CryptoPanel

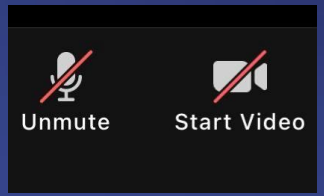
za chwilę zaczynamy...

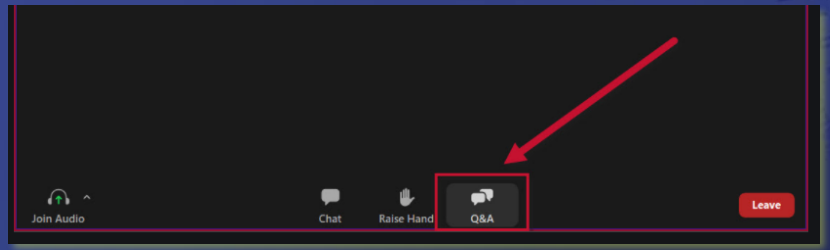
CryptoPanel

THALES

CLICO

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).

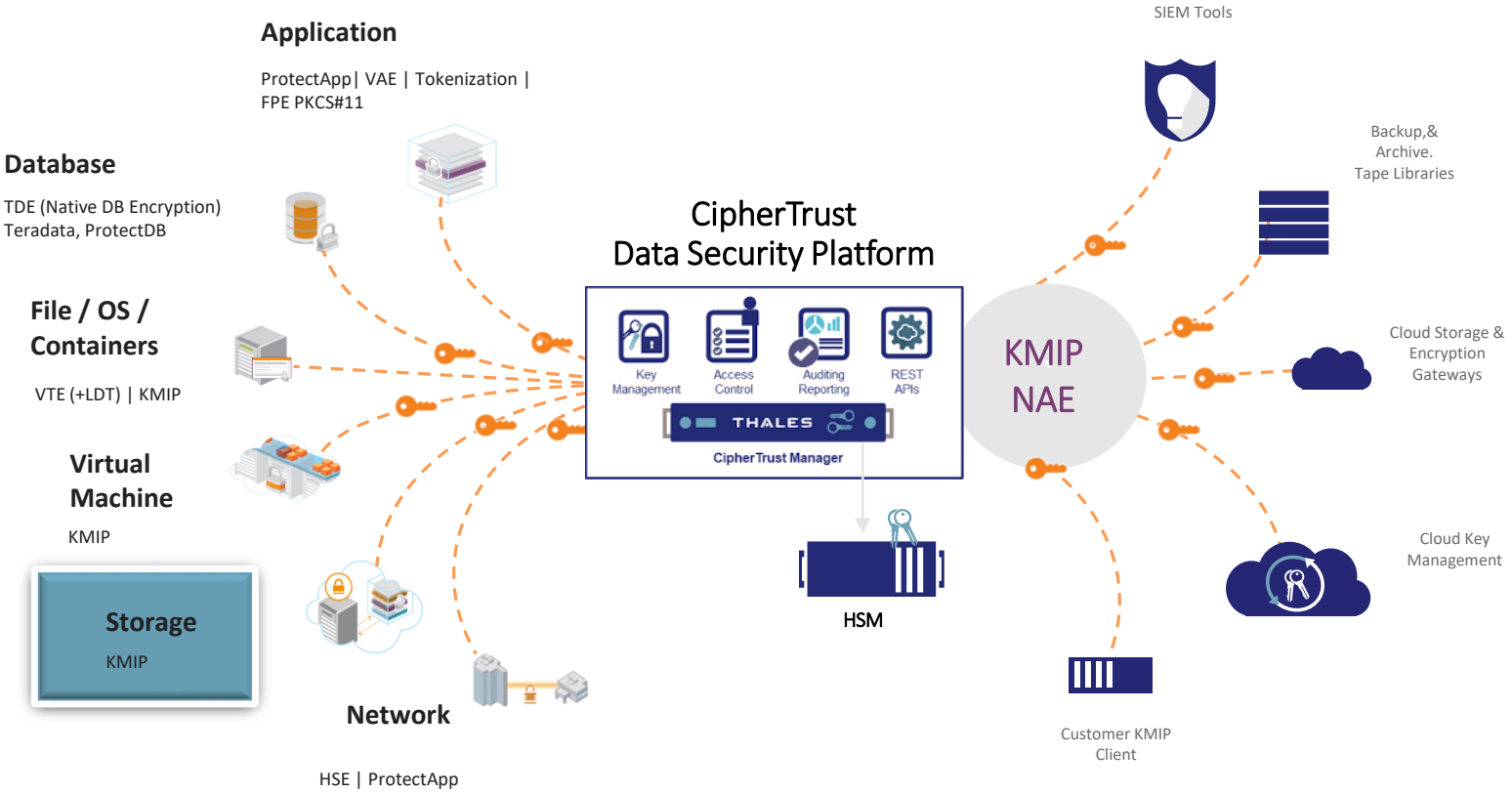
- ...że nie posiadamy centralnego systemu dystrybucji i kontroli kluczy szyfrujących dla różnych systemów gdzie musimy szyfrować dane w spoczynku
- ...że nie rozumiemy modelu licencjonowania, boimy się rosnących kosztów w przypadku powiększania zasobów macierzy dyskowych lub tworzenia układów nadmiarowych
- ...że nie wiemy co de facto się stanie gdy pamięć masowa nie może uzyskać klucza szyfrującego

