

CryptoPanel

edycja #23

Już za moment
zaczynamy...



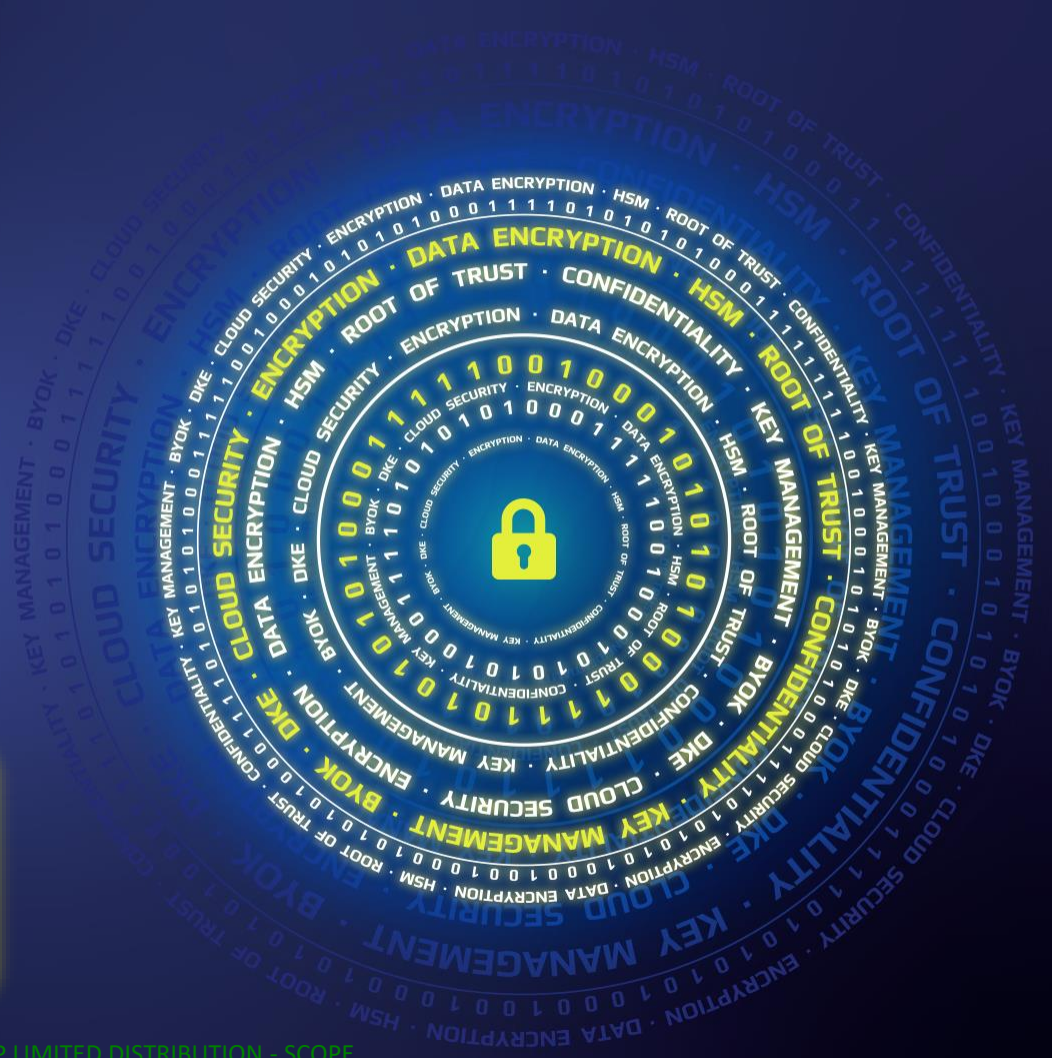
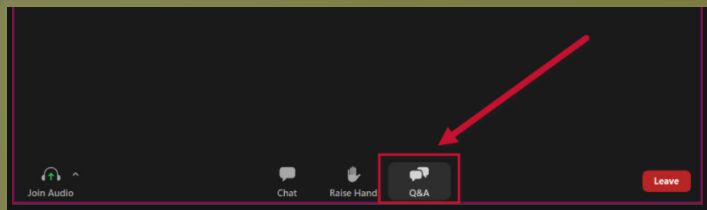
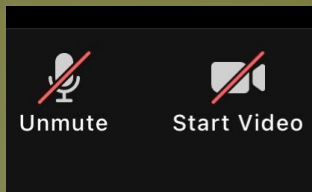
CryptoPanel



THALES



CryptoPanel



CryptoPanel

edycja #23

Jak zabrać się za backup zaszyfrowanych danych?
A może lepiej zaszyfrować backup danych? Jaka
strategię wybrać?



CryptoPanel

dziś dyskutują



Joanna Rzepka

Channel Sales Manager

Joanna.rzepka@thalesgroup.com

mob. +48 600 537 666



Jarosław Ulczok

Pre-sales Consultant

Jaroslaw.Ulczok@thalesgroup.com

mob. +48 603 056 667



CryptoPanel

wakacje przed nami!



