

CryptoPanel

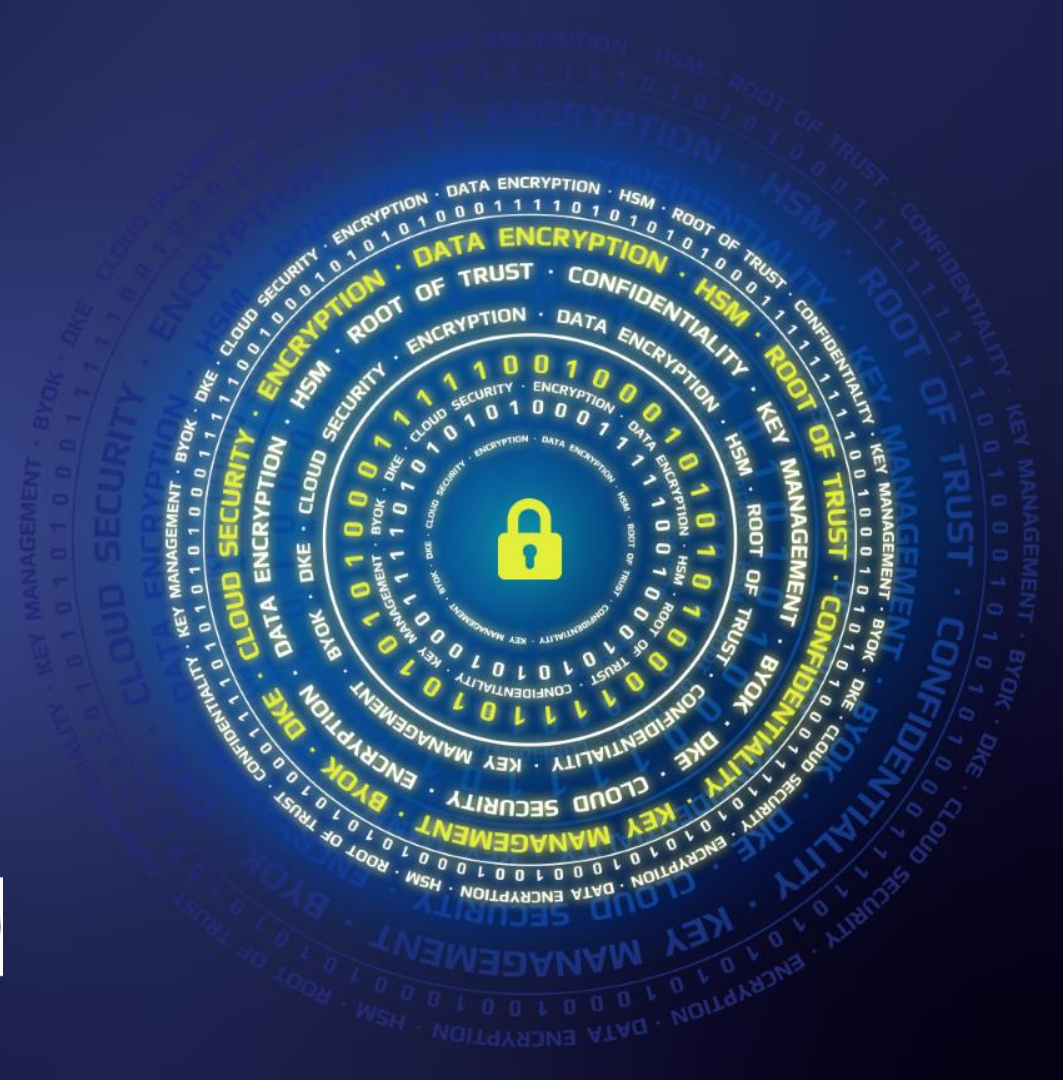
za chwilę zaczynamy...



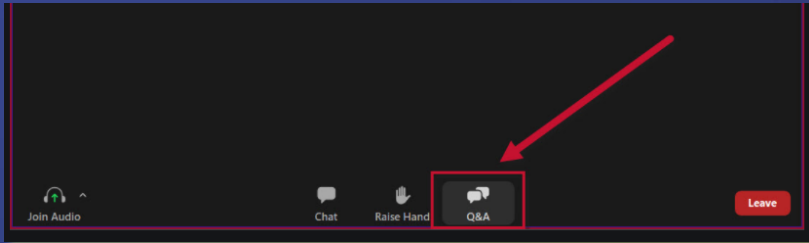
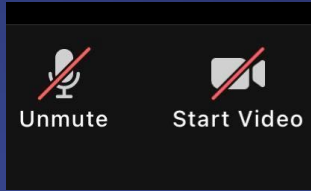
CryptoPanel



THALES



CryptoPanel



CryptoPanel

dziś dyskutują



Joanna Rzepka

Channel Sales Manager

joanna.rzepka@thalesgroup.com

mob. +48 600 537 666



Piotr Majek

Security Specialist

piotr.majek@clico.pl

mob. +48 663 994 996



CryptoPanel

Zewnętrzny system zarządzania kluczami
szyfrującymi dla pamięci masowych
na przykładzie integracji z rozwiązaniami DELL



CryptoPanel



problem



co nas boli...

