在獨立機架式伺服器上配置遠端金鑰管理

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>SED驅動器</u> <u>設定</u> <u>建立客戶端私鑰和客戶端證書</u> <u>在CIMC上配置KMIP伺服器</u> <u>驗證</u> <u>疑難排解</u> <u>相關資訊</u>

簡介

本檔案介紹在獨立機架式伺服器上設定金鑰管理互通性通訊協定(KMIP)。

必要條件

需求

思科建議您瞭解以下主題:

- 思科整合式管理控制器(CIMC)
- 自我加密驅動器(SED)
- KMIP

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- UCSC-C220-M4S, CIMC版本: 4.1(1h)
- SED驅動器
- 800GB企業效能SAS SED SSD(10 FWPD)- MTFDJAK800MBS
- •驅動器部件ID:UCS-SD800GBEK9
- 供應商:微米
- 型號: S650DC-800FIPS
- Vormetric作為第三方金鑰管理器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

KMIP是一種可擴展的通訊協定,它定義了用於在金鑰管理伺服器上處理金鑰的消息格式。這簡化了 加密金鑰管理,從而方便了資料加密。

SED驅動器

SED是硬碟驅動器(HDD)或固態驅動器(SSD),驅動器內建加密電路。它透明地加密寫入介質的所 有資料,並在解鎖後透明地解密從介質讀取的所有資料。

在SED中,加密金鑰本身永遠不會離開SED硬體的限制,因此可以安全抵禦作業系統級別的攻擊。

SED驅動器工作流:



1. SED驅動器流

使用**本地金鑰管理**配置(使用者負責記住金鑰資訊)可在本地獲取解鎖驅動器的密碼。它也可以通 過遠端金鑰管理獲取,其中安全金鑰是從KMIP伺服器建立和提取的,使用者負責在CIMC中配置 KMIP伺服器。

設定

建立客戶端私鑰和客戶端證書

這些命令將使用OpenSSL包在Linux機器上輸入,而不是在Cisco IMC中。確保根CA證書和客戶端 證書中的公用名相同。

附註:確保Cisco IMC時間設定為當前時間。

1.建立2048位RSA金鑰。

openssl genrsa -out client_private.pem 2048 2.使用已建立的金鑰建立自簽名證書。

openssl req -new -x509 -key client_private.pem -out client.pem -days 365 3.有關獲取根CA證書的詳細資訊,請參閱KMIP供應商文檔。

附註: Vormetric要求RootCa證書中的公用名稱與Vormetric主機的主機名匹配。

在CIMC上配置KMIP伺服器

1. 導航到Admin > Security Management > Secure Key Management。

清晰的配置顯示 Export/Delete buttons grayed out, only Download buttons are active.

Chassis •	Certificate Management Secure Key					
Compute	Download Root CA Certificate Export Root	CA Certificate Delete Root CA	Certificate Download Client Certificate Exp	ort Client Certificate		
Notworking	Delete Client Certificate Download Client Private Key Export Client Private Key Delete Client Private Key Delete KMIP Login					
Networking	Enable Secure Key Management:					
Storage +	KMIP Servers	KMIP Servers				
Admin •	Delete Test Connection					
User Management	ID IP Addres	s Port	Timeout			
Networking	0.1	5696	5			
Communication Services	2	5696	5			
Security Management						
Event Management	▼ KMIP Root CA Certificate		 KMIP Client Certifica 	ite		
Firmware Management	Server Root CA Certificate:	Not Available	Client Certificate:	Not Available		
Utilities	Download Status:	NONE	Download Status:	NONE		
Device Connector	Download Progress:	0	Download Progress:	0		
	Export Status:	NONE	Export Status:	NONE		
	Export Progress:	0	Export Progress:	0		
	 KMIP Login Details 		 KMIP Client Private 	Key		
	Use KMIP Login:	0	Client Private Key:	Not Available		
	Login name to KMIP Server:	Enter User Name	Download Status:	NONE		
	Password to KMIP Server:		Download Progress:	0		
	Change Password:	U	Export Status:	NONE		
			Export Progress:	0		