Joanna Rzepka

Channel Sales Manager

Joanna.rzepka@thalesgroup.com

mob. +48 600 537 666

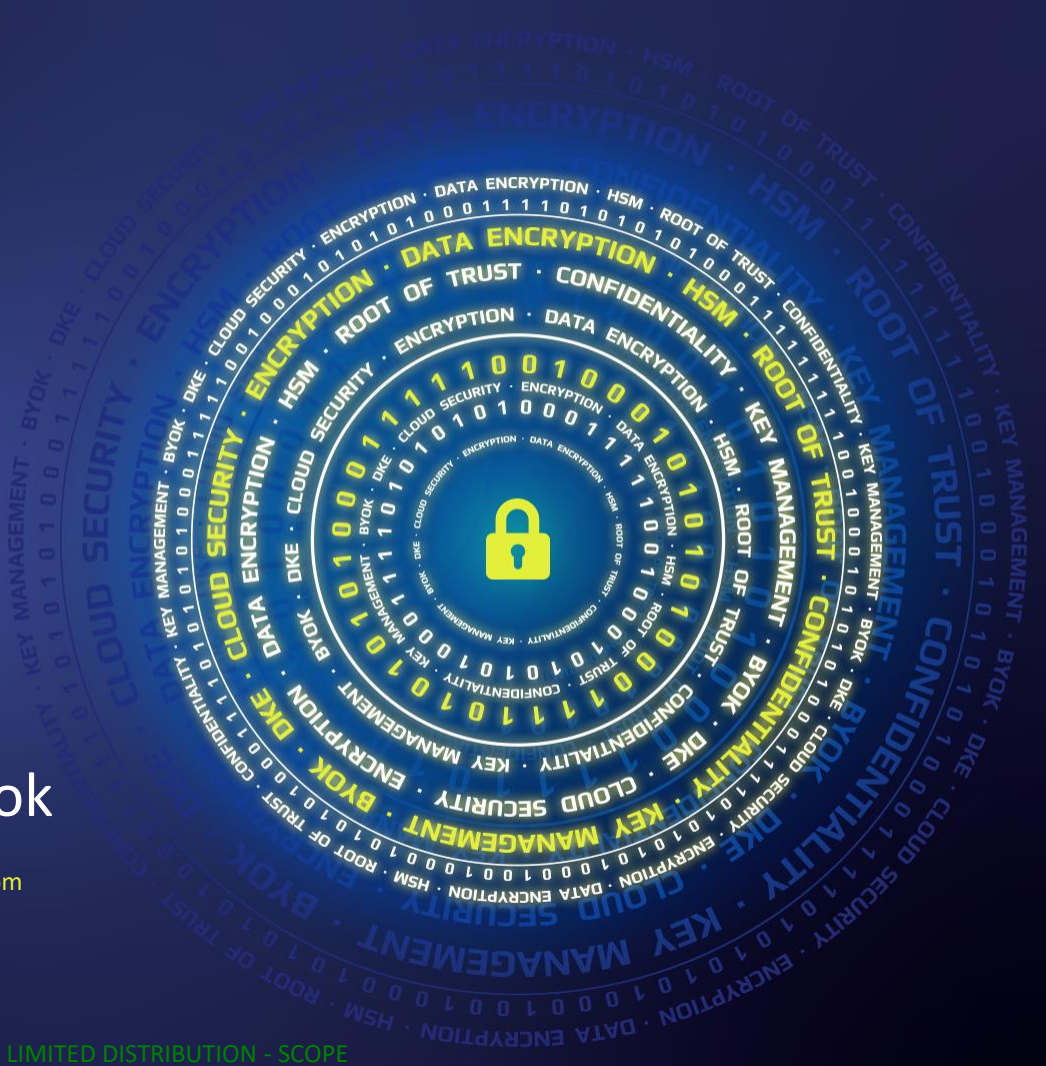


Jarosław Ulczok

Pre-sales Consultant

Jaroslaw.Ulczok@thalesgroup.com

mob. +48 603 056 667



CryptoPanel



problem



- ...jaką strategię ochrony backupu wybrać?
- ...czy szyfrować backup danych czy backupować dane zaszyfrowane?
- .. jakie konsekwencje rodzi każde z podejść?
- ...jakie zmiany w procedurach operacyjnych należy wprowadzić (np. odtwarzanie czy DR)?
- ...

CryptoPanel



rozwiązanie



BACKUP aka „kopia zapasowa”

Backup chroni przed utratą danych

- zapewnia ciągłości działania
- to „coś innego” niż HA
- daje zgodności z przepisami i regulacjami

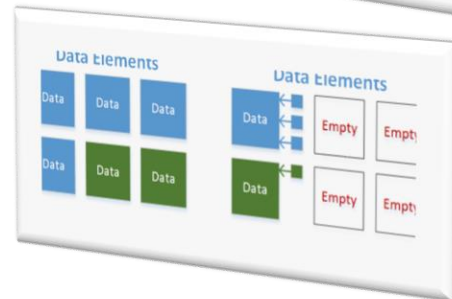
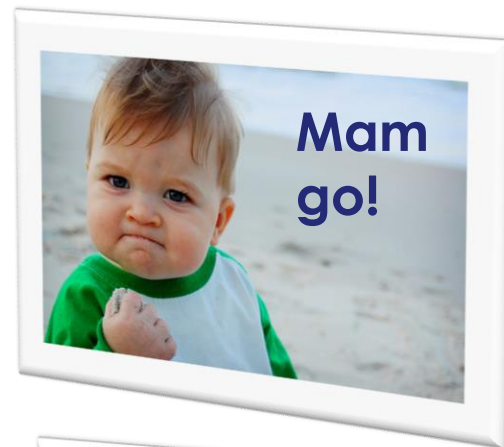
Backup mamy tylko wtedy gdy możemy go odtworzyć

- Kiedy ostatnio odtwarzałeś swój backup? Czy wciąż możesz to zrobić?

Backup zawiera nasze dane i jako taki sam wymaga ochrony

- Każdy z nich: główny, przyrostowy, tymczasowy, długoterminowy...
- Kopia czy archiwum to też backup i vice versa !