- Posiadamy kilka zestawów macierzy dyskowych w swoich zasobach, zamierzamy kupić lub wynająć kolejne.
- Jesteśmy zobligowani do szyfrowania danych w spoczynku dla spełnienia wymogów zgodności.
- Musimy zapewnić wyłączną kontrolę nad danymi przechowywanymi w macierzach dyskowych które wynajmujemy.
- Wysoka dostępność danych przechowywanych w pamięciach masowych jest kluczowa.
- Jeżeli to możliwe chcemy dywersyfikować jakim kluczem szyfrowany jest zasób (wydzielony z pamięci masowej).
- ...że nie posiadamy centralnego systemu dystrybucji i kontroli kluczy szyfrujących dla różnych systemów gdzie musimy szyfrować dane w spoczynku
- ...że nie rozumiemy modelu licencjonowania, boimy się rosnących kosztów w przypadku powiększania zasobów macierzy dyskowych lub tworzenia układów nadmiarowych
- ...że nie wiemy co de facto się stanie gdy pamięć masowa nie może uzyskać klucza szyfrującego



CryptoPanel



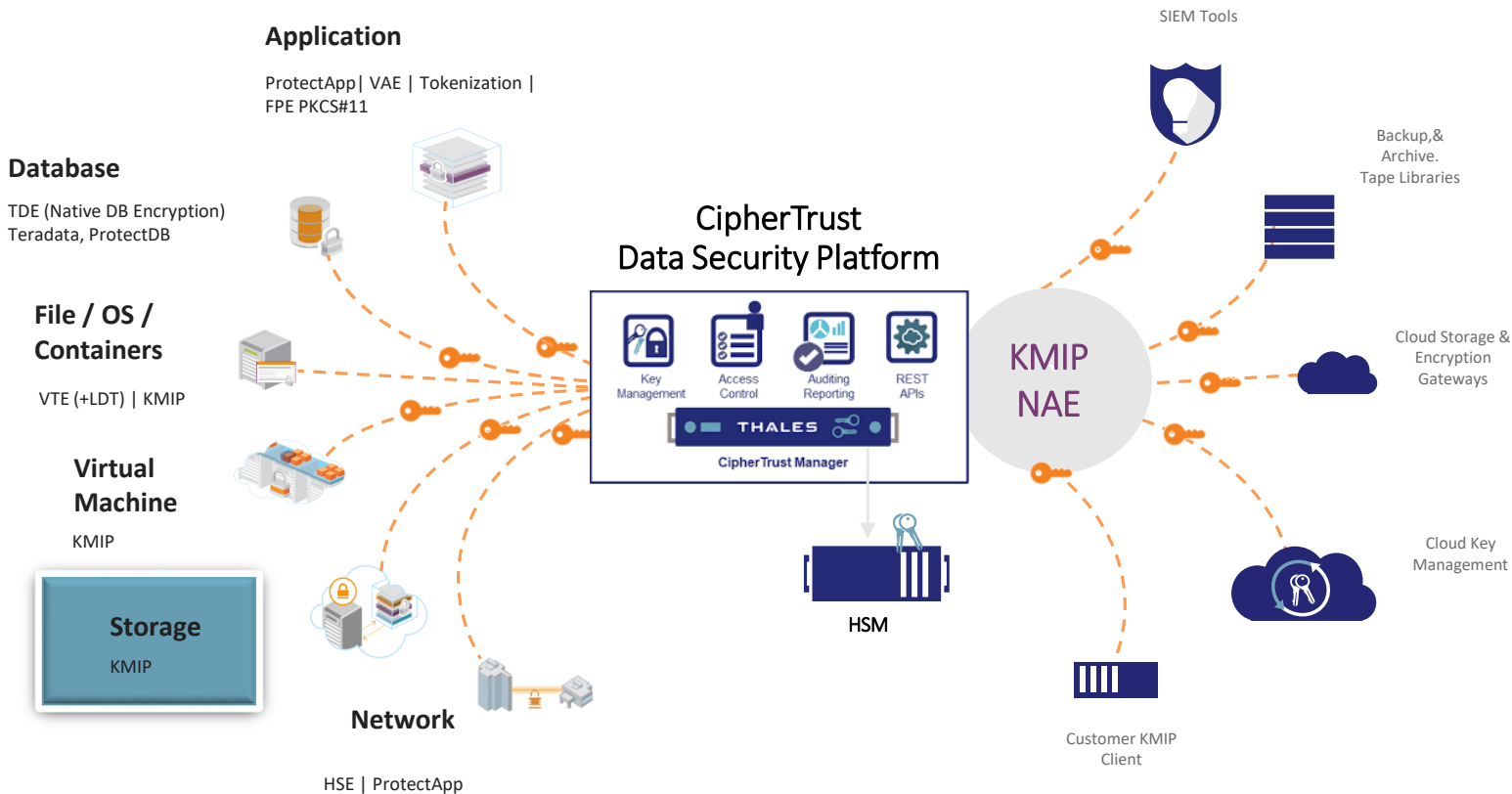
rozwiązanie



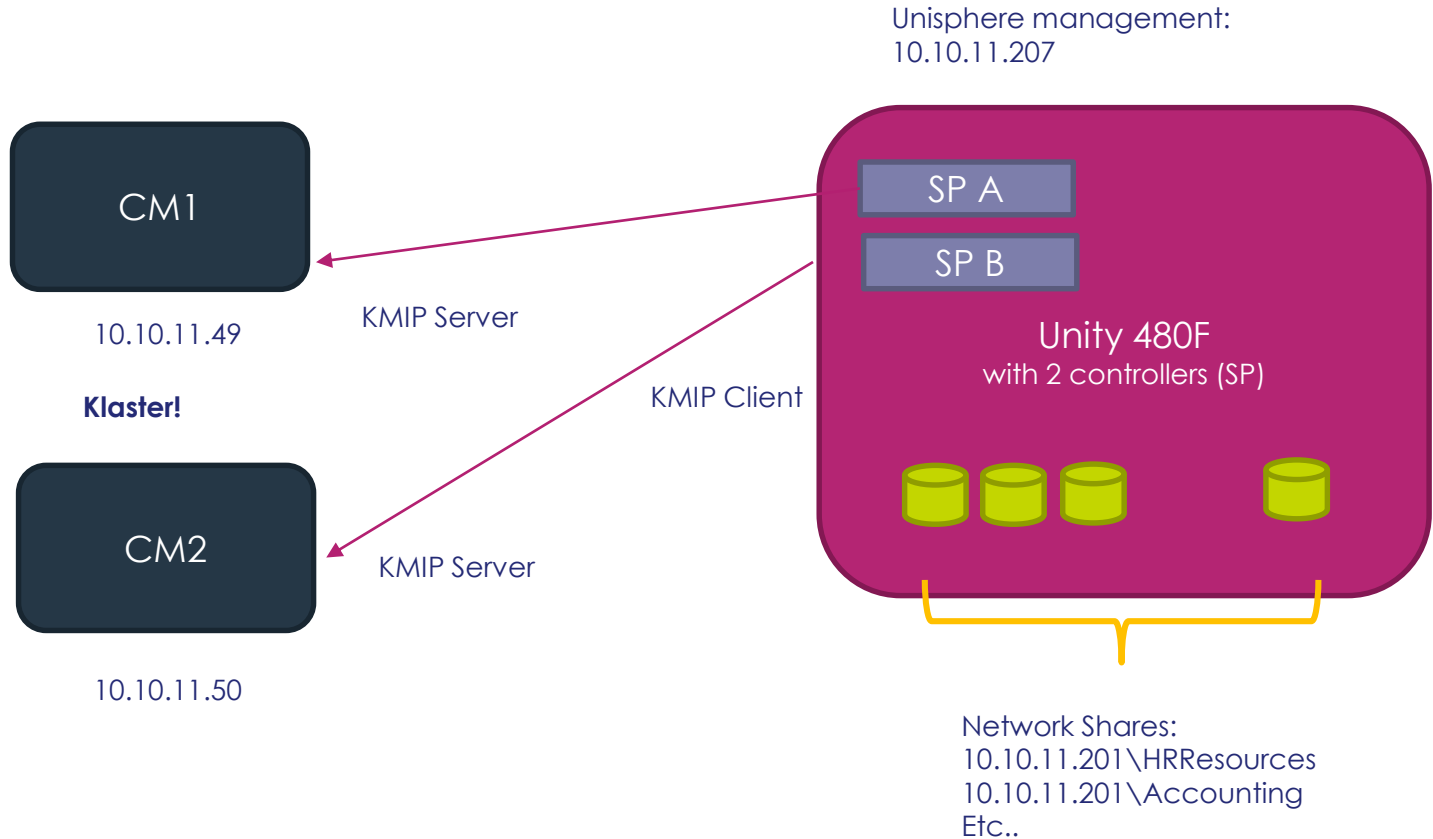
Rozwiązanie – CipherTrust Manager jako wysokodostępny Server KMIP dla pamięci masowych



Enterprise Key Management Solution



Rozwiązanie – przykład



Rozwiązanie – CM w integracji po KMIP. Dlaczego KMIP?

- Wykorzystujemy standard przemysłowy – szeroki zakres współdziałania
- Z definicji: wysoka dostępność
- Łatwość integracji
- Możliwość realizacji HYOK w zasobach dzierżawionych lub „chmurowych”
- Pozwala uzyskać zgodność z regulacjami dotyczącymi szyfrowania i kontroli dostępu i rotacji kluczy,
- Certyfikowane integracje (np. CM2.x a Unisphere 5.1)

Key Management Interoperability Protocol

From Wikipedia, the free encyclopedia

The **Key Management Interoperability Protocol (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 by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both [symmetric](#) and [asymmetric](#) keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

The KMIP standard was first released in 2010. Clients and servers are commercially available from multiple vendors. The KMIP standard effort is governed by the [OASIS standards body](#). Technical details can also be found on the [official KMIP page](#) and [wiki](#).