2.按一下IP地址並設定KMIP伺服器的IP,確保您能夠訪問它,並且在預設埠被使用時,無需更改任 何其他內容,然後儲存更改。

Enable Secure Key Management: 🗹

KMIP Servers

De	lete Test Connec	tion			
	ID	IP Address	Port	Timeout	
	1	10.104.253.26	5696	5	
	2	Save I Cance	el 596	5	

3.將證書和私鑰下載到伺服器。您可以下載 .pem file or just paste the content.

chaore becare ney	Management:			
MIP Servers				Download Root CA Certificate
ID	IP Address	Port	Timeout	O Download from remote location
0 1	10.104.253.26	5696	5	O Download through browser Client
2		5696	5	Paste Content
				Paste Root CA Certificate Content:
KMIP Root C	A Certificate			
Server	Root CA Certificate: Not Available			
	Download Status: NONE			
	Download Progress: 0			
	Export Status: NONE			Download Root CA Certificate Close

4.上傳證書時,您會看到證書顯示為Available,對於未上傳的缺失證書,您會看到Not Available。

僅當所有證書和私鑰都已成功下載到CIMC時,才能測試連線。

 KMIP Root CA Certificate 		 KMIP Client Certificate
Server Root CA Certificate:	Available	Client Certificate: Not Available
Download Status:	NONE	Download Status: NONE
Download Progress:	0	Download Progress: 0
Export Status:	COMPLETED	Export Status: COMPLETED
Export Progress:	100	Export Progress: 100
 KMIP Login Details 		✓ KMIP Client Private Key
 KMIP Login Details Use KMIP Login: 	0	KMIP Client Private Key Client Private Key: Not Available
 KMIP Login Details Use KMIP Login: Login name to KMIP Server: 	Enter User Name	KMIP Client Private Key Client Private Key: Not Available Download Status: NONE
 KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server: 	Enter User Name	KMIP Client Private Key Client Private Key: Not Available Download Status: NONE Download Progress: 0
 KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server: Change Password: 	Enter User Name	 KMIP Client Private Key Client Private Key: Not Available Download Status: NONE Download Progress: 0 Export Status: COMPLETED
 KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server: Change Password: 	Enter User Name	 KMIP Client Private Key Client Private Key: Not Available Download Status: NONE Download Progress: 0 Export Status: COMPLETED Export Progress: 100

5.(可選)一旦您擁有所有證書,則可以選擇新增KMIP伺服器的使用者和密碼,只有作為第三方 KMIP伺服器的SafeNet才支援此配置。

6.測試連線,如果證書正確,並且可以通過配置的埠訪問KMIP伺服器,則連線成功。

÷E	cisco Cisco Inte	grated Mar	nagement Co	ntroller			query on kmip-server run successfully!
۱/	/ Security Manag	ement / Se	ecure Key Ma	inagemer	nt 🚖		·
Certific	ate Management	Secure Key Ma	nagement Se	scurity Config	uration		OK
	te Client Certificate Dre	Export Root G	A Certificate Delet	e Root CA Cer	v Delete Client Private Key	Cate Expo	rt Cient Centricate
		_					
End	able Secure Key Manag	ement: 🗹					
KM	IP Servers						
	Delete Test Conne	ction					
	ID	IP Address		Port	Timeout		
	1	10.104.253.26	6	5696	5		
	2			5696	5		
	KMIP Root CA Carti	ficate			 KMIP Client 	Certificat	ta
	Server Root CA	Certificate: /	huninhla		Client	Certificate:	Ausiable
	Down	load Status: 1	NONE		Downlo	ad Status:	NONE
	Downloa	ad Progress: (0		Download	Progress:	0
	Ex	oport Status: (COMPLETED		Exp	ort Status:	COMPLETED
	Expo	ort Progress:	100		Export	Progress:	100
Ŧ	KMIP Login Details				 KMIP Client 	Private K	Cey
	Use I	KMIP Login:			Client Pr	ivate Key:	Available
	Login name to K	MIP Server:	Enter User Name		Downlo	ad Status:	NONE
	Password to K	MIP Server:	1		Download	Progress:	0
	Change	erassword:			Exp	ort Status:	COMPLETED
					Export	r Progress:	100