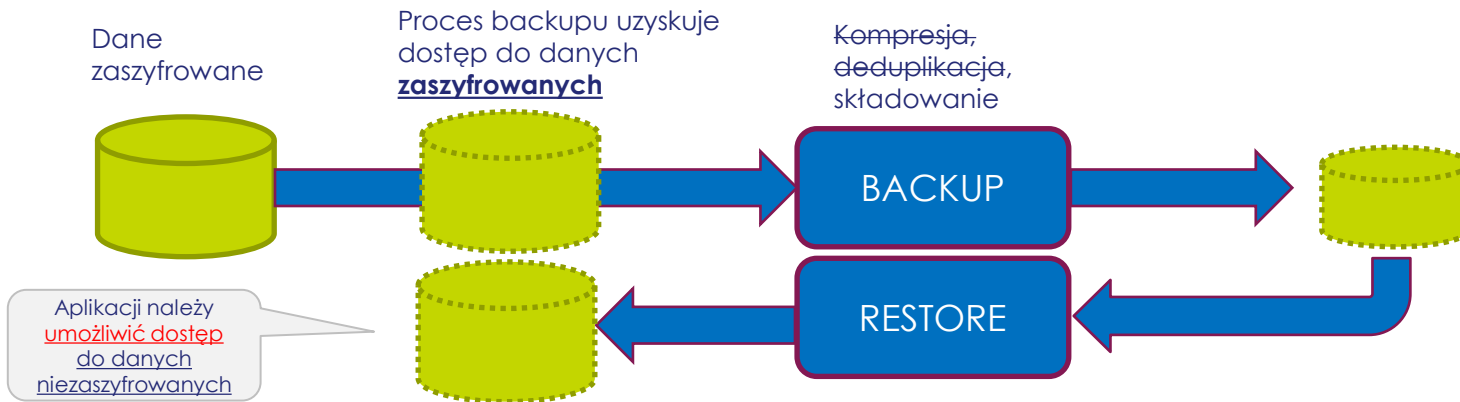
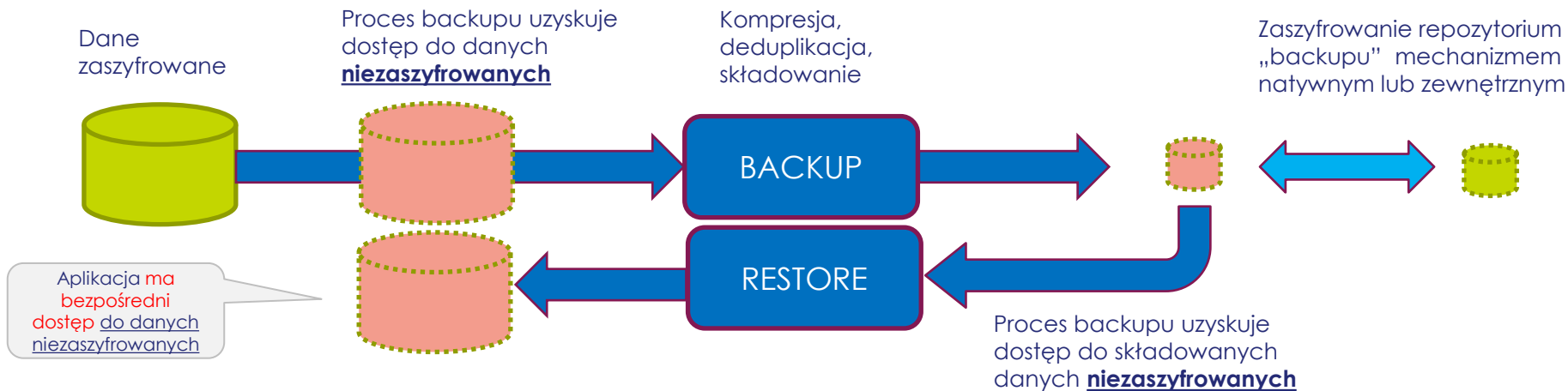
Backup wykorzystuje kompresję i deduplikację



Jak podejść do backupu danych zaszyfrowanych

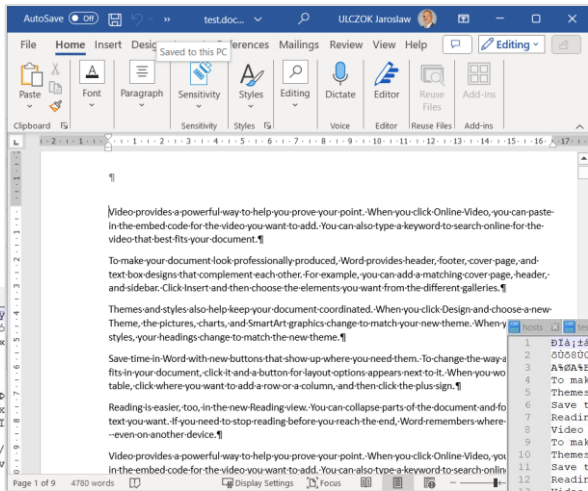


BACKUP a szyfrowane dane



Szyfrowanie vs kompresja i deduplikacja

Szyfrowanie
wbudowane w
Word 97/2003



Video provides a powerful way to help you prove your point. When you click Online Video, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document. ¶

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click **Insert** and then choose the elements you want from the different galleries. ¶

Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you change styles, your headings change to match the new theme.

Save time in Word with new buttons that show up where you need them. To change the way a fits in your document, click it and a button for layout options appears next to it. When you work with a table, click where you want to add a row or a column, and then click the plus sign. ¶

Reading is easier, too, in the new Reading view. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off—even on another device. ¶

Video provides a powerful way to help you prove your point. When you click Online Video, you can search for a video to add to your presentation. You can also type a keyword to search online for a video you want to add. You can also type a keyword to search online for a video you want to add.

[illegible]

Szyfrowanie vs kompresja i deduplikacja

Szyfrowanie
wbudowane w
Word 97/2003

Name	Date modified	Type	Size
test_enc.zip	25.06.2024 09:18	zip Archive	43 KB
test_enc.doc	25.06.2024 09:14	Microsoft Word 97...	57 KB
test.zip	25.06.2024 09:16	zip Archive	10 KB
test.doc	25.06.2024 09:13	Microsoft Word 97...	53 KB

As compression and encryption algorithms usually produce high-entropy data, any file with an entropy greater than **7.0 is likely compressed, encrypted, or packed** (in the case of executables).