Jak to zrobić (na przykładzie DELL Unity)?

1. Login to CM as admin to root domain

1. Check whether KMIP interface is enable and check authentication methods and supported cipher-suites (consult Unity documentation)
2. Create client profile [user name is in CN]
3. Create new registration token based on above profile
4. Add new client (KMIP) use created registration profile and then:
5. Download client cert & private key. Using Openssl create PFX file (cert and private key in one file protected by PWD) to be able to upload it to Unity.
6. Download Internal RootCA of CM

2. Go to Unity: Settings->Management->Encryption->Configure KMIP

1. provide IP of CM, port (default 5696), timeout.
2. Username = **admin** ; password = <CM admin password>
3. Upload client cert (PFX) and CM Internal RootCA cert to Unity
4. Enable KMIP. Unity connects and authenticates to CM, then create 1 symmetric key and export it.

3. Done.



Go to Unity: Ready to configure KMIP

The screenshot displays the EMC Unisphere web interface for a system identified as 'Unisphere CKM00200900601'. The browser's address bar shows the URL '10.10.11.207/index.html#icn=SYSTEM_PERFORMANCE'. The interface includes a sidebar with navigation options such as 'DASHBOARD', 'SYSTEM', 'STORAGE', 'ACCESS', 'PROTECTION & MOBILITY', 'EVENTS', and 'SUPPORT'. The main content area shows performance charts for 'SYSTEM - CPU UTILIZATION' and 'SYSTEM - LUN IOPS'. A 'Settings' dialog box is open, showing the 'Encryption' section. The 'Manage Encryption' section displays 'Mode: Controller Based Encryption', 'Status: Encrypted', and 'KMIP Status: Disabled'. The 'External Key Management' section has a red box around the 'Enable KMIP' button. The 'Keystore' section includes a 'Backup Keystore File' button and a note: 'Note: Data at Rest encryption is activated on the system. EMC recommends that you retrieve and save the keystore file to an external location.' The 'Audit Log' section has 'Download AuditLog & CheckSum' and 'Download CheckSum' buttons. The dialog box also features an 'Initial Configuration Wizard' link and a 'Close' button.



