スタンドアロンラックサーバでのリモートキー 管理の設定

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 背景説明

 SEDドライブ

 設定

 クライアント秘密キーとクライアント証明書の作成

 CIMCでのKMIPサーバの設定

 確認

 トラブルシュート

 関連情報

概要

このドキュメントでは、スタンドアロンラックサーバでのKey Management Interoperability Protocol(KMIP)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco インテグレーテッド マネージメント コントローラ (CIMC)
- ・自己暗号化ドライブ(SED)
- KMIP

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- UCSC-C220-M4S、CIMCバージョン: 4.1(1h)
- ・SEDドライブ
- •800 GBエンタープライズパフォーマンスSAS SED SSD(10 FWPD) MTFDJAK800MBS
- ・ドライブ部品ID:UCS-SD800GBEK9
- ベンダー: ミクロン
- Model:S650DC-800FIPS
- サードパーティのキーマネージャとしてのメトリック

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

KMIPは、キー管理サーバ上の暗号キーを操作するためのメッセージ形式を定義する拡張可能な通 信プロトコルです。これにより、暗号化キーの管理が簡素化されるため、データの暗号化が容易 になります。

SEDドライブ

SEDは、暗号化回路が内蔵されたハードディスクドライブ(HDD)またはソリッドステートドライ ブ(SSD)です。メディアに書き込まれたすべてのデータを透過的に暗号化し、ロック解除される と、メディアから読み取られたすべてのデータを透過的に復号化します。

SEDでは、暗号化キー自体がSEDハードウェアの制約を離れることはないため、OSレベルの攻撃 から安全です。

SEDドライブワークフロー:



(一) SEDドライブフロー

ドライブのロックを解除するためのパスワードは、**ローカルキー管理**設定を使用してローカルで 取得できます。この設定では、ユーザがキー情報を記憶する必要があります。また、Remote Key Management(RRM)を使用して、セキュリティキーを作成してKMIPサーバから取得することもで きます。ユーザの責任は、CIMCでKMIPサーバを設定することです。

設定

クライアント秘密キーとクライアント証明書の作成

これらのコマンドは、Cisco IMCではなく、OpenSSLパッケージを搭載したLinuxマシンで入力す る必要があります。ルートCA証明書とクライアント証明書で共通名が同じであることを確認しま す。

注: Cisco IMC時間が現在の時間に設定されていることを確認します。

1.2048ビットのRSAキーを作成します。

2.既に作成されているキーを使用して自己署名証明書を作成します。

openssl req -new -x509 -key client_private.pem -out client.pem -days 365 3.ルートCA証明書の取得の詳細については、KMIPベンダーのドキュメントを参照してください 。

注:Vormetricでは、RootCa証明書内の共通名がVormetricホストのホスト名と一致する必要 があります。

注:KMIPベンダーの設定ガイドにアクセスするには、アカウントが必要です。 <u>SafeNet</u> 渦の

CIMCでのKMIPサーバの設定

1. [Admin] > [Security Management] > [Secure Key Management] に移動します。

明確な設定は次のとおりです Export/Delete buttons grayed out, only Download buttons are active.



2. IPアドレスをクリックし、KMIPサーバーのIPを設定します。IPアドレスに到達できることを確

Enable Secure Key Management: 🗹

KMIP Servers

Delete Test Connection						
	ID	IP Address	Port	Timeout		
	1	10.104.253.26	5696	5		
	2	Save Cance	96 s	5		

3.証明書と秘密キーをサーバにダウンロードします。ダウンロード可能な .pem file or just paste the content.

	le Secure Key I	fanagement 🗌			
MIP	· Servers				Download Root CA Certificate
	1D 1 2	IP Address 10.104.253.26	Port 5696 5696	Timeout 5 5	Download from remote location Download through browser Client Paste Content
- K	MIP Root CA	Certificate			Paste Root CA Certificate Content:
• к	MIP Root CA Server R	Certificate out CA Certificate: Not Available			Paste Root CA Certificate Content:
• K	MIP Root CA Server R	Certificate oot CA Certificate: Not Available Download Status: NONE			Paste Root CA Certificate Content:
• K	MIP Root CA Server R De	Certificate out CA Certificate: Not Available Download Status: NONE wmload Progress: 0			Paste Root CA Certificate Content:

4.証明書をアップロードすると、証明書が[Available] と表示され、アップロードされていない不足している証明書には[Not Available] と表示されます。

接続をテストできるのは、すべての証明書と秘密キーがCIMCに正常にダウンロードされた場合だ けです。

 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

5.(オプション)すべての証明書を取得したら、オプションでKMIPサーバのユーザとパスワード を追加できます。この設定は、サードパーティのKMIPサーバとしてのSafeNetに対してのみサポ ートされます。

