Troubleshoot Failure to Join SEG to Cluster Due Matching Key Error

Contents

Introduction

This document describes how to troubleshoot a Secure Email Gateway (SEG) is not able to join an existing cluster.

Prerequisited

Cisco recommends that you have knowledge of these topics:

- How to join appliances into a Cluster (Centralized Management).
- All ESAs must have the same AsyncOS versions (down to the revision).

Requirements

The information in this document was created from the devices in a specific lab enviroment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential of any command

Problem

The issue exists when joinging a Secure Email Gateway (SEG) to an existing cluster. The issue promt an error on connection, this is due to the ESA missing some of the kex algorithms/cipher algorithms.

Failed to join the cluster.
Error was: "(3, 'Could not find matching key exchange algorithm.')"
Enter the IP address of a machine in the cluster.

Solution

It is required to use the default values for **sshconfig**

<#root>

```
esa> sshconfig


Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> sshd
```

```
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
```

To apply the default values you can run the command from the **CLI > sshconfig > sshd** on the step-by-step setup:

<#root>

```
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>

rsa1,ssh-dss,ssh-rsa



Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc]>

aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijn



aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijn



Enter the MAC Methods do you want to use
```

```
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160]>
```

hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-9

```
Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1]>
```

diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1

,

diffie-hellman-group14-sha1

,

iffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

Commit the changes

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

After the change, the appliance joins the cluster successfully

Related Information

Configure an Email Security Appliance (ESA) Cluster

ESA FAQ: What are the requirements for setting up a cluster?