Unity: Add KMIP Sever (CM)

KMIP Configuration

Configure key management server properties

Username:

Password:

Port:

Timeout (s):

IP Addresses of the KMIP Server Cluster

10.10.11.49	<input type="button" value="Add"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Remove"/>

Note: First address is the primary KMIP server

The username is taken from CN of Client Certificate (in our case: **admin**)

Provide CM **admin** password

Add IP of first CM (.49)

Manage client certificates...



Unity: Manager Client Certificates

The image shows a composite screenshot of the Unity interface. On the left is the 'KMIP Configuration' panel with fields for Username, Password, Port (5696), and Timeout (10). The main area displays the 'Certificate Management' window with a table of certificates. A red arrow points from the 'Client' row in the table to the 'Import Trusted Certificate' dialog box, which has a file selection field containing 'certificate.pfx' and a 'Passphrase' field. Another red arrow points from the 'Client' row to a text box at the bottom right.

Type	Issued By	Issued To	Valid From	Valid To
Certificate Authority	CN=KeySecure Root CA,O...	CN=KeySecure Root CA,O...	6/22/2021, 2:52:23 PM	6/20/2031, 2:52:23 PM
Client	CN=KeySecure Root CA,O...	UID=admin,CN=b5297b0...	7/19/2021, 3:14:35 PM	7/19/2023, 3:14:35 PM

Type	Issued By	Issued To	Valid From	Valid To
Certificate Authority	CN=KeySecure Root CA,O...	CN=KeySecure Root CA,O...	6/22/2021, 2:52:23 PM	6/20/2031, 2:52:23 PM
Client	CN=KeySecure Root CA,O...	UID=admin,CN=b5297b0...	7/19/2021, 3:14:35 PM	7/19/2023, 3:14:35 PM

Import Trusted Certificate

Wybierz plik certificate.pfx

Passphrase: [REDACTED]

Cancel Import

Type	Issued By	Issued To	Valid From	Valid To
Certificate Authority	CN=KeySecure ...	CN=KeySecure Root CA,O=Gemalto,L=Belcamp,ST=MD,C=US	6/22/2021, 2:52:23 PM	6/20/2031, 2:52:23 PM
Client	CN=KeySecure ...	UID=admin,CN=admin,OU=Thales DIS Polska Sp. z o.o.,O=Thales DIS P...	7/21/2021, 12:19:11 PM	7/21/2023, 12:19:11 PM

Upload Internal Root CA of CM as well

Unity: Ready to enable KMIP

The image displays the Unity Settings application interface. The main window is titled 'Settings' and shows a sidebar with navigation options: 'Software and Licenses', 'Users and Groups', 'Management', 'Storage Configuration', 'Support Configuration', and 'Access'. The 'Management' section is expanded, showing options like 'System Time and NTP', 'DNS Server', 'Unisphere Central', 'Unisphere IPs', 'Remote Logging', 'Failback Policy', 'Performance', and 'Encryption'. The 'Encryption' option is selected, leading to the 'Manage Encryption' section. This section displays the following information:

- Mode: Controller Based Encryption
- Status: Encrypted
- KMIP Status: Disabled

Below this information, there are two sections:

- External Key Management:** Includes a 'Configure' button and an 'Enable KMIP' button.
- Keystore:** Includes a 'Backup Keystore File' button.

A note at the bottom of the 'Manage Encryption' section states: "Note: Data at Rest encryption is activated on the system. EMC recommends that you retrieve and save the keystore file to an external location." Below this note are two buttons: 'Download AuditLog & CheckSum' and 'Download CheckSum'.


A 'Job Properties' dialog box is open in the foreground, showing the details of a job:

- Job Name: Enable/Disable KMIP server
- Overall status: 0%
- Details: Enable/Disable KMIP server Running

Red arrows point from the 'Job Created' status bar (showing 0%) in the background window to the 'Job Properties' dialog box, indicating the job's progress.



Done. If all went well Unity creates keys in CM


Keys 

Name

Filters Basic Raw


Types Size

Latest Version Only

Type: Symmetric Key 

[+ Create a New Key](#)

Key Name	Version	Owner	Modified	Type	Algorithm	Size	Links
ks-916ff31ef69c40cb83b2747f9eab771966a73a30cf...	0	local admin	22 Jul 2021, 01:59	Symmetric	AES	256	...
ks-cf239373f80e4802acc53273e3f820452284ef41ac...	0	local c1bf3735-bd79-48ee-91bb-471aced84207	22 Jul 2021, 11:58	Symmetric	AES	256	...
citrus-66703163-ff25-4c90-9871-d276ae8bccee	0	No owner	23 Jun 2021, 02:54	Symmetric	AES	256	...