<https://github.com/merces/entropy>

Command Prompt

```
C:\Work\Prezentacje\CryptoPanel\CP#23>entropy.exe test*.*
4.77 test.doc
7.96 test.zip
6.82 test_enc.doc
8.00 test_enc.zip

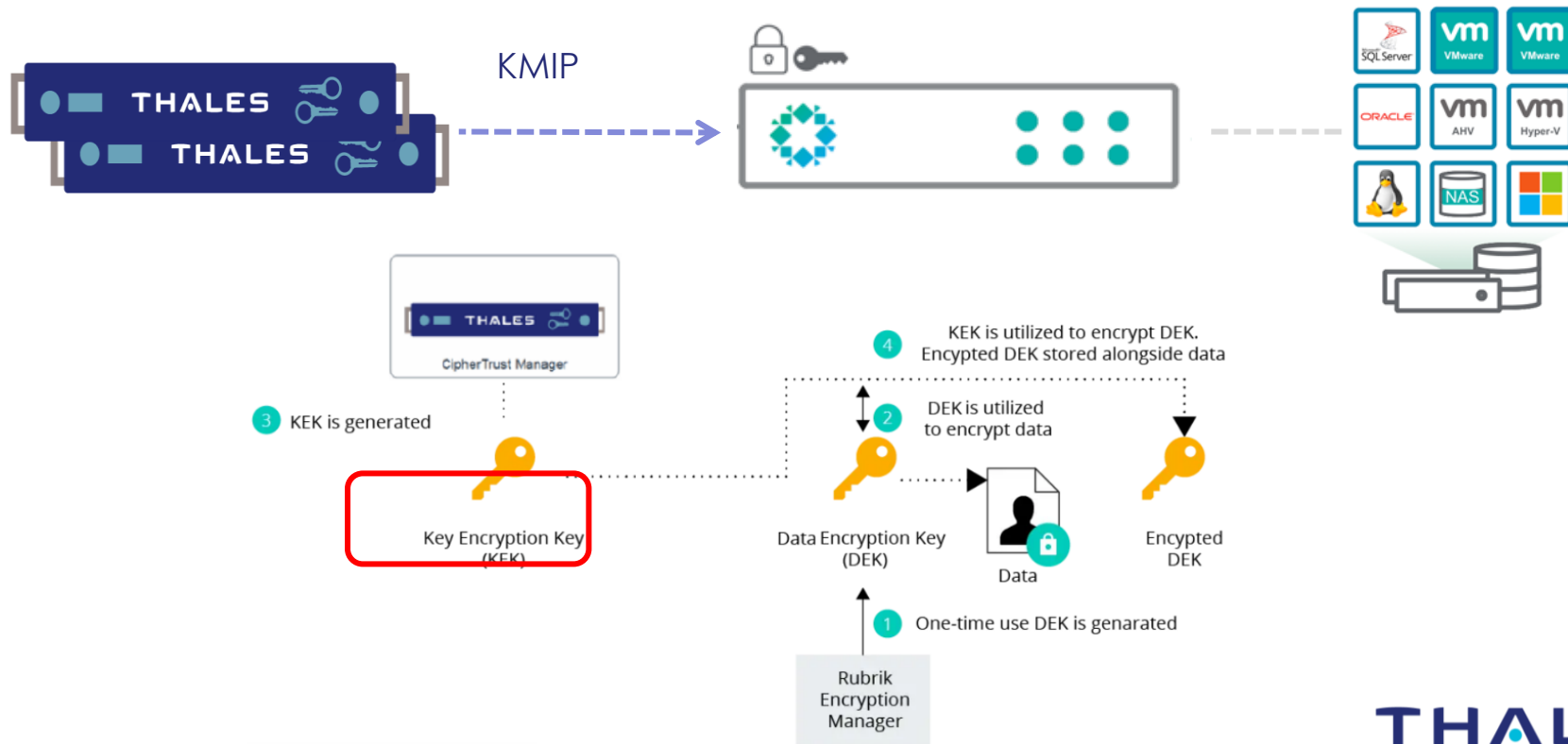
C:\Work\Prezentacje\CryptoPanel\CP#23>
```

Rozwiązanie:

Rubrik



Szyfrowany backupu w Rubrik



Integracja z Rubrik RSC

<https://thalesdocs.com/ctp/ig/rubrik/rubrik-cm/index.html>

The screenshot displays the Rubrik RSC Managed console interface. On the left is a dark sidebar with navigation links: Dashboards, Summary, Monitoring, Compliance, CDP Performance, Databases, System Performance, SLA Domains, Virtual Machines, Servers & Apps, Snapshot Management, Live Mounts, System, and Reports. The main content area has a top header with a search bar and 'RSC Managed' status. Below the header, there are tabs for 'Key Rotation Status' and 'KMIP Settings'. The 'KMIP Settings' tab is active, showing a large padlock icon and the title 'External Key Manager Configuration'. The text below the icon states: 'You must have either a signed client certificate or a client password to configure a KMIP-compliant external key manager for your Rubrik cluster.' It then lists two steps: 1. 'If you need to import a signed client certificate, please [Import Signed Certificate](#).' and 2. 'If you have a signed client certificate or a client password, please [Configure Client Settings](#).' A teal button labeled 'Configure Client Settings' is at the bottom. On the right, a dropdown menu is open, listing various configuration categories. The 'Manage Encryption' option under the 'Crypto Security' section is highlighted with a red rectangle.

Search by Object Search by Name or Location

RSC Managed

Admin User

Key Rotation Status KMIP Settings

Application Configuration

- vCenter Servers
- vCD Instances
- SCVMM Servers
- Nutanix Clusters
- Hosts
- Guest OS Settings

System Configuration

- Replication Targets
- Archival Locations
- Storage Arrays
- Adaptive Backup
- iSCSI Sources
- Certificate Management
- Cluster Settings