CryptoPanel

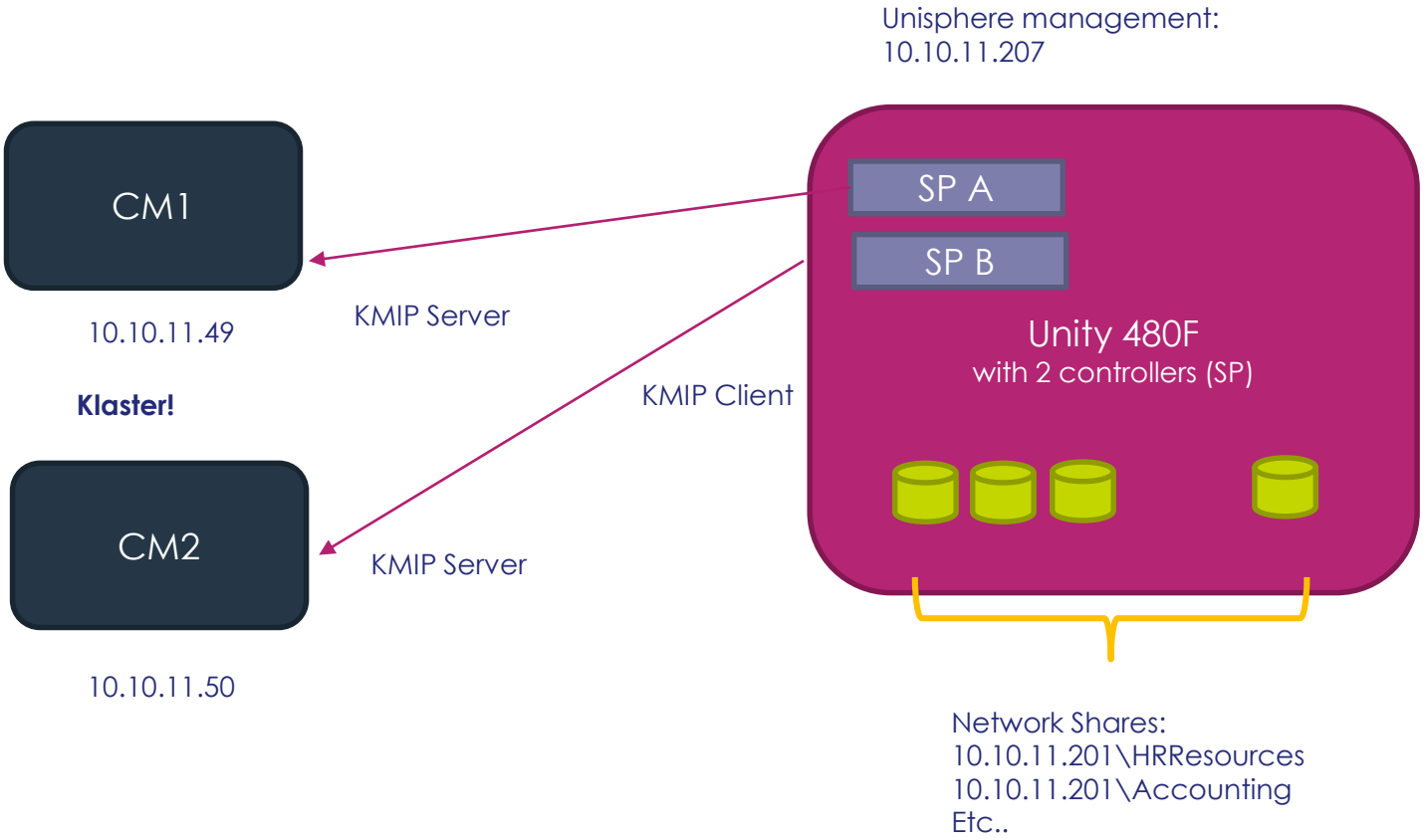
rozwiązanie

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

Key Management Interoperability Protocc

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.

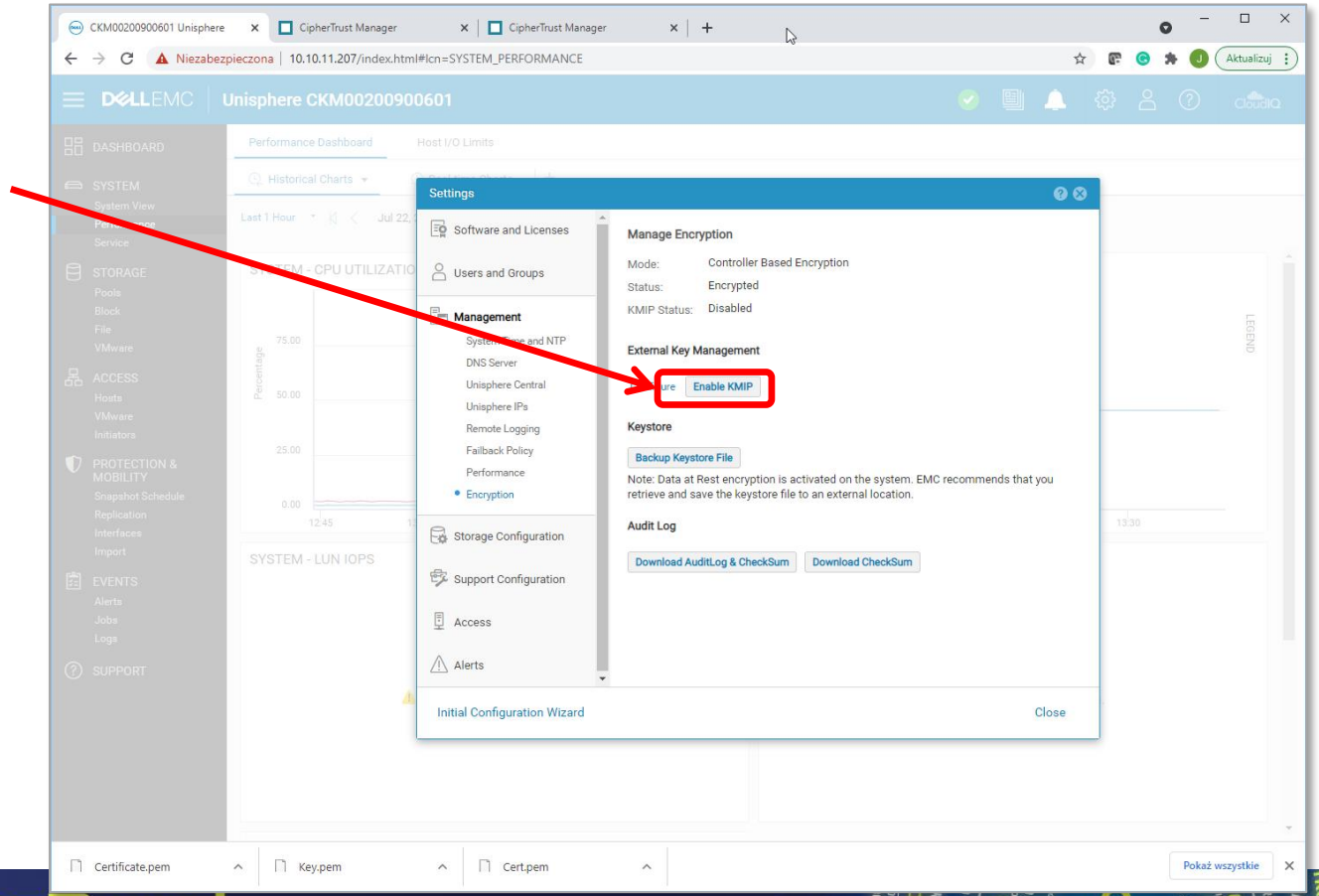
The KMIP standard was first released in 2010. Clients and servers are commercially available from multiple vendors. The KMIP standard effort is governed by the OASIS standards body. Technical details can also be found on the official KMIP pages and wiki.