3 Keys 50 per page 

Records

- Server Records
- Client Records
- Admin Settings

```
{
  "id": "916ff31ef69c40cb83b2747f9eab771966a73a30cf06410c8df9",
  "url": "kylo:kylo:vault:keys:ks-916ff31ef69c40cb83b2747f9eab771966a73a30cf06410c8df9?v0",
  "name": "ks-916ff31ef69c40cb83b2747f9eab771966a73a30cf06410c8df9",
  "size": 256,
  "ownerId": "local|481ed15d-89c0-4a9d-bfe8-e1d2c286692",
  "algorithm": "AES",
  "usageMask": 12,
  "objectType": "Symmetric Key"
}
```



Done. If all went well Unity encrypts drives

```
CKM00200900601_2021_07_21_09_01_00_00000000000001_00000000000002C_full.log — Notatnik
Plik Edycja Format Widok Pomoc
2021-07-15 09:35:01 0000000000000006 ADD_SLIC FCNMD200100048 SPB BE 1
2021-07-15 09:35:06 0000000000000007 ENCRYPTION_ENABLED FCNWS194900079
2021-07-15 09:35:06 0000000000000008 CREATE_RG_KEY OBJ_ID 11 RG_ID 1004 POS 0 DRIVE ZVNA0M701996
2021-07-15 09:35:06 0000000000000009 CREATE_RG_KEY OBJ_ID 11 RG_ID 1004 POS 1 DRIVE ZVNA0M702189
2021-07-15 09:35:06 000000000000000A CREATE_RG_KEY OBJ_ID 11 RG_ID 1004 POS 2 DRIVE ZVNA0M702162
2021-07-15 09:35:06 000000000000000B CREATE_RG_KEY OBJ_ID 11 RG_ID 1004 POS 3 DRIVE ZVNA0M702195
2021-07-15 09:35:06 000000000000000C ENCRYPTION_ENABLED FCNWS194900079
2021-07-15 09:35:06 000000000000000D ENCRYPTION_ACTIVATION_START FCNWS194900079
2021-07-15 09:35:06 000000000000000E ENCRYPTION_ACTIVATION_COMPLETED FCNWS194900079
2021-07-15 09:35:09 0000000000000001 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 0 DRIVE ZVNA0M701996
2021-07-15 09:35:09 0000000000000002 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 1 DRIVE ZVNA0M702189
2021-07-15 09:35:09 0000000000000003 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 2 DRIVE ZVNA0M702162
2021-07-15 09:35:09 0000000000000004 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 3 DRIVE ZVNA0M702195
2021-07-15 09:35:10 0000000000000005 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 0 DRIVE ZVNA0M701996
2021-07-15 09:35:10 0000000000000006 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 1 DRIVE ZVNA0M702189
2021-07-15 09:35:10 0000000000000007 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 2 DRIVE ZVNA0M702162
2021-07-15 09:35:10 0000000000000008 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 3 DRIVE ZVNA0M702195
2021-07-15 09:42:52 0000000000000009 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 0 DRIVE ZVNA0M702235
2021-07-15 09:42:52 000000000000000A CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 1 DRIVE ZVNA0M701812
2021-07-15 09:42:52 000000000000000B CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 2 DRIVE ZVNA0M702013
2021-07-15 09:42:52 000000000000000C CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 3 DRIVE ZVNA0M702070
2021-07-15 09:42:52 000000000000000D CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 4 DRIVE ZVNA0M702230
2021-07-15 09:42:52 000000000000000E CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 5 DRIVE ZVNA0M702232
2021-07-15 09:42:52 000000000000000F CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 6 DRIVE ZVNA0M702162
2021-07-15 09:42:52 0000000000000000 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 7 DRIVE ZVNA0M702195
2021-07-15 09:42:52 0000000000000001 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 8 DRIVE ZVNA0M702189
2021-07-15 09:42:52 0000000000000002 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 9 DRIVE ZVNA0M701996
2021-07-20 12:00:23 0000000000000025 KMIP_ENABLED FCNWS194900079
2021-07-20 12:32:13 0000000000000026 KMIP_DISABLED FCNWS194900079
2021-07-20 12:34:06 0000000000000027 BACKUP_START FCNWS194900079
2021-07-20 12:34:10 0000000000000028 BACKUP_COMPLETED FCNWS194900079
2021-07-20 12:34:11 0000000000000029 BACKUP_START FCNWS194900079
2021-07-20 12:34:15 000000000000002A BACKUP_COMPLETED FCNWS194900079
2021-07-20 13:21:42 000000000000002B KMIP_ENABLED FCNWS194900079
2021-07-20 13:29:51 000000000000002C KMIP_DISABLED FCNWS194900079
```



What happens when key (KMIP Server) is not available for Unity Storage?



Niestety... nie można przejść do tej strony

Witryna 10.10.11.207 potrzebowała za dużo czasu na odpowiedź

Spróbuj wykonać:

- Sprawdzenie połączenia
- [Sprawdzenie serwera proxy i zapory](#)
- [Uruchamianie diagnostyki sieci systemu Windows](#)

ERR_CONNECTION_TIMED_OUT

▼ Szczegóły

The screenshot displays the Unity Storage management console. Two storage processors, A (Primary) and B, are shown. Both have a status of 'Service' and a warning icon. The error message for both is: 'Cannot retrieve encryption key from the external KMIP server configured on this Storage Processor (SP)'. The recommended action is: 'Please use svc_kmip command to change KMIP configuration or contact your service provider.' Below the error messages, there is a menu with options: 'Enter Service Mode', 'Reboot', 'Reimage', and 'Reset and Hold'. The 'Enter Service Mode' option is highlighted, and a description states: 'Entering Service Mode stops I/O on the SP so that service tasks can be safely performed.' An 'Execute' button is visible next to the description.

If they the KMIP Server is not accessible then:

- Problem to access web UI of Unity
- Unity **Storage runs in Service Mode** (Resources are not available!)
- To regain access to resources: make KMIP Server (and key) available and restart Storage Processors (SPA & SPB &). It takes a while (up to 20 min per each SP)



Adding second KMIP Server (CM) to Unity

KMIP Configuration

Configure key management server properties

Username:

Password:

Port:

Timeout (s):

IP Addresses of the KMIP Server Cluster

- 10.10.11.49
- 10.10.11.50

Note: First address is the primary KMIP server

Go to Unity: Settings->Management->Encryption->Configure KMIP

- Click: „Configure KMIP” then:
 - Add second CM (.50) as KMIP Server
 - Put username = **admin**
 - Put password = <CM admin password>
 - Click OK
- Done.

