VCS Web介面上的TLS握手失敗

目錄

<u>簡介</u> <u>問題</u> <u>解決方案</u>

簡介

思科視訊通訊伺服器(VCS)使用使用者端憑證進行驗證和授權程式。此功能在某些環境中非常有用 ,因為它允許增加一層安全性,並且可用於單點登入目的。但是,如果配置不正確,管理員可能會 被鎖定在VCS Web介面之外。

本文中的步驟用於在Cisco VCS上禁用基於客戶端證書的安全性。

問題

如果在VCS上啟用了基於客戶端證書的安全功能,並且配置不正確,則使用者可能無法訪問VCS Web介面。嘗試訪問Web介面時遇到了傳輸層安全(TLS)握手失敗。

以下是觸發此問題的配置更改:

Administration access	
Session time out (minutes)	* 30
Per-account session limit	<u>+</u> 0
System session limit	• 0 (i)
Serial port / console	On - (1)
Telnet service	Off - 🕧
SSH service	On - (1)
Web interface (over HTTPS)	On - (j)
Client certificate-based security	Not required
WARNING	Not required Certificate validation Certificate-based authentication

解決方案

完成以下步驟,以停用使用者端憑證型安全性,並將系統回復到管理員可以存取VCS的Web介面的 狀態:

- 1. 通過安全殼層(SSH)以根身份連線到VCS。
- 以root使用者身份輸入此命令,以便對Apache進行硬編碼,使其永遠不會使用基於客戶端證書 的安全性:

echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf

附註:輸入此命令後,在刪除**removecba.conf**檔案並重新啟動VCS之前,無法將VCS重新配置 為基於客戶端證書的安全性。

3. 您必須重新啟動VCS才能使此配置更改生效。當您準備好重新啟動VCS時,請輸入以下命令: ^{tshell}

xcommand restart

附註:這將重新啟動VCS並丟棄所有呼叫/註冊。

4. VCS重新載入後,基於客戶端證書的安全功能將被禁用。但是,它不會以理想的方式禁用。使 用讀寫管理員帳戶登入到VCS。在VCS上導航到**System > System**頁面。

CISCO Cisco TelePresence Video (

Status	System	VCS configuration	Appli
Overvier	System		
Overvie	Ethernet		
System inf	IP		
System nar	Quality of	Service	
Up time	Quality of	Service	
Software ve	DNS		
IPv4 addres	Time		
<u>Options</u>	Login pag	je	
Resource (SNMP		
Non-travers: Ext	External n	nanager	
	TMS Prov	isioning Extension serv	vices
	Firewall ru	lles	P
	in presentation	sweisene einer einer einer einer einer	HERE/PHASENS

在VCS的系統管理頁面上,確保基於客戶端證書的安全設定為「不需要」:

Administration access	
Session time out (minutes)	* 30 i
Per-account session limit	★ 0
System session limit	• 0
Serial port / console	On - i
Telnet service	Off - (1)
SSH service	On - i
Web interface (over HTTPS)	On - i
Client certificate-based security	Certificate validation
Certificate revocation list (CRL) checking	Certificate validation Certificate-based authentication

進行此更改後,儲存更改。

5. 完成後,在SSH中輸入以下命令作為root,以便將Apache重置為正常狀態: rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf **警告:**如果跳過此步驟,則決不能重新啟用基於客戶端證書的安全性。
6. 再次重新啟動VCS以驗證過程是否有效。現在您已經具有Web訪問許可權,可以從

Maintenance > Restart下的Web介面重新啟動VCS。

祝賀你!現在,VCS在禁用基於客戶端證書的安全的情況下運行。