由於十六進位制字首處理，在ISE 3.4上配置NTP身份驗證失敗

目錄

問題

當使用經過身份驗證的NTP和長度為40個字元的SHA1金鑰時，思科身份服務引擎(ISE)3.4.0.608 Patch 1無法與NTP伺服器同步。在CLI上接受了NTP authentication key命令，沒有錯誤，但是啟用身份驗證時不會發生NTP同步。如果沒有身份驗證，NTP同步將正常工作。其他網路裝置（包括Cisco交換機）使用相同的金鑰ID和金鑰值成功通過同一NTP伺服器進行身份驗證。

在故障排除期間，資料包捕獲分析顯示ISE傳送帶有正確金鑰ID和MAC/身份驗證器欄位的已驗證NTP請求，但是，伺服器回覆包含全部為零的金鑰ID且沒有MAC/身份驗證器，從而導致ISE拒絕身份驗證。充當NTP伺服器的Cisco交換機的調試輸出顯示「SHA1-Match:0」表示身份驗證失敗。

環境

- 思科身份服務引擎(ISE)版本3.4.0.608，帶補丁1
- 使用SHA1演演算法的NTP驗證
- 長度為40個字元的NTP身份驗證金鑰
- 執行17.12.04版的Cisco Catalyst 9500交換器(C9500-24Y4C)
- 具有經過身份驗證的NTP配置的NTP伺服器裝置

解析

此問題是由思科錯誤ID導致的：CSCwq79772，影響ISE在需要HEX字首時處理長NTP身份驗證金鑰的方式。此錯誤已在ISE 3.4補丁8和ISE 3.5補丁3中修正。

瞭解根本原因

在Cisco裝置上配置NTP身份驗證金鑰時，20個字元或更長的金鑰將自動視為十六進位制字串而不是純文字檔案。這要求ISE在配置金鑰時使用「HEX：」字首。但是，由於該錯誤，ISE僅接受36個字元的40字元金鑰，因為額外的「HEX：」字首處理，導致身份驗證失敗。

即時解決方法選項

在可以將ISE軟體升級到包含修復程式的版本之前，請使用以下替代方法之一：

選項 1:使用36位元的SHA1金鑰

使用36個字元的SHA1金鑰而不是40個字元的金鑰配置NTP伺服器和ISE。

在ISE上：

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

在NTP伺服器上（Cisco交換機示例）：

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
ntp trusted-key 1
```

選項 2:使用MD5身份驗證

從SHA1切換到MD5身份驗證，此身份驗證未表現出相同的長度限制。

在ISE上：

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

在NTP伺服器上：

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

驗證步驟

實施任一解決方法後，驗證NTP同步：

在ISE上：

```
show ntp
show clock
```

在交換機上（如果使用交換機作為NTP伺服器）：

```
show ntp associations
show ntp status
```

當一側禁用了身份驗證而在另一側啟用身份驗證時，通過確認NTP同步失敗來查詢成功的同步指示符，並驗證身份驗證是否正常工作。

永久決議

將ISE升級為包含思科錯誤ID修復程式的以下版本之一：CSCwq79772:

- ISE 3.4補丁8（如果可用）
- ISE 3.5補丁3或更高版本

升級後，原始40個字元的SHA1金鑰組態會使用HEX首碼正常運作。

原因

此問題是由思科錯誤ID導致的：CSCwq79772，在ISE版本3.4 Patch 8和3.5 Patch 3之前。當NTP身份驗證金鑰為20個字元或更長時，思科裝置將這些金鑰視為十六進位制字串，在配置中需要「HEX：」字首。由於此錯誤，ISE在使用HEX字首時錯誤地處理金鑰長度計算，僅接受40字元金鑰的36個字元。這會導致ISE和NTP伺服器之間的金鑰不匹配，從而導致NTP同步嘗試期間的身份驗證失敗。

相關內容

- Cisco錯誤CSCwq79772
- 思科無線控制器命令參考 — NTP身份驗證
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。