Configure Remote Key Management on Standalone Rack Servers

Contents

Introduction Prerequisites Requirements Components Used Background Information SED Drives Configure Create a Client Private Key and Client Certificate Configure KMIP Server on the CIMC Verify Troubleshoot Related Information

Introduction

This document describes the configuration of the Key Management Interoperability Protocol (KMIP) on standalone rack servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Integrated Management Controller (CIMC)
- Self-encrypting drive (SED)
- KMIP

Components Used

The information in this document is based on these software and hardware versions:

- UCSC-C220-M4S, CIMC Version: 4.1(1h)
- SED Drives
- 800GB Enterprise performance SAS SED SSD (10 FWPD) MTFDJAK800MBS
- Drive Part ID: UCS-SD800GBEK9
- Vendor: MICRON
- Model: S650DC-800FIPS
- Vormetric as third-party key manager

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The KMIP is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption because simplifies encryption key management.

SED Drives

A SED is a hard disk drive (HDD) or solid-state drive (SSD) with an encryption circuit built into the drive. It transparently encrypts all data written to the media and, when unlocked, transparently decrypts all data read from the media.

In a SED, the encryption keys themselves never leave the confines of the SED hardware and therefore are safe from OS-level attacks.

SED drives workflow:



1. SED drive flow

The password to unlock the drive can be obtained locally with Local Key

Management configuration where the user's responsibility is to remember the key information. It can also be obtained with Remote Key Management where the security key is created and fetched from a KMIP server and the user's responsibility is to configure the KMIP server in CIMC.

Configure

Create a Client Private Key and Client Certificate

These commands are to be entered on a Linux machine with the OpenSSL package, not in the Cisco IMC. Ensure that the Common Name is the same in the Root CA certificate and in the Client certificate.

Note: Ensure that the Cisco IMC time is set to the current time.

1. Create a 2048-bit RSA key.

2. Create a self-signed certificate with the key already created.

openssl req -new -x509 -key client_private.pem -out client.pem -days 365 3. Refer to the KMIP vendor documentation for details about the obtention of the Root CA certificate.

Note: Vormetric requires that the common name in the RootCa certificate match the hostname of the Vormetric host.

Note: You must have an account to have access to the configuration guides for the KMIP vendors: <u>SafeNet</u> Vormetric

Configure KMIP Server on the CIMC

1. Navigate to Admin > Security Management > Secure Key Management.

A clear configuration shows Export/Delete buttons grayed out, only Download buttons are active.



2. Click on the IP address and set the IP for the KMIP server, ensure that you are able to reach it

and in case the default port is used nothing else needs to be changed, then save the changes.

Enable Secure Key Management: 🗹

KMIP Servers

Delete Test Connection							
	ID	IP Address	Port	Timeout			
	1	10.104.253.26	5696	5			
	2	Save Cance	96 396	5			

3. Download the certificates and private key to the server. You can download the .pem file or just paste the content.

		agement.			
MIF	Servers				Download Root CA Certificate
	ID	IP Address	Port	Timeout	Download from remote location Download from remote location
	1 2	10.104.253.26	5696 5696	5	Paste Content
					Paste Root CA Certificate Content:
• к	MIP Root CA Ce	rtificate			Paste Root CA Certificate Content:
• K	MIP Root CA Cer Server Root (rtificate CA Certificate: Not Available			Paste Root CA Certificate Content:
• К	MIP Root CA Cer Server Root (Dow Down	rtificate CA Certificate: Not Available wnioad Status: NONE load Progress: 0			Paste Root CA Certificate Content:
• K	MIP Root CA Cer Server Root (Dow Downi	rtificate CA Certificate: Not Available www.oad Status: NONE load Progress: 0 Export Status: NONE			Paste Root CA Certificate Content:

4. When you upload the certificates, you see that certificates show as **Available**, for the missing certificates that are not uploaded you see **Not Available**.

You can only test the connection when all certificates and private keys have been successfully downloaded to the CIMC.

 KMIP Root CA Ce 	rtificate	 KMIP Client Certificate 	e
Server Root	CA Certificate: Available	Client Certificate:	Not 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 	s	✓ KMIP Client Private Ke	ey
▼ KMIP Login Detail Us	ls e KMIP Login: 🗌	 KMIP Client Private Key: 	ey Not Available
✓ KMIP Login Detail Us Login name to	IS e KMIP Login: • KMIP Server: Enter User Nam	KMIP Client Private Key: Download Status:	Not Available
 KMIP Login Detail Us Login name to Password to 	IS e KMIP Login: • KMIP Server: Enter User Nam • KMIP Server: •••••	KMIP Client Private Key: Client Private Key: Download Status: Download Progress:	Not Available NONE 0
 KMIP Login Detail Us Login name to Password to Char 	IS e KMIP Login: • KMIP Server: Enter User Nam • KMIP Server: ••••• nge Password:	KMIP Client Private Key: Client Private Key: Download Status: Download Progress: Export Status:	ey Not Available NONE 0 COMPLETED
 KMIP Login Detail Us Login name to Password to Char 	IS e KMIP Login: • KMIP Server: Enter User Nam • KMIP Server: ••••• nge Password:	 KMIP Client Private Key: Client Private Key: Download Status: Download Progress: Export Status: Export Progress: 	Not Available NONE 0 COMPLETED 100

5. (optional) Once you have all the certificates, you can optionally add the user and password for the KMIP server, this configuration is only supported for SafeNet as a third party KMIP server.