Be sure that dialog is filled up with proper data for each node. Don't believe in what is prompted.

KMIP Configuration

Configure key management server properties

Username:

Password:

Port:

Timeout (s):

IP Addresses of the KMIP Server Cluster

- 10.10.11.49
- 10.10.11.50

Note: First address is the primary KMIP server

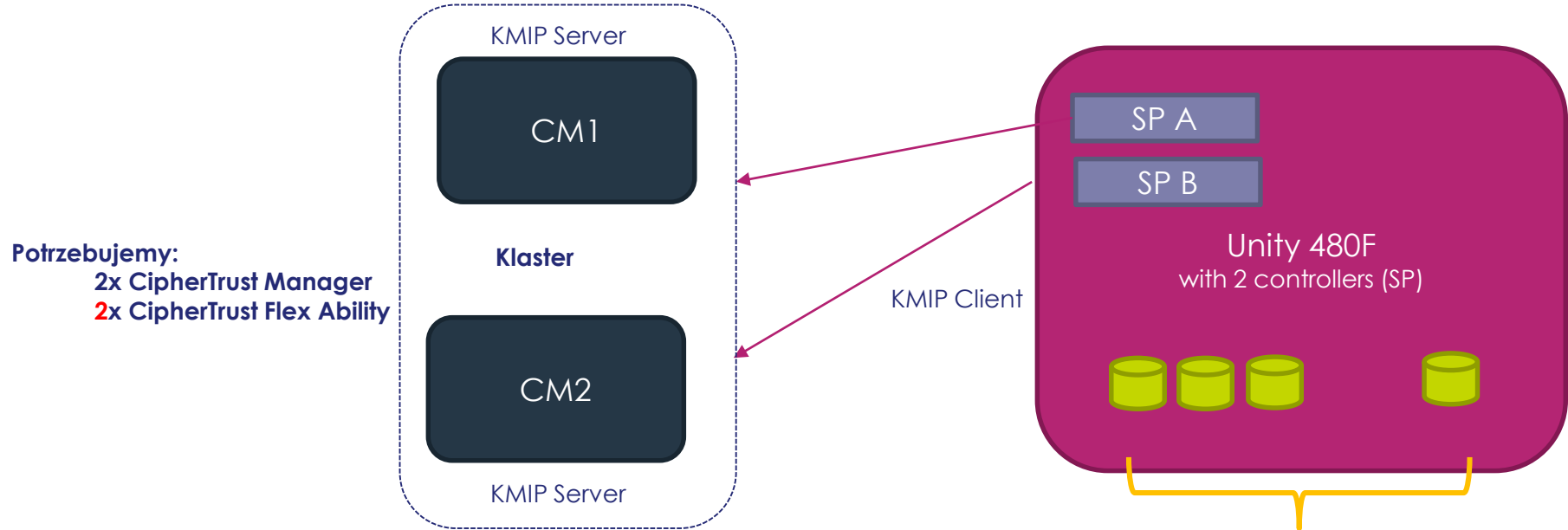
Configuration verified

Conclusion

- CM 2.4 and Unity Storage 480F integration over KMIP is easy and straightforward.
- Unity properly utilize CM cluster to obtain key.
- After enabling KMIP Sever on Unity – this resource becomes critical.
- Try to upgarde Unity to 5.1



A co z licencjonowaniem? #1



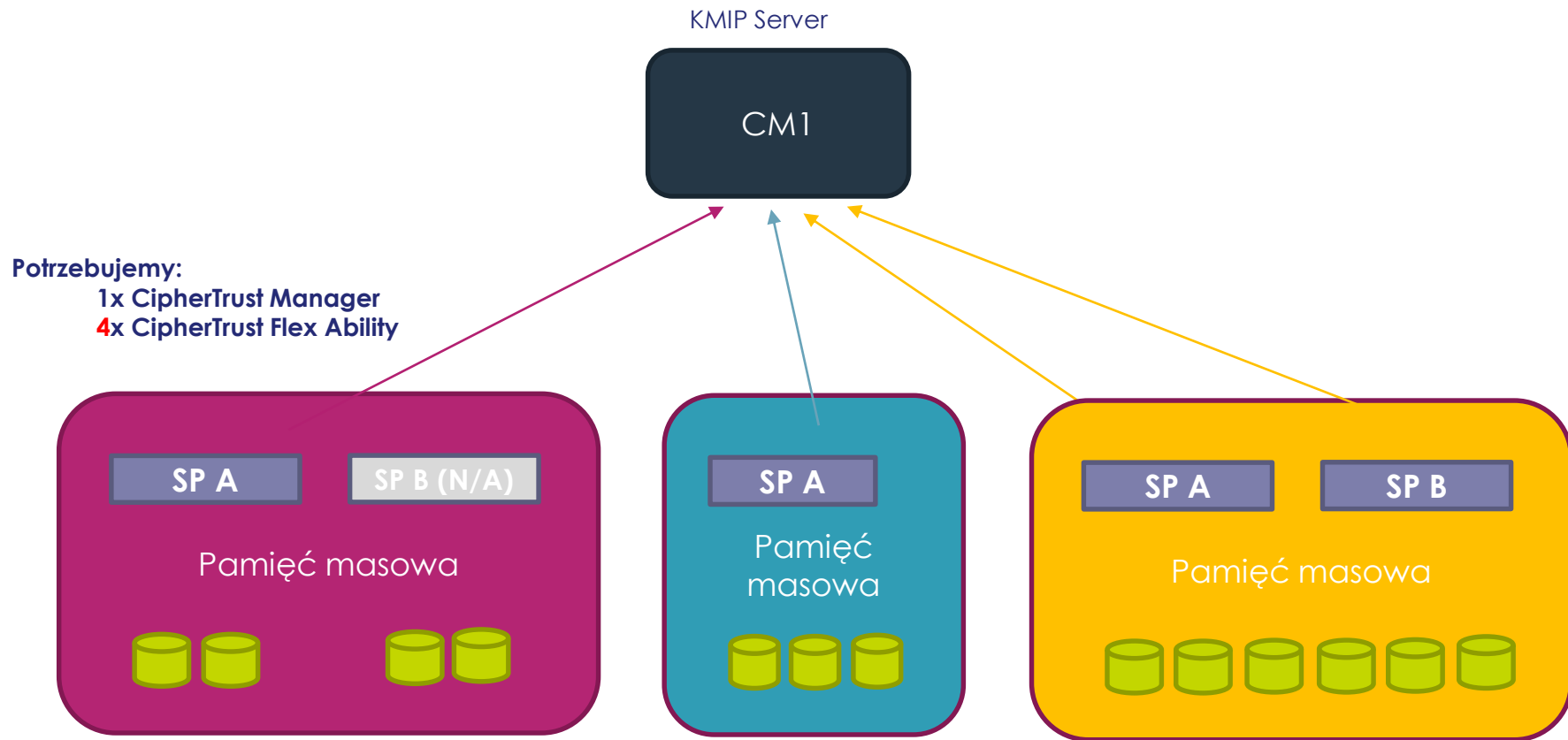
CipherTrust Flex Ability Connectors (KIP)