Crypto Security

Manage Encryption

Network Configuration

- Proxy Settings
- Network Settings
- Network Throttling
- Notification Settings

Access Management

- Two-Person Rule
- Users
- Organizations

Support

- Support Bundle
- Support Tunnel
- About Rubrik CDM

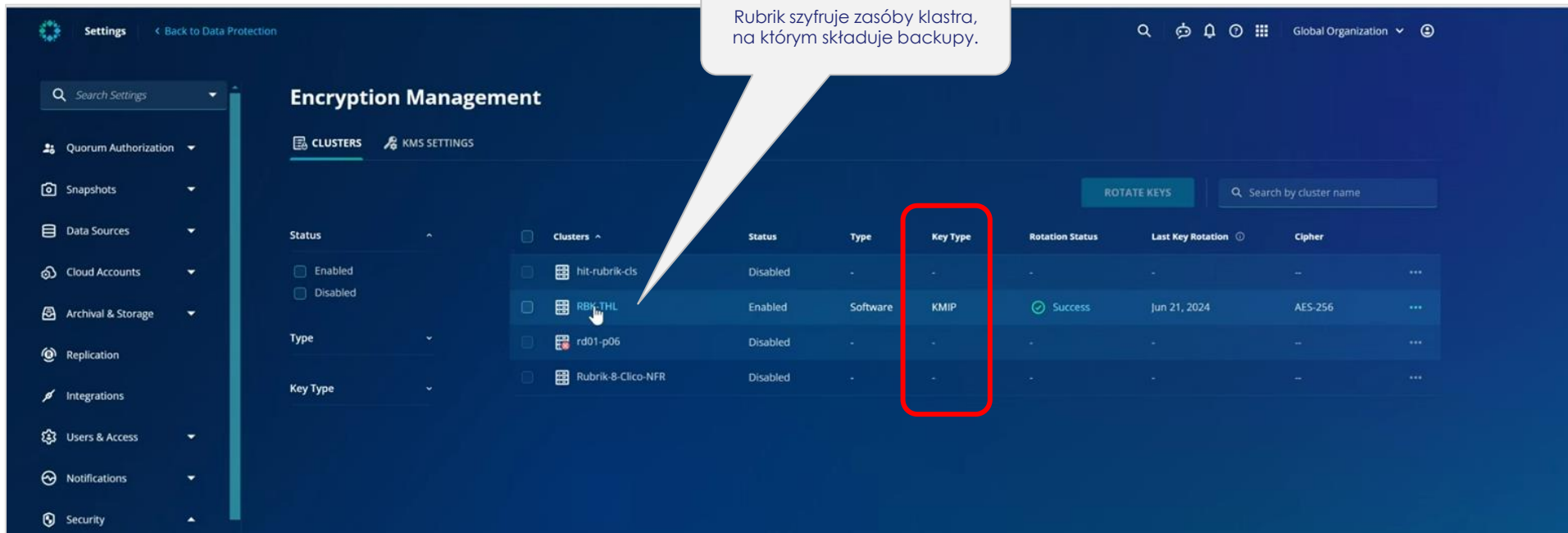
External Key Manager Configuration

You must have either a signed client certificate or a client password to configure a KMIP-compliant external key manager for your Rubrik cluster.

1. If you need to import a signed client certificate, please [Import Signed Certificate](#).
2. If you have a signed client certificate or a client password, please [Configure Client Settings](#).

[Configure Client Settings](#)

Integracja z Rubrik RSC



Settings Back to Data Protection

Encryption Management

CLUSTERS KMS SETTINGS

ROTATE KEYS Search by cluster name

Status	Clusters	Status	Type	Key Type	Rotation Status	Last Key Rotation	Cipher
☐ Enabled ☐ Disabled	☐ hit-rubrik-cl	Disabled	-	-	-	-	-
Type	☐ RBK-THL	Enabled	Software	KMIP	Success	Jun 21, 2024	AES-256
Key Type	☐ rd01-p06	Disabled	-	-	-	-	-
	☐ Rubrik-8-Clco-NFR	Disabled	-	-	-	-	-

Rubrik szyfruje zasoby klastra, na którym składuje backupy.

Integracja z Rubrik RSC

Settings

<

Back to Data Protection

Search Settings

Quorum Authorization

Snapshots

Data Sources

Cloud Accounts

Archival & Storage

Replication

Integrations

Encryption Management

CLUSTERS

KMS SETTINGS

ADD KMIP SERVER

Search by KMIP server

Rubrik Cluster

☐

hit-rubrik-cls

☐

RBK-THL

☐

rd01-p06

☐

Rubrik-8-Clcio-NFR

Server Address

Port

Clusters

10.10.11.233

5697

1

...

Cluster

Server Certificate

RBK-THL

CM_Local_CA

Settings

<

Back to Data Protection

Search Settings

Quorum Authorization

Snapshots

Data Sources

Cloud Accounts

Archival & Storage

Replication

Integrations

Encryption Management

CLUSTERS

KMS SETTINGS

All clusters > Rotation Status for RBK-THL

Search by node ID

Rotation Status for {clusterNa}

☐

Succeeded

☐

In progress

☐

Queued

Node ID

Rotation Status

Started On

Key Type

VRVW421C7ECB0

Succeeded

June 21, 2024 at 3:16 PM

KMIP

Integracja z Rubrik - aktywność po stronie CM – eksport KEK-a

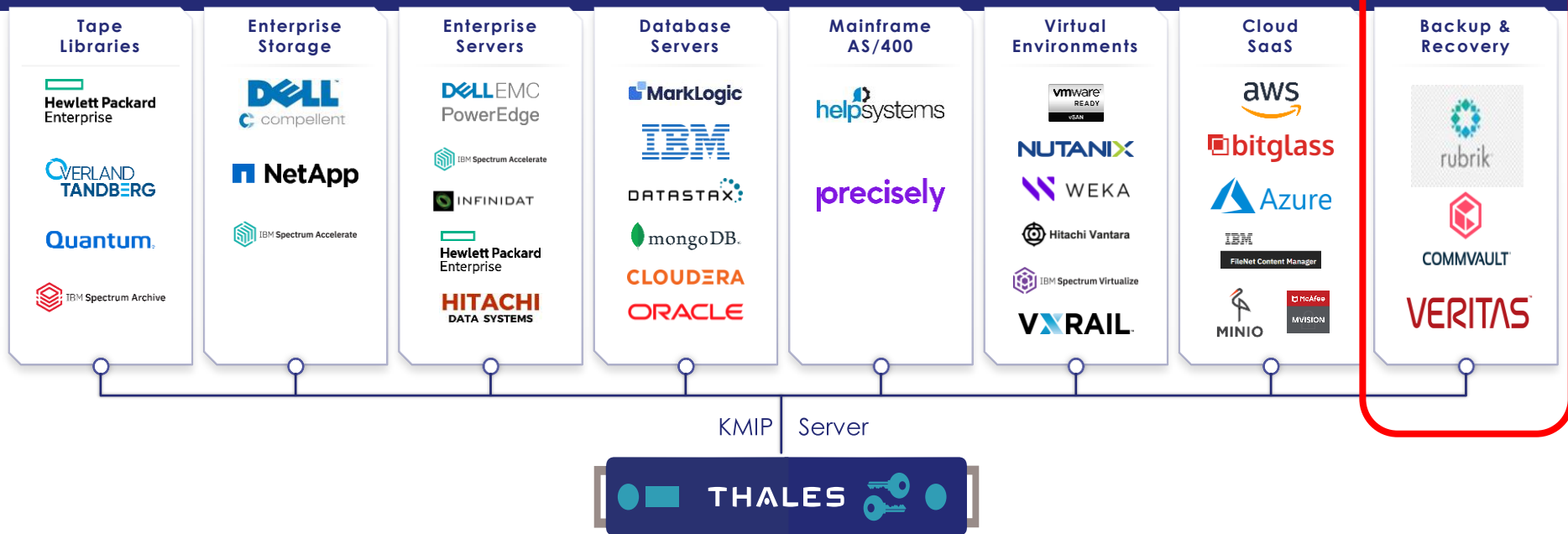
✓	INFO	Jun 23rd 2024 - 13:43:29	Revoke Refresh Token	<pre>{ "id": "6085944d-f21c-4c05-b914-56cc9d91d832", "user_id": "local 62bcfd59-42e7-477f-b49d-02a55e2b8b70", "username": "RubrikSrv9", "client_id": "0a8ff721-bad3-4e25-81df-4fe6d8b3a158", "connection": "local_account" }</pre>	RubrikSrv9	ciphertrust	...
---	------	--------------------------	----------------------	--	------------	-------------	-----