6. Test the connection and if the certificates are correct and you are able to reach the KMIP server through the configured port, you see a successful connection.

÷	cisco Cisco In	tegrated Manag	gement Contr	oller			query on kmip-server run successfully!	
) / /	/ Security Mana	agement / Sec	ure Key Mana	gement 🚽	r			ок
Certific	ate Management	Secure Key Mana	gement Secur	ty Configuratio	n			
Down	load Root CA Certifica	ite Export Root CA C	ertificate Delete R	ot CA Certificat	e Download Client Certifi	icate Export	Client Certificate	
	e Client Certificate D	Download Client Private	Key Export Client	Private Key D	elete Client Private Key	Delete KMIP L	ogin	
Ena	ble Secure Key Man	agement: 🗹						
KM	P Servere							
- NW	Delete Test Con	notion						
	rest Con	mecuon						
	ID	IP Address	Po	et Ti	neout			
	1	10.104.253.26	56	6 5				
	2		56)6 5				
- ¥ 1	KMIP Root CA Ce	rtificate			 KMIP Client 	t Certificate		
	Server Root	CA Certificate: Auai	lable		Client	Certificate:	Available	
	Dov	wnload Status: NOP	ε		Downlo	oad Status:	NONE	
	Down	load Progress: 0			Download	d Progress:	0	
		Export Status: COI	IPLETED		Exp	oort Status:	COMPLETED	
	Đ	oport Progress: 100			Expor	t Progress:	100	
- ¥ 1	KMIP Login Detai	Is			 KMIP Client 	t Private Ke	у	
	Us	e KMIP Login:			Client P	rivate Key:	Available	
	Login name to	KMIP Server: Ente	er User Name		Downlo	ood Status:	NONE	
	Password to	KMIP Server:			Download	d Progress:	0	
	Char	nge Password:			Exp	oort Status:	COMPLETED	
					Expor	t Progress:	100	

7. Once our connection with KMIP is successful, you can enable remote key management.

Navigate to **Networking > Modular Raid Controller > Controller Info**.

Note: If previously **Local Key Management** was enabled, you are asked for the current key in order to change for remote management

Controller Info Physical Drive Info Vi	tual Drive Info Battery Backup Unit	Storage 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 En	ble Drive Security Disable Drive Security Clea	ar Cache Clear all Configuration Set Factory Defau	its (
Switch to Remote Key Management Switch to Loc	al Key Management						
Enable Dr	ive Security	⊙ ×					
Health/Status Controller Security: Disabled							
Comp Key Mar	agement: Remote Key Management	O Local Key Management al:	300 sec				
Conti		Save Cancel le:	30 %				
RAID Chip Temperature:	68	Patrol Read Rate:	30 %				
Storage Firmware Log Status:	Not Downloaded	Consistency Check Rate:	30 %				
- Flannen Mansland		Reconstruction Rate:	30 %				
Firmware versions		Cache Flush Interval:	4 sec				
Product Name:	Cisco 12G Modular Raid Controller with:	Max Drives To Spin Up At Opcer	4				

Verify

Use this section in order to confirm that your configuration works properly.

From the CLI you can verify the configuration.

1. Verify if KMIP is enabled.

C-Series-12# scope kmip C-Series-12 /kmip # show detail Enabled: yes 2. Verify the IP address, port, and timeout.

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. Verify if the certificates are available.

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. Verify log in details.

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

5. Test the connection.

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!

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

If the test connection with the KMIP server is not successful, ensure you can ping the server.

Cisco Integrated Management Controller			÷ V2	admin())10.82.171.164 - C-Series-12 Q
/ Security Management / Secure Key Manageme	nt	Refresh Host Pow	ar Launch KVM Ping	CIMC Reboot Locator LED 🔞
rtificate Management Secure Key Management Security Con	figuration Ping Details	_	• ×	
Download Root CA Certificate Export Root CA Certificate Delete Root CA Ce Delete Client Certificate Download Client Private Key Export Client Private K	* HostnameIP Address * Number of Retries	10.104.253.26		
Enable Secure Key Management: 🗹	* Timeout Ping Status	10 Success	Details	
KMIP Servers Delete Test Connection		•	Gancel	

Ensure that port 5696 is opened on the CIMC and the KMIP server. You can install an NMAP version on our PC, as this command is not available on CIMC.

You can install <u>NMAP</u> on your local machine, to test if the port is opened; under the directory where the file was installed, use this command:

nmap <ipAddress> -p <port>

The output shows an open port for KMIP service:



The output shows a closed port for KMIP service:



Related Information

- <u>C Series Configuration Guide Self Encrypting Drives</u>
- C Series Configuration Guide Key Management Interoperability Protocol
- Technical Support & Documentation Cisco Systems