

# eVIP, IKE Distribution Not Possible

Evolved Virtual IP

OPERATING INSTRUCTIONS

**Copyright**

© Ericsson AB 2015, 2016. 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
<b>2</b>	<b>Alarm Description</b>	<b>3</b>
2.1	Alarm Attributes	3
<b>3</b>	<b>Procedure</b>	<b>5</b>
3.1	Action Overview	5
3.2	Check Target Pool Configuration	5
3.3	Actions for Faulty Configuration	6



eVIP, IKE Distribution Not Possible



# 1 Introduction

This document describes the **eVIP, IKE Distribution Is Not Possible** and the alarm handling procedure to follow.

## 1.1 Prerequisites

This section describes the possible documents, tools, and conditions needed before performing the steps described in Section 3 on page 5.

### 1.1.1 Documents

Before starting this procedure, ensure that the following document have been read:

- eVIP Management Guide

Before starting this procedure, ensure that you have access to:

- Managed Object Model evip\_cm

### 1.1.2 Tools

Before starting this procedure, ensure that the COM CLI is installed and accessible on the system.



eVIP, IKE Distribution Not Possible



## 2 Alarm Description

The alarm is issued when the distribution of Internet Key Exchange (IKE) processes cannot be resolved, there are no available blades for every IKE instance.

IKE process is used to process the key exchange in case of IPsec communication.

If IKE is enabled in the eVIP configuration, the IKE processes are started to fulfill the following requirements:

- An IKE process is started on already available/online/running payload node/blade.
- A given number of IKE processes are started according to the eVIP configuration; Exactly one IKE process instance is started in each ALB.
- An IKE process can be started only on the given nodes according to the eVIP configuration; These nodes are defined under `Evip=1, EvipAlbs=1, EvipAlb=x, EvipTargetPools=1, Target Pool=y` in `EvipPayload` objects. For ALB, x collect every value of y and the corresponding nodes.
- At most one IKE process can be started on a payload node/blade.

The possible alarm causes are as follows:

- Faulty initial configuration.
- Faulty node in the cluster.

In case of faulty eVIP configuration, it is not possible to start the IKE processes with the current eVIP configuration to fulfill the requirements.

In case of faulty nodes in the cluster, it is possible that there are not enough available/running nodes to start IKE processes to fulfill the requirements.

**Note:** The alarm can appear as a result of an installation.

### 2.1 Alarm Attributes

This alarm is compliant with the Ericsson SNMP Fault Management MIB, which conforms to the X.733 alarm reporting function. However, the following X.733 parameters are not supported: Correlated Notifications, Additional Info, Monitored Attributes, Proposed Repair Action, Trend Indication, Threshold Information, Backed Up Object, and State Change Definition.

The most essential statical attributes of this alarm and their values are listed in Table 1:



Table 1 Alarm Attributes

Attribute Name	Attribute Value
MajorType	193
MinorType	2129526786
Managed Object Class	EvipAlb
Managed Object Instance	ManagedElement=<node_name>,Transport=1,Evip=1,EvipAlbs=1,EvipAlb=<alb_name>
Specific Problem	eVIP, IKE Distribution Is Not Possible
Event Type	communicationsAlarm (2)
Additional Text	Fault in IKE distribution
Perceived Severity	major (4)

The Alarm Type of the alarm is identified by the two integers: `majorType` and `minorType`. The Alarm Type is unique within the system type and maps to the X.733 Managed Object Instance. The `eventType`, `probableCause`, and `specificProblem` are always the same for a given Alarm Type.





## 3 Procedure

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

### 3.1 Action Overview

To start the troubleshooting:

1. Identify the cause of the alarm.
  - Check if COM SA, CLM Cluster Node Unavailable has also raised. If yes, the cause of the alarm can be a faulty node in the cluster.
  - Investigate the last configuration changes. The likely cause is that a reconfiguration event violated the listed rules of IKE distribution. The cause is faulty configuration.
  - Investigate the target pool configuration. See Section 3.2 Check Target Pool Configuration on page 5. Target pools limited to a few payload blades, blade processors, or targets in an ALB can violate listed rules.
2. When the cause has been identified, take relevant corrective measures.
  - Follow the instructions on the OPI COM SA, CLM Cluster Node Unavailable if there is a faulty node in the cluster.
  - If there is a configuration fault, follow the actions in Section 3.3 Actions for Faulty Configuration on page 6.