✓	INFO	Jun 23rd 2024 - 13:34:35	Export Key	<pre>{ "id": "668b2af6eb69417489258a87a80c571afc54a94d492b492a8bb253ee43342687" }</pre>	RubrikSrv9	ciphertrust	10.10.11.236	...
---	------	--------------------------	------------	---	------------	-------------	--------------	-----

✓	INFO	Jun 23rd 2024 - 13:34:06	Create Token	<pre>{ "label": ["nae-auth"], "domain": "", "user_id": "local 62bcfd59-42e7-477f-b49d-02a55e2b8b70", "username": "RubrikSrv9", "client_id": "0a8ff721-bad3-4e25-81df-4fe6d8b3a158", "domain_id": "", "connection": "local_account", "grant_type": "user_impersonation", "auth_domain": "", "client_name": "AutoClient-dbe89327edd974de", "client_type": "confidential", "refresh_token_id": "6085944d-f21c-4c05-b914-56cc9d91d832", "renew_refresh_token": false, "refresh_token_counts": { "total": 1, "labels": { "nae-auth": 1 } }, "no_label": 0 }</pre>	RubrikSrv9	ciphertrust	10.10.11.236	...
---	------	--------------------------	--------------	--	------------	-------------	--------------	-----

Integracje z wykorzystaniem KMIP

CipherTrust Manager współpracuje z szeroką gamą środowisk przechowywania danych, chmur i środowisk wirtualnych przy użyciu protokołu interoperacyjności zarządzania kluczami (KMIP)



CipherTrust Manager

Key Management and Access Control Policies

THALES GROUP LIMITED DISTRIBUTION - SCOPE

THALES

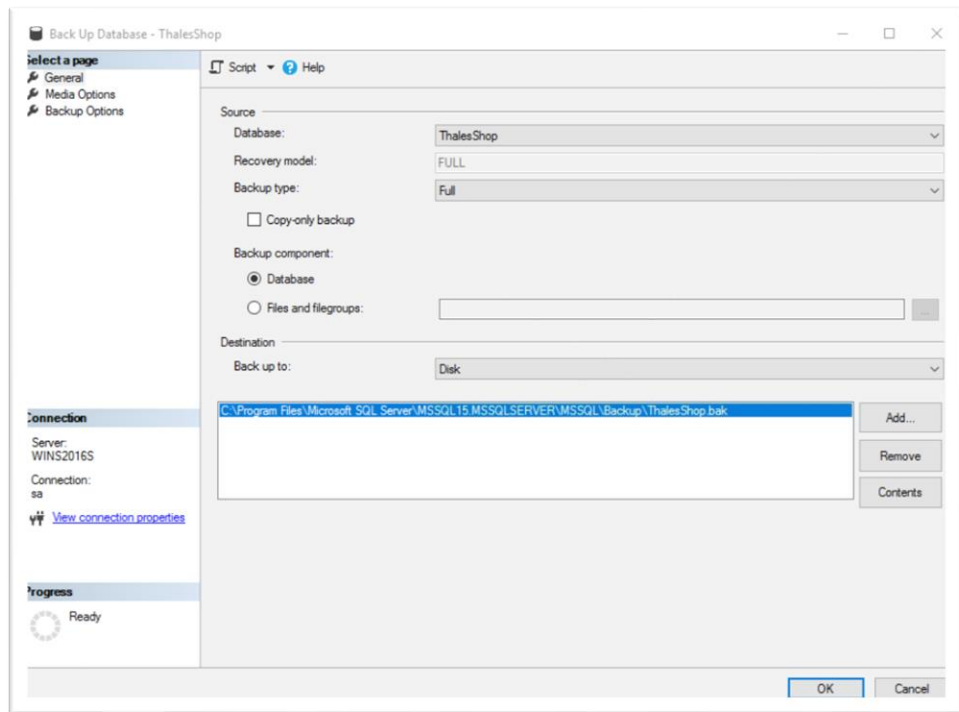
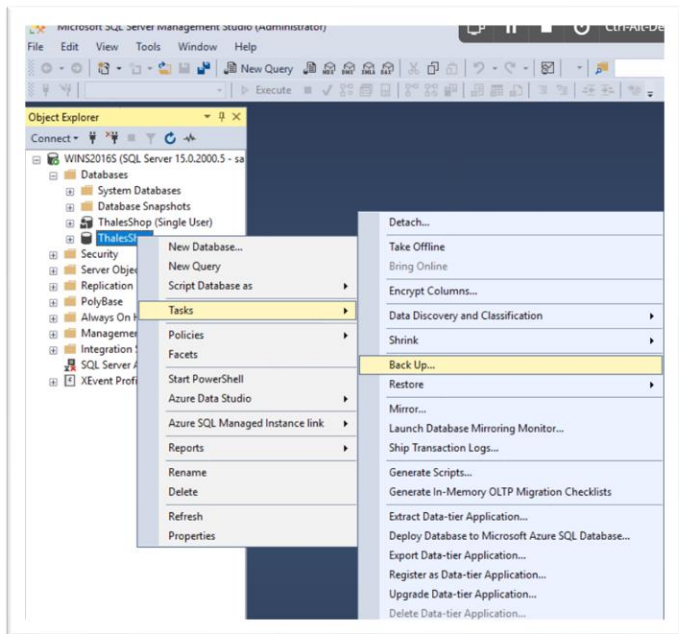
Rozwiązanie:

MS SQL Server i CTE

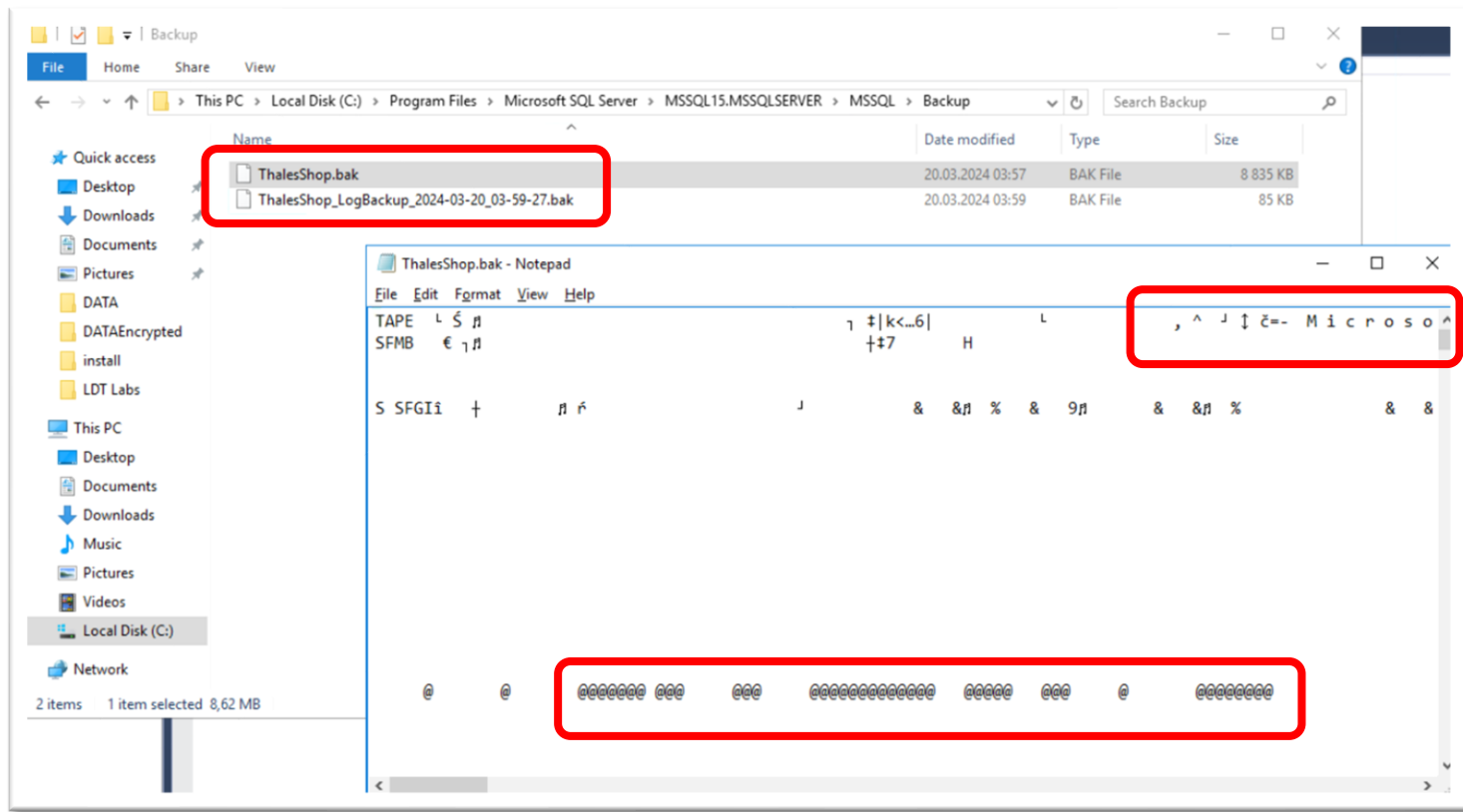


MS SQL – Back Up/Restore

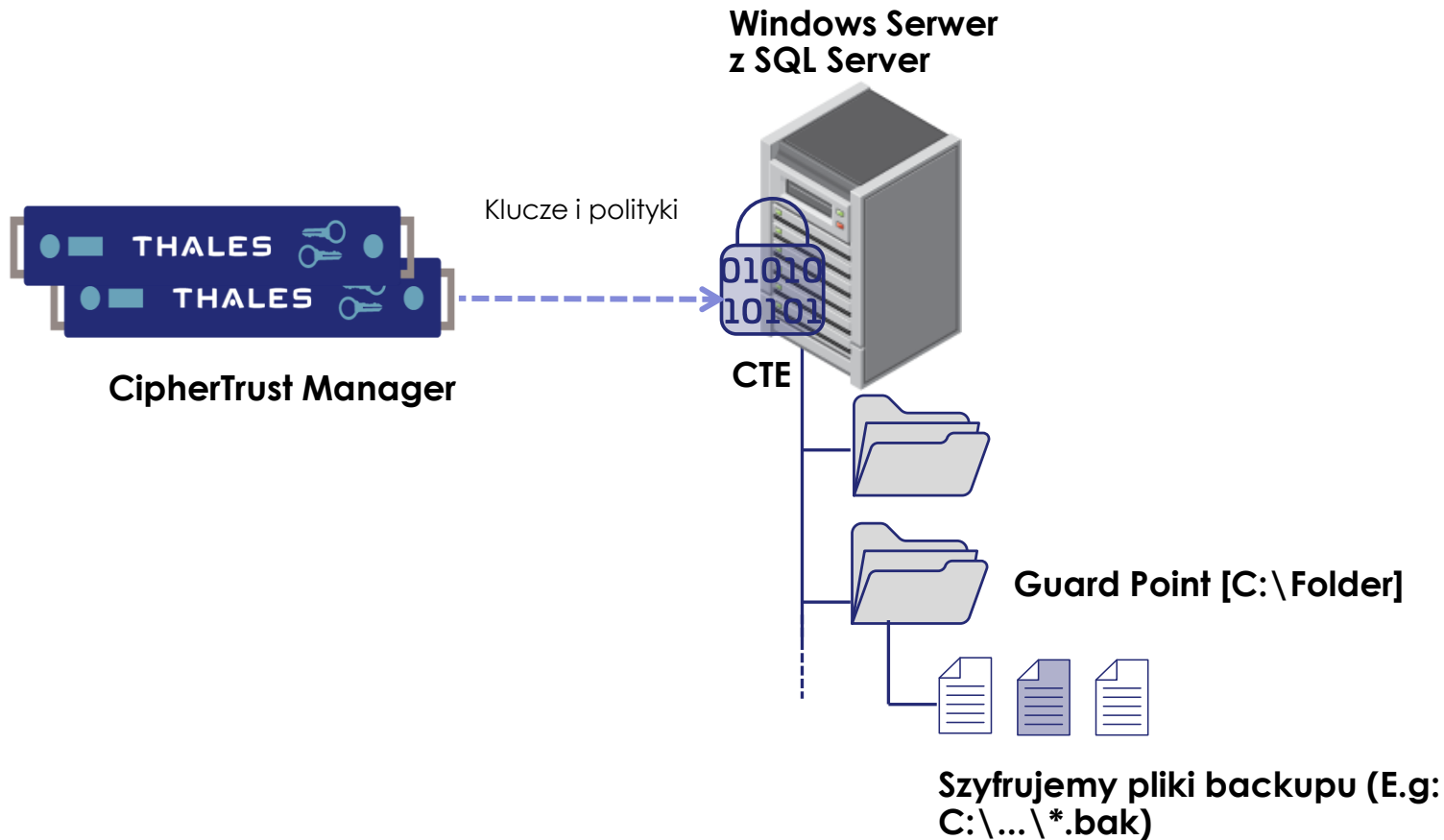
Mechanizm backupu musi mieć dostęp do danych niezaszyfrowanych



