Risoluzione dei problemi di aggiunta di SEG al cluster a causa di un errore di corrispondenza della chiave

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'impossibilità di aggiungere un gateway di posta elettronica protetto (SEG) a un cluster esistente.

Prerequisito

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come unire gli accessori in un cluster (gestione centralizzata).
- Tutte le ESA devono avere le stesse versioni AsyncOS (fino alla revisione).

Requisiti

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente le potenzialità di qualsiasi comando

Problema

Il problema si verifica quando si aggiunge un gateway di posta elettronica protetto (SEG, Secure Email Gateway) a un cluster esistente. La questione promette un errore di connessione, questo è dovuto alla ESA che manca alcuni algoritmi di cifratura/algoritmi di kex.

Impossibile aggiungere il computer al cluster.
Errore: "(3, 'Impossibile trovare l'algoritmo di scambio chiave corrispondente.')"
Immettere l'indirizzo IP di un computer nel cluster.

Soluzione

È necessario utilizzare i valori predefiniti per 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
```

Per applicare i valori predefiniti, è possibile eseguire il comando da CLI > sshconfig > sshd durante l'installazione dettagliata:

<#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

Conferma le modifiche

```
esa> commit

Please enter some comments describing your changes:

[]> Edit the SSHD values
```

Dopo la modifica, l'accessorio verrà aggiunto al cluster

Informazioni correlate

[Configurazione di un cluster ESA (Email Security Appliance)]

[Domande frequenti ESA: quali sono i requisiti per la configurazione di un cluster?]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).