- 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)

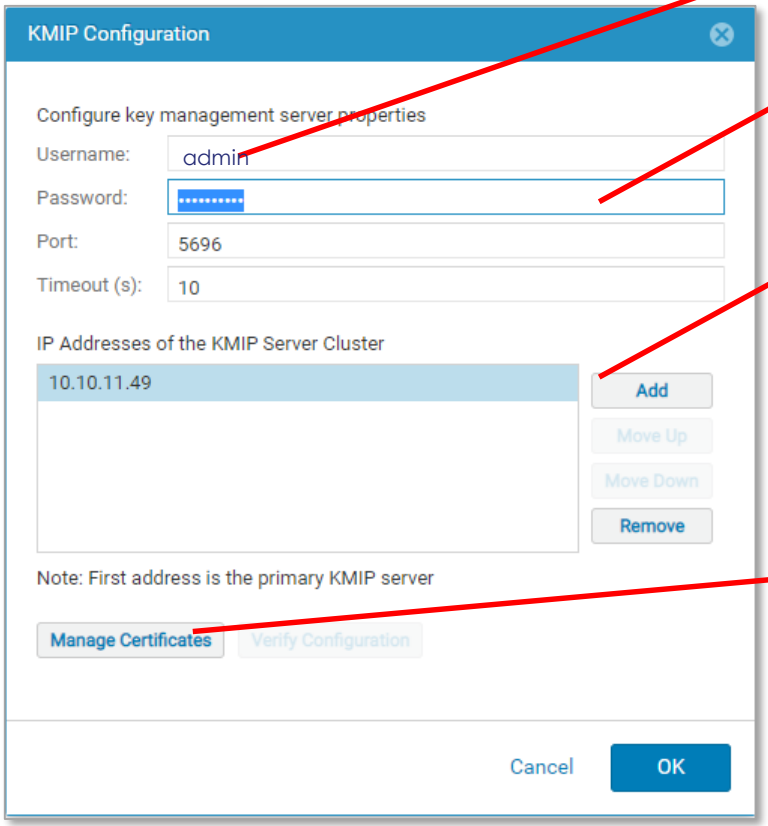
Jak to zrobić (na przykładzie DELL Unity)?

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



Unity: Add KMIP Sever (CM)



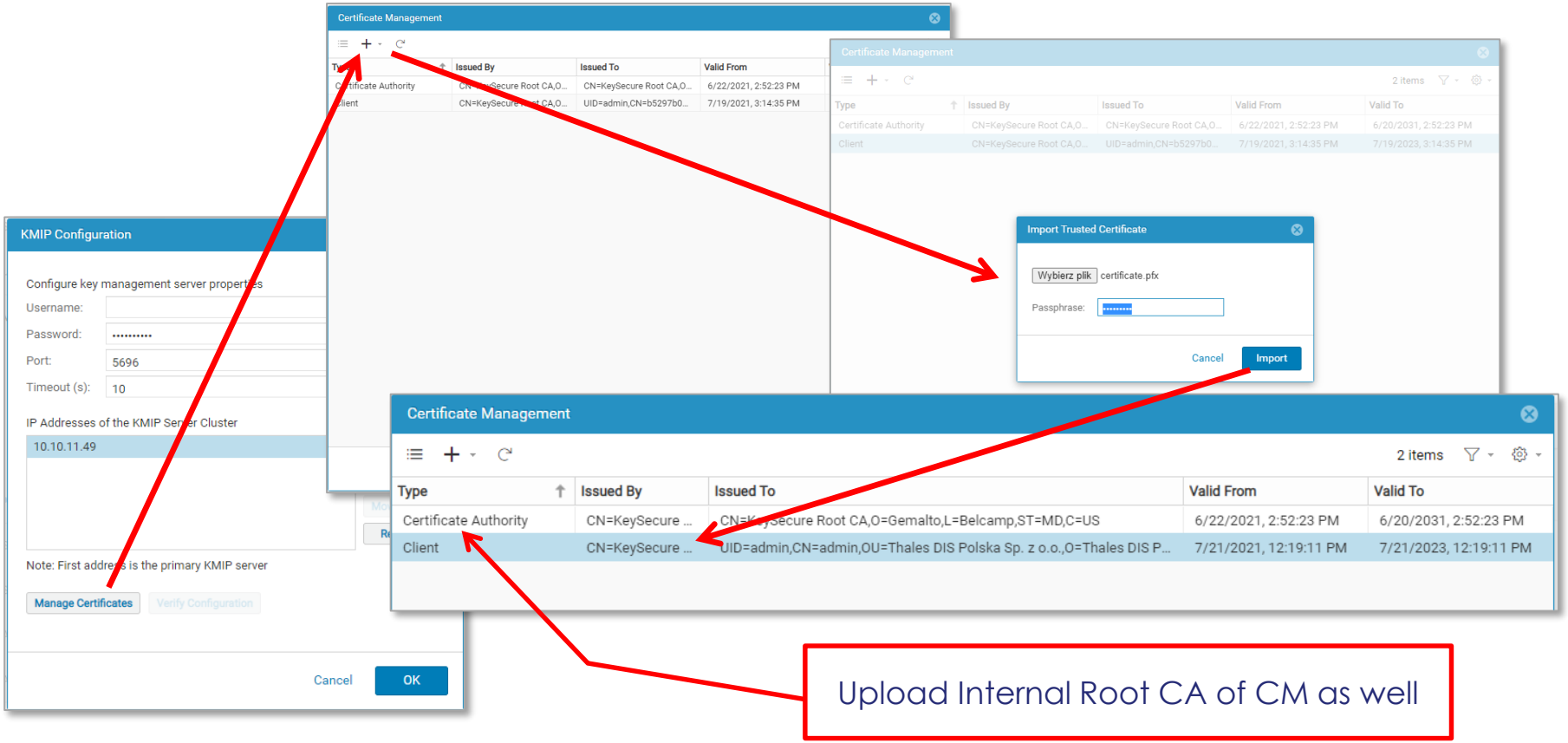
The username is taken from CN of Client Certificate (in our case: **admin**)

Provide CM **admin** password

Add IP of first CM (.49)