- CipherTrust Flex Ability, Perpetual
- CipherTrust Flex Ability, Term Based, Enhanced Support
- CipherTrust Flex Ability, Perpetual, Non-Prod
- CipherTrust Flex Ability, Term Based, Enhanced Support, Non-Prod

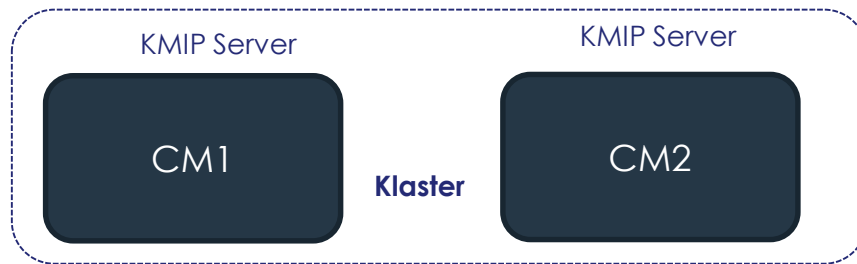
Network Shares:
10.10.11.201\HRResources
10.10.11.201\Accounting
Etc..



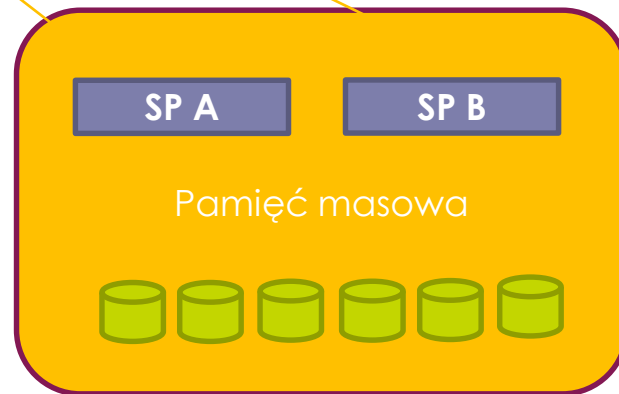
A co z licencjonowaniem? #2



A co z licencjonowaniem? #3



Potrzebujemy:
2x CipherTrust Manger
4x CiperTrust Flex Ability

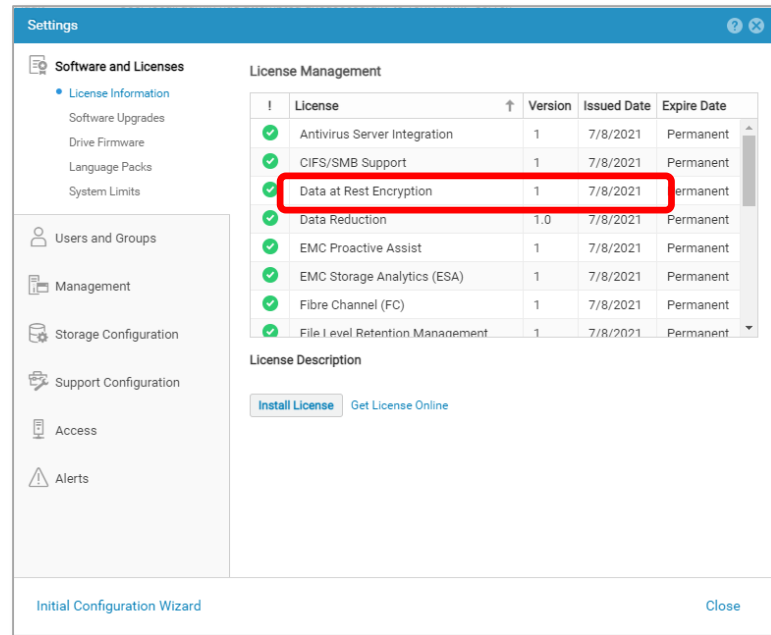


Nauczki, czyli lessons learned #1/2

1. Przed przystąpieniem do zabawy upewnij się, że macierz potrafi skorzystać z zewnętrznego serwera KMIP (licencje)

➤ Za darmo z nabyciem nowej DELL!

