Remote Key Management auf eigenständigen Rack-Servern konfigurieren

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen SED-Laufwerke Konfigurieren Erstellen eines privaten Clientschlüssels und eines Clientzertifikats KMIP-Server auf dem CIMC konfigurieren Überprüfung Fehlerbehebung Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Konfiguration des Key Management Interoperability Protocol (KMIP) auf eigenständigen Rack-Servern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Integrated Management Controller (CIMC)
- Selbstverschlüsselndes Laufwerk (SED)
- KMIP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- UCSC-C220-M4S, CIMC-Version: 4,1 (1 Std.)
- SED-Laufwerke
- 800 GB Enterprise Performance SAS SED SSD (10 FWPD) MTFDJAK800MBS
- Laufwerkteil-ID: UCS-SD800GBEK9
- Anbieter: MIKRON
- Modell: S650DC-800FIPS

Vormetrisch als Drittanbieter-Schlüsselmanager

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

KMIP ist ein erweiterbares Kommunikationsprotokoll, das Nachrichtenformate für die Bearbeitung kryptografischer Schlüssel auf einem Schlüsselverwaltungsserver definiert. Dies erleichtert die Datenverschlüsselung, da die Verschlüsselungsschlüsselverwaltung vereinfacht wird.

SED-Laufwerke

Ein SED ist eine Festplatte (HDD) oder ein Solid-State-Laufwerk (SSD) mit integrierter Verschlüsselungsschaltung. Es verschlüsselt auf transparente Weise alle auf das Medium geschriebenen Daten und entschlüsselt, wenn es entsperrt wird, transparent alle vom Medium gelesenen Daten.

Bei einer SED verlassen die Verschlüsselungsschlüssel selbst nie die Grenzen der SED-Hardware und sind daher vor Angriffen auf Betriebssystemebene sicher.

SED-Laufwerke Workflow:



1. SED-Antriebsfluss

Das Kennwort zum Entsperren des Laufwerks kann lokal über die Konfiguration der **lokalen Schlüsselverwaltung** abgerufen werden, wobei der Benutzer dafür verantwortlich ist, sich die Schlüsselinformationen zu merken. Er kann auch über die Remote Key-Verwaltung abgerufen werden. Dabei wird der Sicherheitsschlüssel von einem KMIP-Server erstellt und abgerufen, und der Benutzer ist dafür verantwortlich, den KMIP-Server im CIMC zu konfigurieren.

Konfigurieren

Erstellen eines privaten Clientschlüssels und eines Clientzertifikats

Diese Befehle müssen auf einem Linux-System mit dem OpenSSL-Paket eingegeben werden, nicht im Cisco IMC. Stellen Sie sicher, dass der Common Name im Root-Zertifizierungsstellenzertifikat und im Clientzertifikat identisch ist.

Anmerkung: Stellen Sie sicher, dass die Cisco IMC-Zeit auf die aktuelle Zeit eingestellt ist.

1. Erstellen Sie einen 2048-Bit-RSA-Schlüssel.

openssl genrsa -out client_private.pem 2048

2. Erstellen Sie ein selbstsigniertes Zertifikat mit dem bereits erstellten Schlüssel.

openssl req -new -x509 -key client_private.pem -out client.pem -days 365

3. Weitere Informationen zum Erhalt des Zertifikats der Stammzertifizierungsstelle finden Sie in der Dokumentation des KMIP-Anbieters.

Anmerkung: Für Vormetric muss der allgemeine Name im RootCa-Zertifikat mit dem Hostnamen des Vormetric-Hosts übereinstimmen.

Anmerkung: Sie benötigen ein Konto, um auf die Konfigurationsanleitungen für die KMIP-Anbieter zugreifen zu können: <u>SafeNet</u> <u>Vormetrisch</u>

KMIP-Server auf dem CIMC konfigurieren

1. Navigieren Sie zu Admin > Security Management > Secure Key Management.

Eine übersichtliche Konfiguration zeigt Export/Delete buttons grayed out, only Download buttons are active.