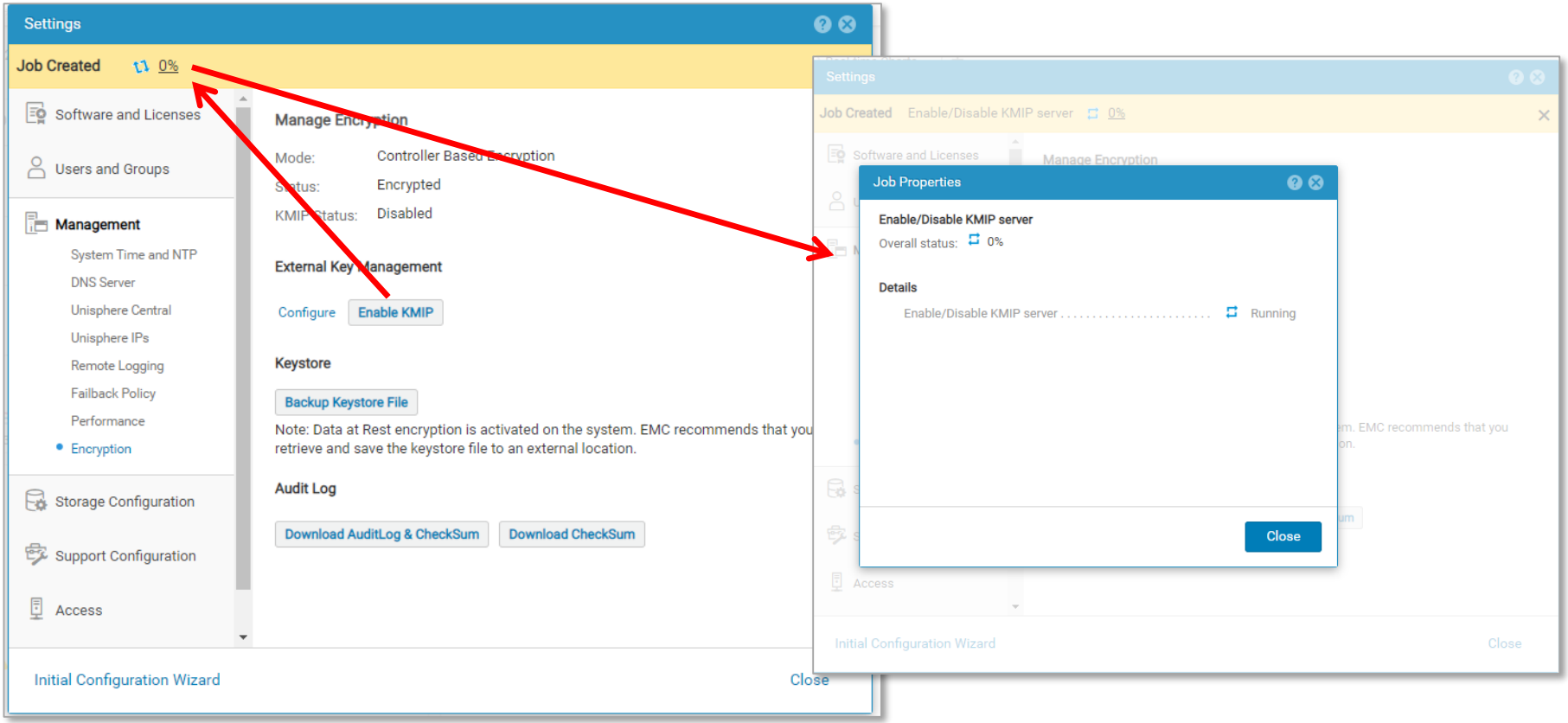
Manage client certificates…

Unity: Manager Client Certificates

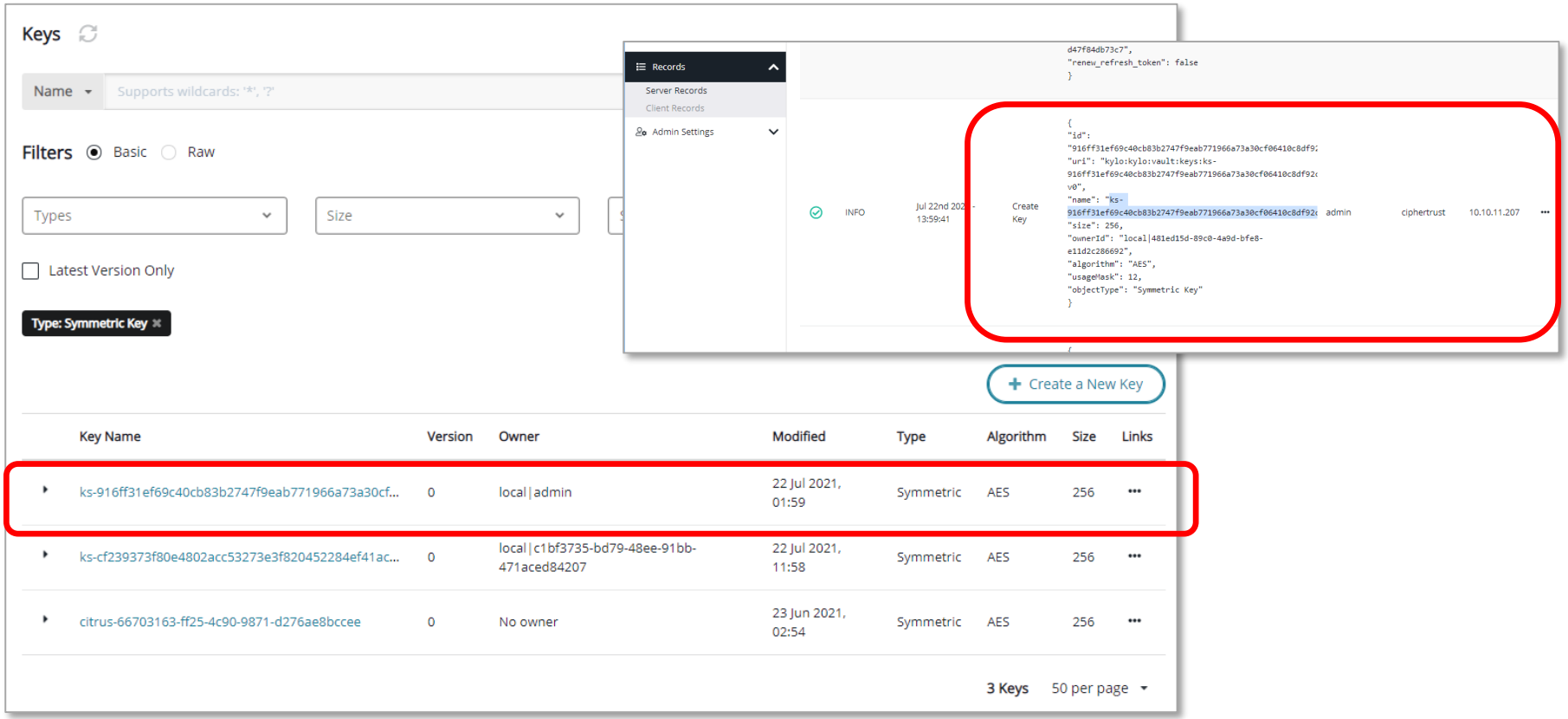


Upload Internal Root CA of CM as well

Unity: Ready to enable KMIP



Done. If all went well Unity creates keys in CM



Done. If all went well Unity encrypts drives

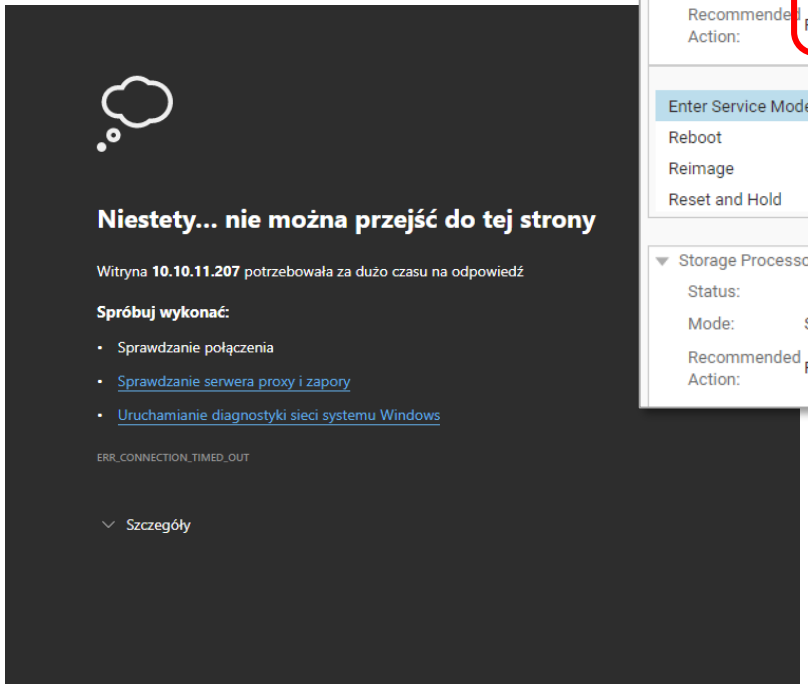
CKM00200900601_2021_07_21_09_01_00_0000000000000001_000000000000002C_full.log — Notatnik

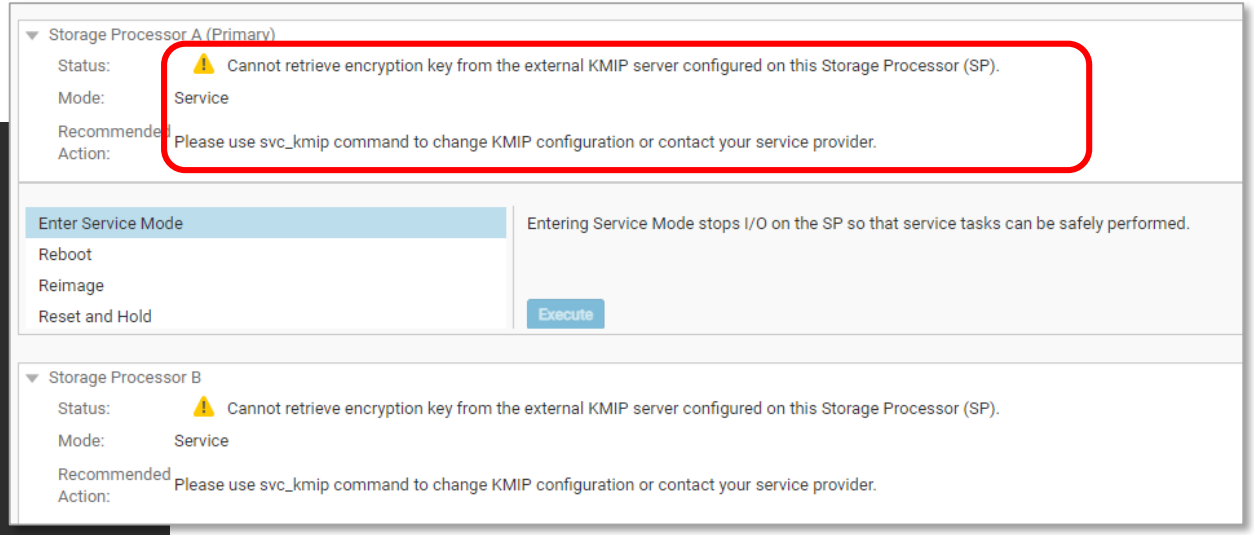
Plik Edycja Format Widok Pomoc

```
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 000000000000000F RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 0 DRIVE ZVNA0M701996
2021-07-15 09:35:09 0000000000000010 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 1 DRIVE ZVNA0M702189
2021-07-15 09:35:09 0000000000000013 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 2 DRIVE ZVNA0M702162
2021-07-15 09:35:09 0000000000000014 RG_ENCRYPTION_COMPLETED OBJ_ID 11 RG_ID 1004 POS 3 DRIVE ZVNA0M702195
2021-07-15 09:35:10 0000000000000015 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 0 DRIVE ZVNA0M701996
2021-07-15 09:35:10 0000000000000016 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 1 DRIVE ZVNA0M702189
