changed compared to previously known working configuration. Further actions are outside the scope of this document. Proceed with Step 14.

Note: If there is a mismatch that can cause IKE negotiation to fail, the configuration parameters must be changed.

No: Continue with the next step.

5. Check that the IKE authentication information is also correct:

- For Preshared Keys (PSKs):

Check that the same PSKs are installed on both gateways (it is not possible to list/reveal the previously installed PSK), for example:

```
>ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,IpsecTunnel=1min,Ikev2Session=1,installPreSharedKey mySecr3t123XC
```

- For certificates:

Check the certificate references, for example:

```
>show ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min,credential
```

```
>show ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min,trustCategory
```



Check Network Connectivity

Note: In most configurations, the security gateways can ping each other (the addresses used as security gateways).

The security gateway addresses cannot be pinged, for example, if the traffic selectors also cover these addresses or some discard policies are added on either side.

The security gateway addresses can be listed using the ECLI, for example:

- `>show ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,IpsecTunnel=1min,localAddressStr="10.0.20.101"`
- `>show ManagedElement=NODE06ST,Transport=1,Host=eVIP_ALB_alb_1,IpsecTunnel=1min,remoteAddressStr="10.128.171.101"`

To ping the address configured in `remoteAddressStr` from eVIP, one must find a node that is part of that specific Abstract Load Balancer (ALB).

6. Identify the ALB, for example.

```
>show ManagedElement=NODE06ST,Transport=1,Host=eVIP_
ALB_alb_1,l3Ref
```

The following is an example output:

```
l3Ref="ManagedElement=NODE06ST,Transport=1,Evip=1,EvipAlbs=1,EvipAlb=alb_1"
```

7. View the target pools in the ALB, for example:

```
>show -r ManagedElement=NODE06ST,Transport=1,Evip=1,Evi
pAlbs=1,EvipAlb=alb_1,EvipTargetPools=1
```

The following is an example output:

```
EvipTargetPools=1
  EvipTargetPool=6PLs_lc
    distributionMethod="least_connection"
    stickyGroup="no"
    udpStateless="no"
    EvipPayload=3
    EvipPayload=4
[...]
```

8. Select an `EvipPayload` from a target pool that is referenced by a flow policy having the IP address that is set as `localAddressStr` and log on to the corresponding node in the cluster, for example:



```
>ssh -l <user> PL-3
```

9. Use the information from Step 2 to test connectivity between the gateway addresses, for example:

```
PL-2-3:~ #ping -I 10.0.20.101 10.128.171.101
```

The following is an example output:

```
PING 10.128.171.101 (10.128.171.101) from 10.0.20.101 : 56(84) bytes =>
of data.
64 bytes from 10.128.171.101: icmp_seq=1 ttl=60 time=0.610 ms
64 bytes from 10.128.171.101: icmp_seq=2 ttl=60 time=0.446 ms
[...]
```

10. Is there connectivity between the gateway addresses?

Yes: Continue with the next step.

No: If the remote gateway cannot be reached (and there are no policies blocking this traffic), the two IKE daemons cannot communicate. Ensure that there are no connectivity issues. Proceed with Step 12.

11. Is the alarm cleared?

Yes: Proceed with Step 14.

No: Continue with the next step.

12. Perform data collection, refer to *Data Collection Guideline*.

13. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.

14. Job is completed.