* *	diate Cisco Int	tegrated Management C	ontroller Ianageme	ent ÷	_			
Chassis •	Certificate Management							
Compute	Download Root CA Certificat	te Export Root CA Certificate De Download Client Private Key Export	lete Root CA Ce Client Private K	ertificate Download Client Certificate Exp ev Delete Client Private Key Delete KMB	ort Client Certificate			
Networking +	Enable Secure Key Management:							
Storage +	KMIP Servers							
Admin 👻	Delete Test Con							
User Management	ID	IP Address	Port	Timeout				
Networking	0 1		5696	5				
Communication Services	2		5696	5				
Security Management								
Event Management	▼ KMIP Root CA Ce	rtificate		 KMIP Client Certifica 	ite			
Firmware Management	Server Root	CA Certificate: Not Available		Client Certificate:	Not Available			
Utilities	Dov	wnload Status: NONE		Download Status:	NONE			
Device Connector	Down	load Progress: 0		Download Progress:	0			
		Export Status: NONE		Export Status:	NONE			
	Б.	port Progress: 0		Export Progress:	0			
	 KMIP Login Detail 	ls		 KMIP Client Private Key 				
	Us	e KMIP Login:		Client Private Key:	Not Available			
	Login name to	KMIP Server: Enter User Name		Download Status:	NONE			
	Password to	KMIP Server:		Download Progress:	0			
	Char	nge Password:		Export Status:	NONE			
				Export Progress:	0			

2. Klicken Sie auf die IP-Adresse und legen Sie die IP für den KMIP-Server, stellen Sie sicher, dass Sie in der Lage sind, sie zu erreichen und wenn der Standard-Port verwendet wird nichts anderes geändert werden muss, dann speichern Sie die Änderungen.

Enable Secure Key Management: 🗹								
KMIP	Servers							
De	elete Test Connec	tion						
	ID	IP Address	Port	Timeout				
	1	10.104.253.26	5696	5				
	2	Save Cano	el 396	5				

3. Laden Sie die Zertifikate und den privaten Schlüssel auf den Server herunter. Sie können die **.pem** file or just paste the content.

inable Secure Ke	y Management: 🗌			
MIP Servers				Download Root CA Certificate
ID	IP Address	Port	Timeout	O Download from remote location
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
	Extent Department - 0			

4. Wenn Sie die Zertifikate hochladen, sehen Sie, dass die Zertifikate als **Verfügbar** angezeigt werden. Für die fehlenden Zertifikate, die nicht hochgeladen werden, sehen Sie **Nicht verfügbar**.

Sie können die Verbindung nur testen, wenn alle Zertifikate und privaten Schlüssel erfolgreich auf den CIMC heruntergeladen wurden.

v	KMIP Root CA Certificate		 KMIP Client Certifica 	te
	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
v	KMIP Login Details		 KMIP Client Private K 	(ey
¥	KMIP Login Details Use KMIP Login:	0	 KMIP Client Private K Client Private Key: 	Key Not Available
•	KMIP Login Details Use KMIP Login: Login name to KMIP Server:	Enter User Name	 KMIP Client Private K Client Private Key: Download Status: 	Not Available
*	KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server:	Enter User Name	 KMIP Client Private K Client Private Key: Download Status: Download Progress: 	Not Available NONE 0
•	KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server: Change Password:	Enter User Name	 KMIP Client Private K Client Private Key: Download Status: Download Progress: Export Status: 	Not Available NONE 0 COMPLETED
¥	KMIP Login Details Use KMIP Login: Login name to KMIP Server: Password to KMIP Server: Change Password:	Enter User Name	 KMIP Client Private K Client Private Key: Download Status: Download Progress: Export Status: Export Progress: 	Not Available NONE 0 COMPLETED 100

5. (optional) Sobald Sie über alle Zertifikate verfügen, können Sie optional den Benutzer und das Kennwort für den KMIP-Server hinzufügen. Diese Konfiguration wird nur für SafeNet als Drittanbieter-KMIP-Server unterstützt.

6. Testen Sie die Verbindung, und wenn die Zertifikate korrekt sind und Sie den KMIP-Server über den konfigurierten Port erreichen können, wird eine erfolgreiche Verbindung angezeigt.