2021-07-15 09:35:10 0000000000000017 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 2 DRIVE ZVNA0M702162
2021-07-15 09:35:10 0000000000000018 RG_ENCRYPTION_FINALIZED OBJ_ID 11 RG_ID 1004 POS 3 DRIVE ZVNA0M702195
2021-07-15 09:42:52 0000000000000019 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 0 DRIVE ZVNA0M702235
2021-07-15 09:42:52 000000000000001A CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 1 DRIVE ZVNA0M701812
2021-07-15 09:42:52 000000000000001B CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 2 DRIVE ZVNA0M702013
2021-07-15 09:42:52 000000000000001C CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 3 DRIVE ZVNA0M702070
2021-07-15 09:42:52 000000000000001D CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 4 DRIVE ZVNA0M702230
2021-07-15 09:42:52 000000000000001E CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 5 DRIVE ZVNA0M702232
2021-07-15 09:42:52 000000000000001F CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 6 DRIVE ZVNA0M702162
2021-07-15 09:42:52 0000000000000020 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 7 DRIVE ZVNA0M702195
2021-07-15 09:42:52 0000000000000021 CREATE_RG_KEY OBJ_ID 106 RG_ID 0 POS 8 DRIVE ZVNA0M702189
2021-07-15 09:42:52 0000000000000022 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
```