3. Confirm that the alarm does not reappear.

If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

### 3.2 Check Target Pool Configuration

To investigate the target pool configuration, do the following:

1. Check the number of ALBs to determine the number of IKE processes.

An ALB list is shown in the following example. The example output shows that 2 ALBs are configured, it means that two IKE processes must be started.

```
>show ManagedElement=NODE06ST,Transport=1,Evip=1,EvipAlbs=1
EvipAlbs=1
    EvipAlb=alb_0
    EvipAlb=alb_1
```



2. Check the ALB configuration one by one to determine where the IKE process can be started within an ALB.

The output in the following example shows that only node 6 is available for two ALBs: alb\_0 and alb\_1.

The IKE distribution is not possible with the configuration in this example.

```
>show all ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_0,EvipTargetPools=1
EvipTargetPools=1
  EvipTargetPool=SCs_rr
    distributionMethod="round_robin"
    stickyGroup="no"
    udpStateless="no"
    EvipPayload=6
  EvipTargetPool=sticky-SCs_rr
    distributionMethod="round_robin"
    stickinessTimeout="300"
    stickyGroup="yes"
    udpStateless="no"
    EvipPayload=6
>show all ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_1,EvipTargetPools=1
EvipTargetPools=1
  EvipTargetPool=SCs_rr
    distributionMethod="round_robin"
    stickyGroup="no"
    udpStateless="no"
    EvipPayload=6
  EvipTargetPool=sticky-SCs_rr
    distributionMethod="round_robin"
    stickinessTimeout="300"
    stickyGroup="yes"
    udpStateless="no"
    EvipPayload=6
```

### 3.3 Actions for Faulty Configuration

---

---

#### Warning!

The Target Pool plays a central role on traffic handling. If you are not familiar with eVIP configuration, consult with next level of maintenance support.

---

---

To clear the faulty configuration:



1. Configure new target pools or add one or more nodes to the existing target pools.

Addition of payloads 1.5 to target pools in alb\_0 and payload 4 to alb\_1 is shown in the following example.

```
(config)>ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_0,EvipTargetPools=1,
EvipTargetPool=SCs_rr
(config-EvipTargetPool=SCs_rr)>EvipPayload=1
(config-EvipTargetPool=SCs_rr)>commit
(config-EvipTargetPool=SCs_rr)>up
(config-EvipTargetPools=1)>EvipTargetPool=sticky-SCs_rr
(config-EvipTargetPool=sticky-SCs_rr)>EvipPayload=5
(config-EvipTargetPool=sticky-SCs_rr)>commit
(config-EvipTargetPool=sticky-SCs_rr)>top
(config)>ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_1,EvipTargetPools=1,
EvipTargetPool=SCs_rr
(config-EvipTargetPool=SCs_rr)>EvipPayload=4
(config-EvipTargetPool=SCs_rr)>commit
(config-EvipTargetPool=SCs_rr)>up
(config-EvipTargetPools=1)>EvipTargetPool=sticky-SCs_rr
(config-EvipTargetPool=sticky-SCs_rr)>EvipPayload=4
(config-EvipTargetPool=sticky-SCs_rr)>commit
```

2. Check the ALB configuration one by one to determine where the IKE process can be started.

The output in the following example shows that eVIP can start the IKE process on the following payload nodes 1, 5, 6 in ALB alb\_0:

```
>show all ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_0,EvipTargetPools=1
EvipTargetPools=1
  EvipTargetPool=SCs_rr
    distributionMethod="round_robin"
    stickyGroup="no"
    udpStateless="no"
    EvipPayload=1
    EvipPayload=6
  EvipTargetPool=sticky-SCs_rr
    distributionMethod="round_robin"
    stickinessTimeout="300"
    stickyGroup="yes"
    udpStateless="no"
    EvipPayload=5
    EvipPayload=6
```



The output in the following example shows that eVIP can start the IKE process on the following payload nodes 4 and 6 in ALB alb\_1:

```
>show all ManagedElement=NODE06ST,Transport=1,Evip=1,
EvipAlbs=1,EvipAlb=alb_1,EvipTargetPools=1
EvipTargetPools=1
  EvipTargetPool=SCs_rr
    distributionMethod="round_robin"
    stickyGroup="no"
    udpStateless="no"
    EvipPayload=4
    EvipPayload=6
  EvipTargetPool=sticky-SCs_rr
    distributionMethod="round_robin"
    stickinessTimeout="300"
    stickyGroup="yes"
    udpStateless="no"
    EvipPayload=4
    EvipPayload=6
```

If payload node 1, 4, 5, 6 all are running/available a possible IKE distribution is that two IKE processes are started on payload node 1 and 4.

3. Check the available payload nodes to determine where the IKE process can be started.

If you can log on to the nodes in question, the node is running and the IKE distribution can be done. See the following example:

```
ssh -l <user> SC-1
ssh -l <user> PL-4
ssh -l <user> PL-5
ssh -l <user> PL-6
```