7.一旦我們與KMIP的連線成功,就可以啟用遠端金鑰管理。

導覽至Networking > Modular Raid Controller > Controller Info。

選擇Enable Drive Security,然後選擇Remote Key Management。

附註:如果以前啟用了Local Key Management,則會要求您輸入當前金鑰,以便進行遠端管 理

Controller Info	Physical Drive Info Vir	tual Drive Info	Battery Backup Unit	Storag	je Log			
Create Virtual Drive from Unused Physical Drives Create Virtual Drive from an Existing Virtual Drive Group Import Foreign Config Clear Foreign Config								
Clear Boot Drive Get Storage Firmware Log Enable Drive Security Disable Drive Security Clear Cache Clear all Configuration Set Factory Defaults								
Switch to Remote H	Switch to Remote Key Management Switch to Local Key Management							
	Enable Drive Security							
 Health/Sta 	Health/Status Controller Security: Disabled							
	Comp Key Mar	agement: 💿 i	Remote Key Management	0	Local Key Management	al:	300 sec	
	Cont				Save Cancel	te:	30 %	
	RAID Chip Temperature:	68			Patrol Read	Rate:	30 %	
	Storage Firmware Log Status:	Not Downloaded	1		Consistency Check	Rate:	30 %	
• Firmware	Versions				Reconstruction	Rate:	30 %	
- Timmare	**************************************				Cache Flush Inte	erval:	4 sec	
	Product Name:	Cisco 12G Modu	Jar Raid Controller with :)	May Daisson To Cain He At /			

驗證

使用本節內容,確認您的組態是否正常運作。

您可以在CLI中驗證設定。

1.驗證是否已啟用KMIP。

C-Series-12# scope kmip C-Series-12 /kmip # show detail Enabled: yes 2.檢驗IP地址、埠和超時。

C-Series-12 /kmip # show kmip-server Server number Server domain name or IP address Port Timeout

----- 1 10.104.253.26 5696 5 2 5696 5

3.驗證證書是否可用。

C-Series-12 /kmip # show kmip-client-certificate KMIP Client Certificate Available: 1 C-Series-12 /kmip # show kmip-client-private-key KMIP Client Private Key Available: 1 C-Series-12 /kmip # show kmip-root-ca-certificate KMIP Root CA Certificate Available: 1

4.驗證登入詳細資訊。

C-Series-12 /kmip # show kmip-login Use KMIP Login Login name to KMIP server Password to KMIP server ----- no ****** 5.測試連線。

C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server # test-connectivity Result of test-connectivity: query on kmip-server run successfully!

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

如果與KMIP伺服器的測試連線失敗,請確保可以ping通該伺服器。

cisco Cisco Integrated Management Controller			🐥 🗸 2	admin@10.82.171.164 - C-Series-12 2
/ Security Management / Secure Key Managemen	nt	Refresh Host Pr	ower Launch KVM Ping	CIMC Roboot Locator LED 🔞
rtificate Management Secure Key Management Security Conf	auration Ping Details	_	0 X	
Download Root CA Certificate Export Root CA Certificate Delete Root CA Ce Delete Client Certificate Download Client Private Key Export Client Private Ke	* Hostname/IP Address * Number of Retries	10.104.253.26 3		
Enable Secure Key Management: 🗹	* Timeout Ping Status	10 Success	Details	
KMIP Servers Delete Test Connection			Ping Cancel	

確保在CIMC和KMIP伺服器上開啟埠5696。您可以在我們的PC上安裝NMAP版本,因為此命令在 CIMC上不可用。

可以在本地電腦上安裝<u>NMAP</u>,以測試埠是否開啟;在安裝檔案的目錄下,使用以下命令:

nmap <ipAddress> -p <port>

輸出顯示KMIP服務的開放埠:



輸出顯示KMIP服務的關閉埠:



相關資訊

- C系列配置指南 自我加密驅動器
- C系列配置指南 金鑰管理互操作性協定
- 技術支援與文件 Cisco Systems

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)。