Lin 23, kol 49 100% Windows (CRI

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

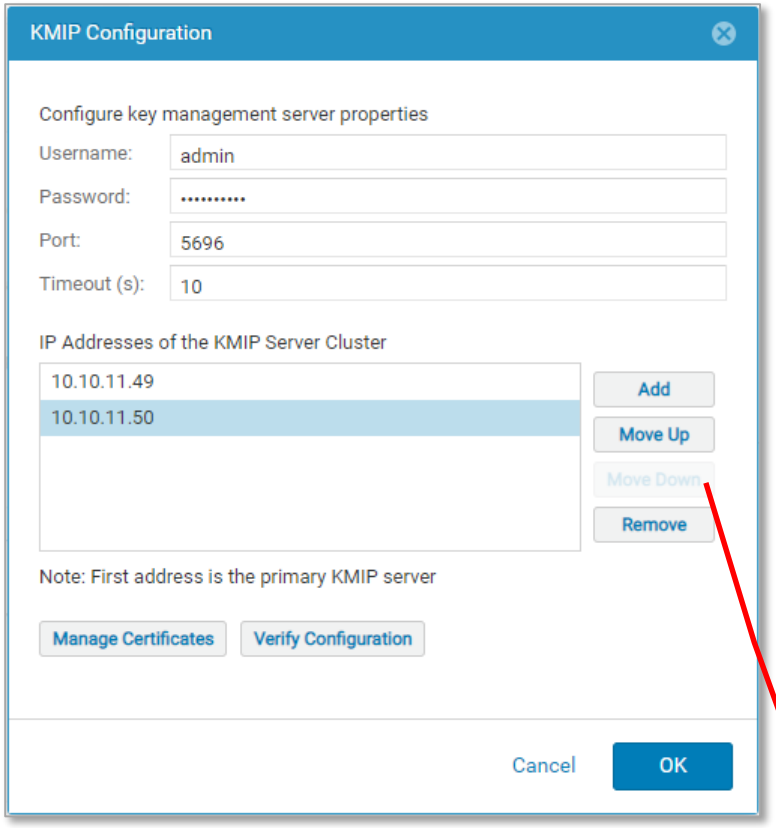




If they the KMIP Server is not accessible then:

- 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)

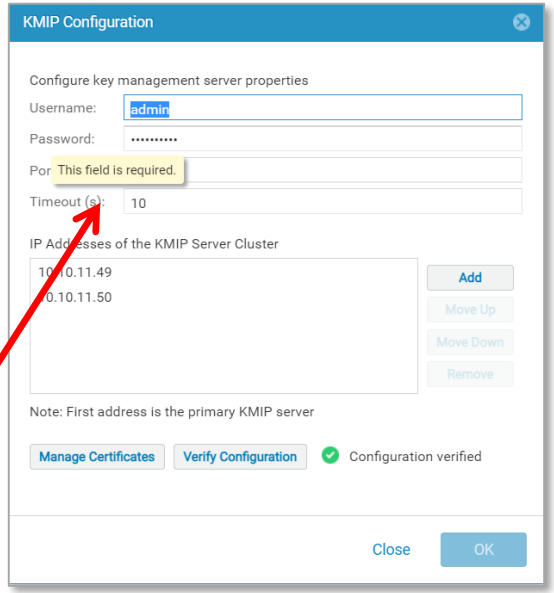
Adding second KMIP Server (CM) to Unity



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.

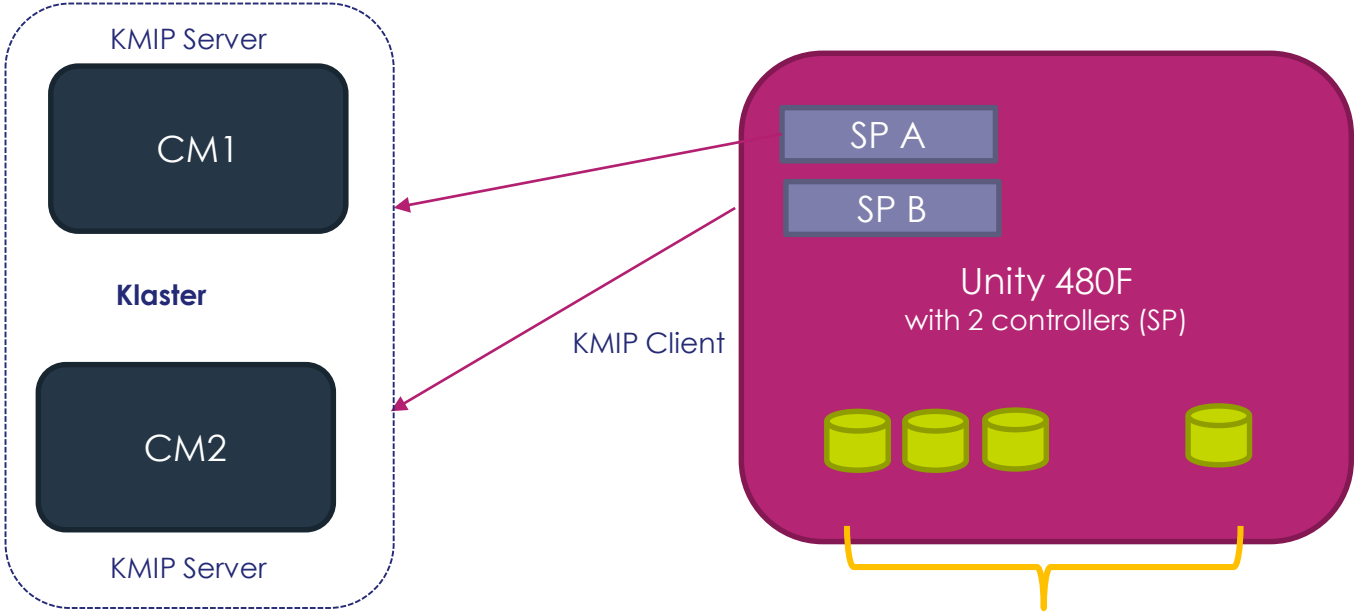
Be sure that dialog is filled up with proper data for each node. Don't belive in what is prompted.