😸 📲 diale Cisco Integrated Ma	anagement Co	query on kmip-server run successfully!		
/ / Security Management / S	Secure Key Ma			
Certificate Management Secure Key I	Management Se	scurity Con	fguration	
Download Root CA Certificate Export Root	CA Certificate Delet	e Root CA C	ertificate Download Client Certificate Expo	ort Client Certificate
Delete Client Certificate Download Client P	hivate Key Export Cl	ient Private I	Key Delete Client Private Key Delete KMIP	
Fnable Secure Key Management				
Chaste Secure way management:				
KMIP Servers				
Delete Test Connection				
ID IP Addres	5	Port	Timeout	
1 10.104.253	26	5696	5	
2		5696	6	
 KMIP Root CA Certificate 			 KMIP Client Certifica 	te
Server Root CA Certificate:	Available		Client Certificate:	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 F 	Key
Use KMIP Login:			Client Private Key:	Available
Login name to KMIP Server:	Enter User Name		Download Status:	NONE
Password to KMIP Server:			Download Progress:	0
Change Password:			Export Status:	COMPLETED
			Export Progress:	100

7. Sobald unsere Verbindung mit KMIP erfolgreich ist, können Sie die Remote-Schlüsselverwaltung aktivieren.

Navigieren Sie zu Networking > Modular Raid Controller > Controller Info.

Wählen Sie Laufwerksicherheit aktivieren und dann Remote Key Management aus.

Anmerkung: Wenn die **lokale Schlüsselverwaltung** zuvor aktiviert war, werden Sie aufgefordert, den aktuellen Schlüssel einzugeben, um ihn zur Remote-Verwaltung zu ändern.

Controller Info Physical Drive	Info Virtual	Drive Info	Battery Backup Uni	t Stora	ge Log		
Create Virtual Drive from Unused Phys	ical Drives Crea	te Virtual Drive f	rom an Existing Virtual C	Drive Group	Import Foreign Config Clear Foreign C	lonfig	
Clear Boot Drive Get Storage Firmw	are Log Enable I	Drive Security	Disable Drive Security	Clear Cach	e Clear all Configuration Set Factory	Defaul	ts (
Switch to Remote Key Management	Switch to Local Ke	y Management					
 Enable Drive Security 							300 sec
Cont					Save Cancel	te:	30 %
RAID Chip 1	emperature: 68	3			Patrol Read I	cate:	30 %
Storage Firmware	Log Status: N	ot Downloaded			Consistency Check I	Rate:	30 %
- Eirmuusra Varalana					Reconstruction F	tate:	30 %
Pittiware versions					Cache Flush Inte	rval:	4 sec
Pr	oduct Name: C	isco 12G Modula	ar Raid Controller with	0	Max Drives To Spin Up At C		

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Über die CLI können Sie die Konfiguration überprüfen.

1. Überprüfen Sie, ob KMIP aktiviert ist.

C-Series-12# scope kmip C-Series-12 /kmip # show detail Enabled: yes 2. Überprüfen Sie IP-Adresse, Port und Timeout.

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

3. Überprüfen Sie, ob die Zertifikate verfügbar sind.

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. Überprüfen der Anmeldedetails

C-Series-12 /kmip # show kmip-login Use KMIP Login Login name to KMIP server Password to KMIP server ----- no ******

5. Testen Sie die Verbindung.

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!

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Wenn die Testverbindung mit dem KMIP-Server nicht erfolgreich hergestellt werden kann, stellen Sie sicher, dass Sie den Server pingen können.

cisco Integrated Management Controller			🕂 🗸 2	admin@10.82.171.164 - C-Series-12	¢
/ Security Management / Secure Key Manageme	ent	Refresh Host Power	Launch KVM Ping	CIMC Reboot Locator LED 🖗	•
rtificate Management Secure Key Management Security Cor	figuration Ping Details	_	• ×		-
Download Root CA Certificate Export Root CA Certificate Delete Root CA C Delete Client Certificate Download Client Private Key Export Client Private F	* HostnamelIP 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		

Stellen Sie sicher, dass der Port 5696 auf dem CIMC- und dem KMIP-Server geöffnet ist. Sie können eine NMAP-Version auf unserem PC installieren, da dieser Befehl auf CIMC nicht verfügbar ist.

Sie können <u>NMAP</u> auf Ihrem lokalen Computer installieren, um zu testen, ob der Port geöffnet ist. Verwenden Sie in dem Verzeichnis, in dem die Datei installiert wurde, den folgenden Befehl:

nmap <ipAddress> -p <port>

Die Ausgabe zeigt einen offenen Port für den KMIP-Service:



Die Ausgabe zeigt einen geschlossenen Port für den KMIP-Service:



Zugehörige Informationen

- Konfigurationsanleitung für die C-Serie Selbstverschlüsselnde Laufwerke
- Konfigurationsanleitung für die C-Serie Key Management Interoperability Protocol
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.