6.接続をテストし、証明書が正しく、設定されたポートを介してKMIPサーバに到達できる場合は、正常に接続されていることを確認します。

€ duals Cisco In	tegrated Management	Controller		query on kmip-server run successfully!
/ / Security Mana	agement / Secure Key	Managem	ent 🚖	U OK
Certificate Management	Secure Key Management	Security Con	fguration	
Download Root CA Certifica	te Export Root CA Certificate	Selete Root CA C	Certificate Download Client Certificate Expo	of Client Certificate
Delete Client Certificate D	lownload Client Private Key Exp	rt Client Private I	Key Delete Client Private Key Delete KMIP	Login
Enable Secure Key Man	agement: 🗹			
KIND Convers				
Rivine Servers	nester			
Delete	inection			
ID	IP Address	Port	Timeout	
1	10.104.253.26	5696	5	
2		5696	6	
▼ KMIP Root CA Ce	rtificate		▼ KMIP Client Certifica	te
Server Root	CA Certificate: Available		Client Certificate:	Available
Dov	wnload Status: NONE		Download Status:	NONE
Down	load Progress: 0		Download Progress:	0
	Export Status: COMPLETED		Export Status:	COMPLETED
Ex	port Progress: 100		Export Progress:	100
▼ KMIP Login Detail	ls		 KMIP Client Private F 	Key
Us	e KMIP Login:		Client Private Key:	Available
Login name to	KMIP Server: Enter User Nam	e	Download Status:	NONE
Password to	KMIP Server:		Download Progress:	0
Char	nge Password:		Export Status:	COMPLETED
			Export Progress:	100

7. KMIPとの接続が成功したら、リモートキー管理を有効にできます。

[Networking] > [Modular Raid Controller] > [Controller Info] に移動します。

注:以前に**ローカルキー管理**が有効になっていた場合は、リモート管理に変更するために現 在のキーを入力するように求められます

Controller Info	Physical Drive Info Vin	tual Drive Info Battery Backup	Unit Stor	age Log				
Create Virtual Drive	a from Unused Physical Drives C	Create Virtual Drive from an Existing Virt	al Drive Group	Import Foreign Config Clear Foreig	n 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	Key Management Switch to Loca	al Key Management						
	Enable Dri	ive Security		0	×			
 Health/Sta 	Health/Status Controller Security: Disabled							
	Comp Key Man	agement: Remote Key Manager	nent C	Local Key Management	al:	300 sec		
	Conti			Save Cano	el te:	30 %		
	RAID Chip Temperature:	68		Patrol Re-	ad Rate:	30 %		
	Storage Firmware Log Status:	Not Downloaded		Consistency Che	ck Rate:	30 %		
- Eirmurara	Versions			Reconstruction	on Rate:	30 %		
• Firmware	Versions			Cache Flush	Interval:	4 sec		
	Product Name:	Cisco 12G Modular Raid Controller w	th: 🕜	Max Driver To Spin Ho /	t Oncor	4		

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CLIから設定を確認できます。

1. KMIPが有効かどうかを確認します。

C-Series-12# scope kmip C-Series-12 /kmip # show detail Enabled: yes 2. IPアドレス、ポート、およびタイムアウトを確認します。

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.証明書が使用可能かどうかを確認します。

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.ログインの詳細を確認します。

C-Series-12 /kmip # show kmip-login Use KMIP Login Login name to KMIP server Password to KMIP

5.接続をテストします。

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!

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

KMIPサーバとのテスト接続が成功しない場合は、サーバにpingできることを確認します。

Cisco Integrated Management Controller			₽ V 2	admin@10.82.171.164 - C-Series-12 🥻
/ Security Management / Secure Key Managemen	Refresh Host Power La	CIMC Reboot Locator LED 🔞		
rtificate Management Secure Key Management Security Conf	fouration Ping Details	_	• ×	
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 D	etails	
KMIP Servers Delete Test Connection		Ping	Cancel	

CIMCとKMIPサーバでポート5696が開いていることを確認します。このコマンドはCIMCでは使 用できないため、NMAPバージョンをPCにインストールできます。

ローカルマシンに<u>NMAP</u>をインストールして、ポートが開いているかどうかをテストできます。 ファイルがインストールされたディレクトリで、次のコマンドを使用します。

nmap <ipAddress> -p <port> 出力は、KMIPサービスのオープンポートを示しています。



出力は、KMIPサービスのクローズポートを示しています。



関連情報

- <u>Cシリーズ構成ガイド 自己暗号化ドライブ</u>
- Cシリーズ構成ガイド Key Management Interoperability Protocol
- ・テクニカル サポートとドキュメント Cisco Systems

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。