Conslusion

- 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

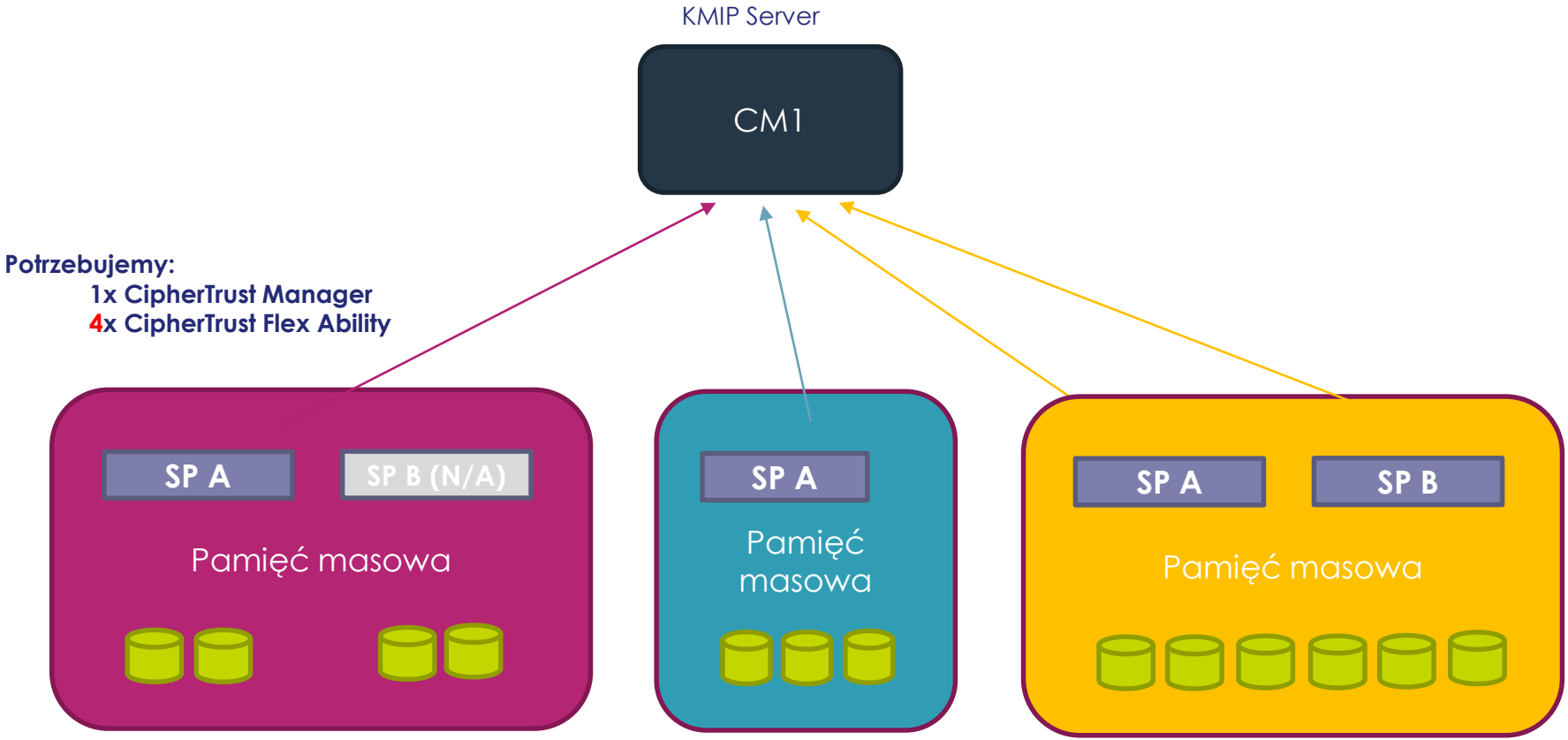


Potrzebujemy:
2x CipherTrust Manager
2x CipherTrust Flex Ability

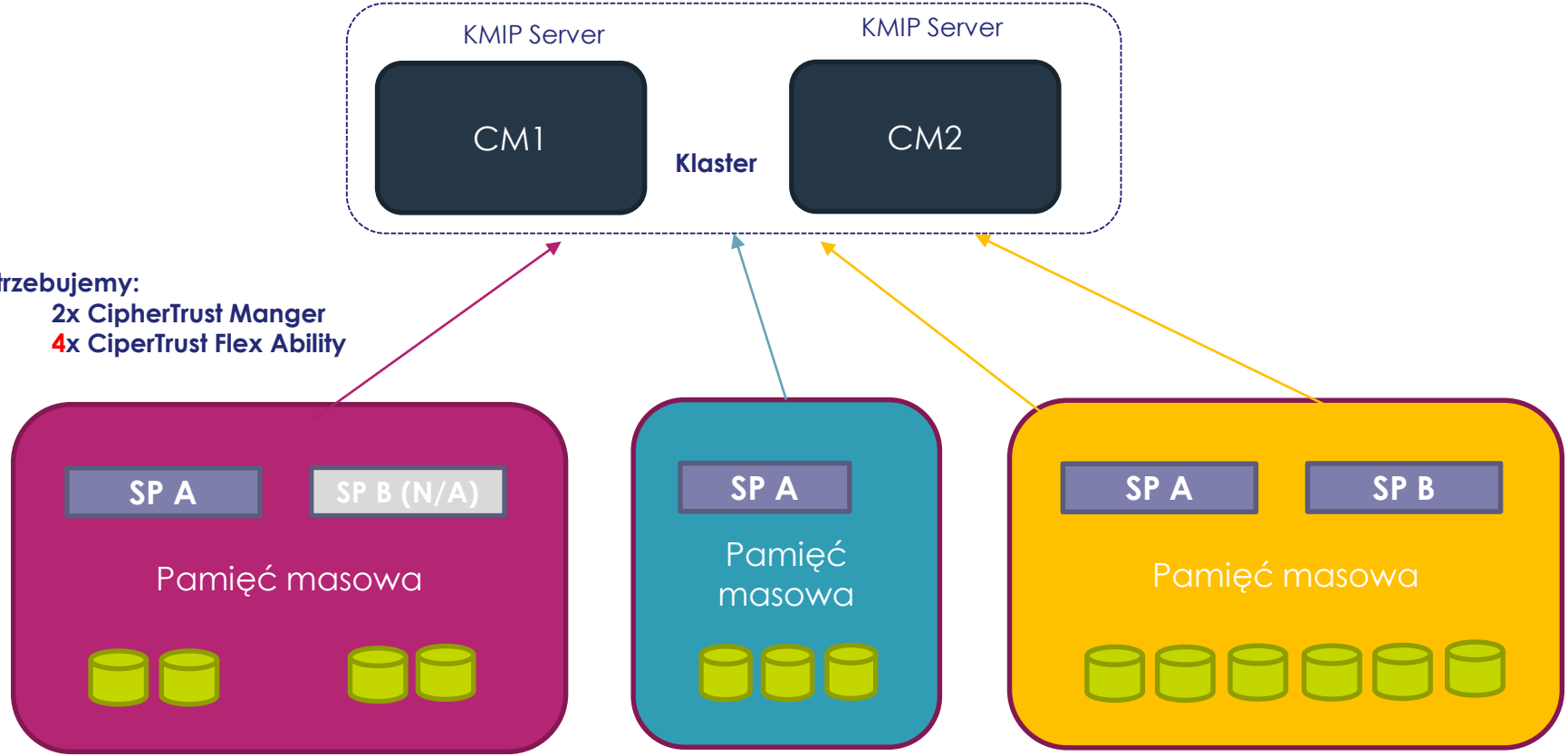
CipherTrust Flex Ability Connectors (KMIP)
CipherTrust Flex Ability,Perpetual
CipherTrust Flex Ability,Term Based, Enhanced Support
CipherTrust Flex Ability,Perpetual, Non-Prod
CipherTrust Flex Ability,Term Based, Enhanced Support, Non-Prod