Ustanowienie zaufania KMIP Server (CM) – KMIP Client (macierz) oparte jest na certyfikatach. Wszystkie certyfikaty kiedyś wygasają – bądź przygotowany! Wpisz do kalendarza alarmy, ...



The screenshot shows the 'Settings' application window, specifically the 'License Management' section. The left sidebar contains a navigation menu with items like 'Software and Licenses', 'Users and Groups', 'Management', 'Storage Configuration', 'Support Configuration', 'Access', and 'Alerts'. The main area displays a table of licenses. The 'Data at Rest Encryption' license is highlighted with a red box. Below the table, there are buttons for 'Install License' and 'Get License Online'.

!	License	Version	Issued Date	Expire Date
✓	Antivirus Server Integration	1	7/8/2021	Permanent
✓	CIFS/SMB Support	1	7/8/2021	Permanent
✓	Data at Rest Encryption	1	7/8/2021	Permanent
✓	Data Reduction	1.0	7/8/2021	Permanent
✓	EMC Proactive Assist	1	7/8/2021	Permanent
✓	EMC Storage Analytics (ESA)	1	7/8/2021	Permanent
✓	Fibre Channel (FC)	1	7/8/2021	Permanent
✓	File Level Retention Management	1	7/8/2021	Permanent



Nauczki, czyli *lessons learned* #2/2

- ▮ Odebranie dostępu do klucza w KMS lub jego niedostępność powoduje niemożliwość uruchomienia macierzy!
- ▮ Zapewnij backup KMS! Przećwicz jego odtwarzanie! To teraz twój najważniejszy zasób 😊

▼ Storage Processor A (Primary)

Status: Cannot retrieve encryption key from the external KMIP server configured on this Storage Processor (SP).

Mode: Service

Recommended Action: Please use svc_kmip command to change KMIP configuration or contact your service provider.

Enter Service Mode Entering Service Mode stops I/O on the SP so that service tasks can be safely performed.

Reboot

Reimage

Reset and Hold Executes

▼ Storage Processor B

Status: Cannot retrieve encryption key from the external KMIP server configured on this Storage Processor (SP).

Mode: Service

Recommended Action: Please use svc_kmip command to change KMIP configuration or contact your service provider.



Tego nie znajdziecie w dokumentacji DELL-a

„When KMIP is disabled on Unity, the Encryption Key is deleted from the KMIP Server and persisted in a secure file on the array.”

*„...While KMIP is enabled Unity does a KMIP ‘heartbeat’ every **30 minutes**. This consists of connecting to each configured KMIP Server and retrieving the Encryption Key. If this fails for one or more KMIP Servers – e.g., cannot connect to the server, or the key is not retrieved – Unity sends an alert to notify the user, so the issue can be resolved...”*

Agree with kmip client logic is fuzzy..

So yes 2x should be more or scaling should be more.. but some kmip clients load balance horrible.. or some establish kmip connections to all registered CMs at some point.. If kmip types are known you might be able to drill down into them a little for more predictable scaling.



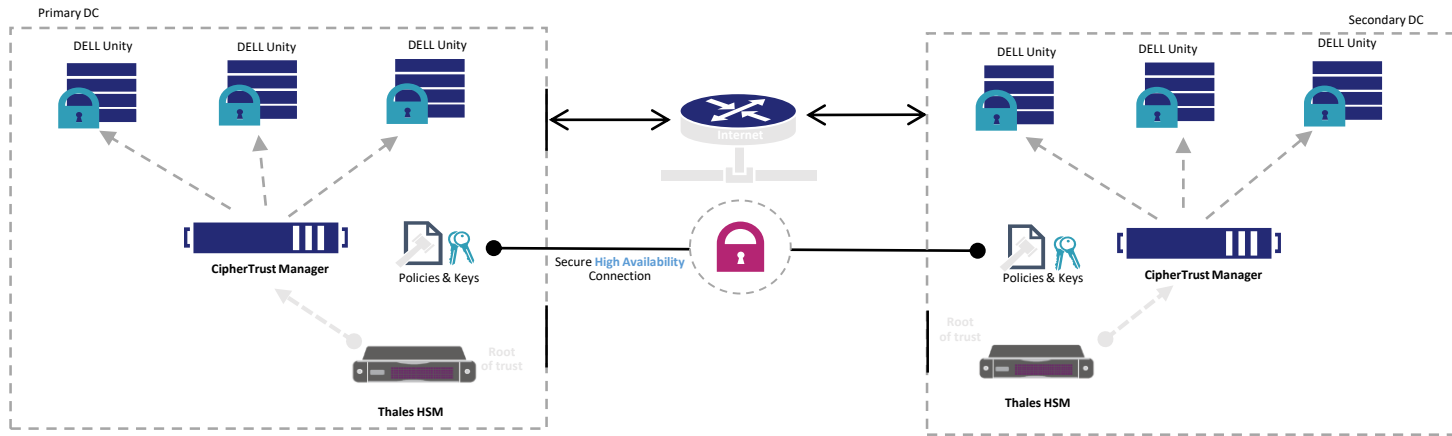
CryptoPanel



podsumowanie



podsumowanie



- produkty dostępne w kanale partnerskim
- licencja dożywotnia lub subskrypcja
- licencja demo do testów
- zalecane użycie urządzenia HSM

- CipherTrust Manager – 14,5k Euro netto
- CipherTrust Flex Ability (KMIP) – 450 Euro netto



CryptoPanel