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

A co z licencjonowaniem? #2



A co z licencjonowaniem? #3

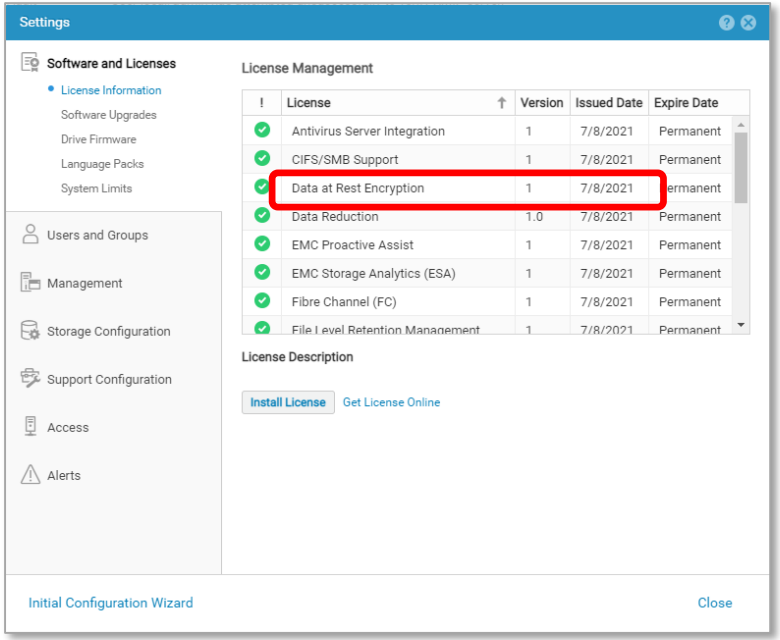


Nauczki, czyli *lessons learned #1/2*

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

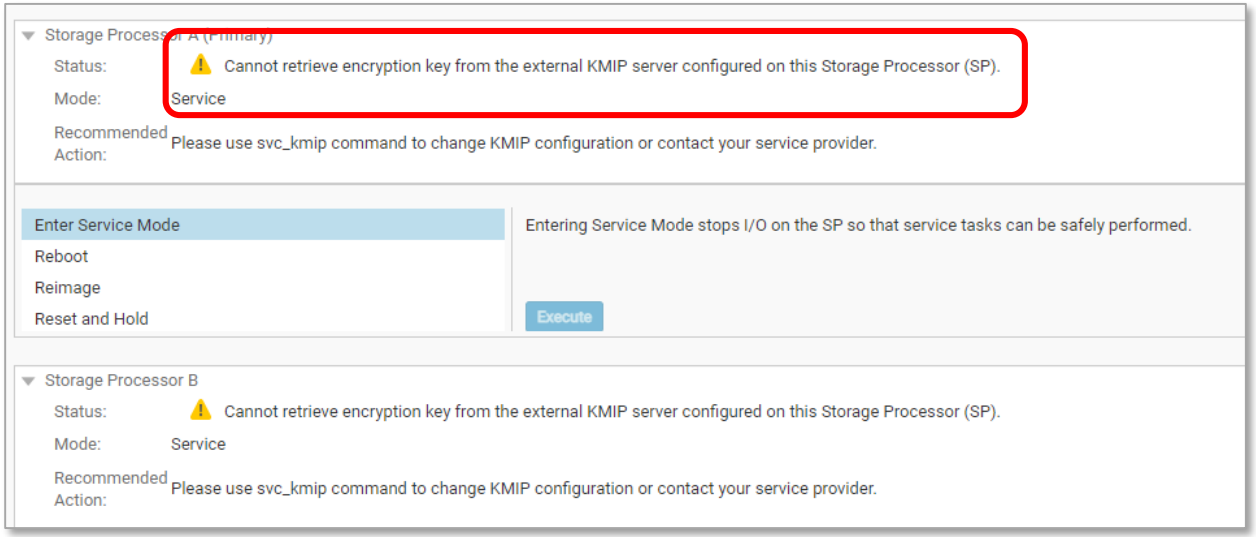
- Za darmo z nabyciem nowej DELL!

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



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 ☺



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…"*

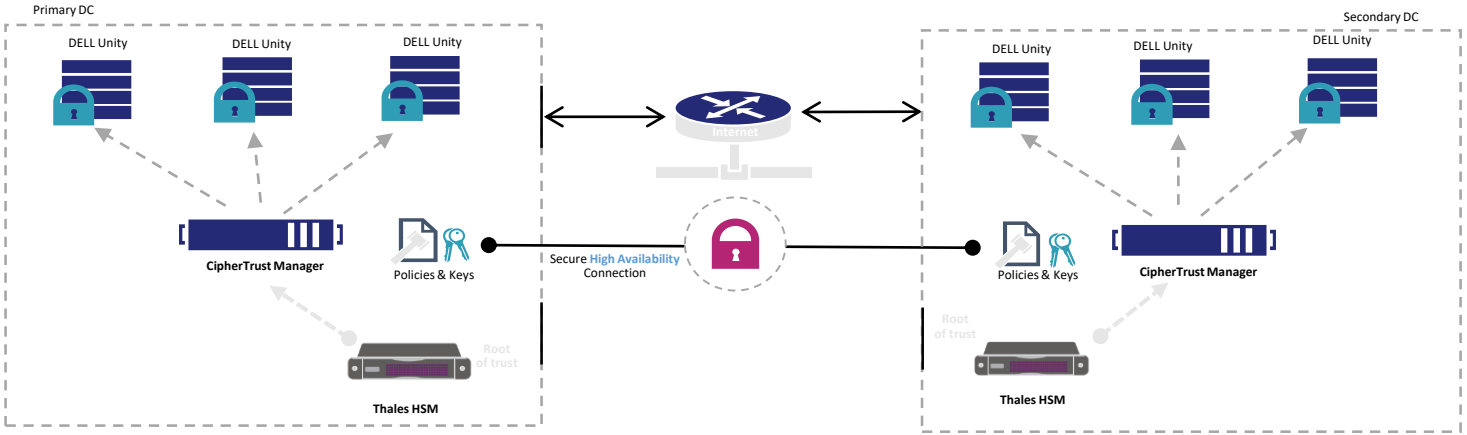
Agree with .... kmip client logic is fuzzy..

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