Backup bazy domyślnie jest **niezaszyfrowany**



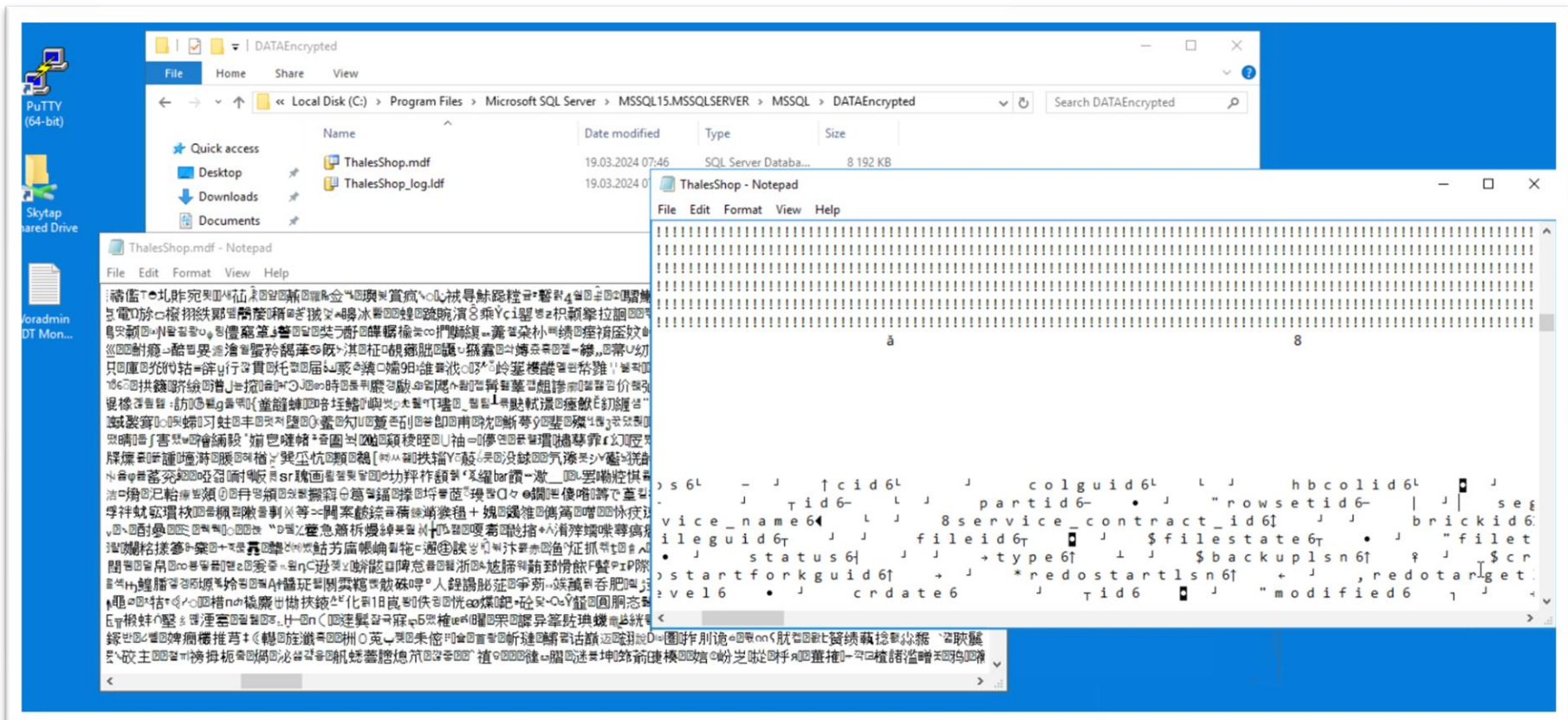
CTE dla ochrony plików baz danych i ich backupów



Polityka CTE, pozwala na dostęp do zaszyfrowanego backupu

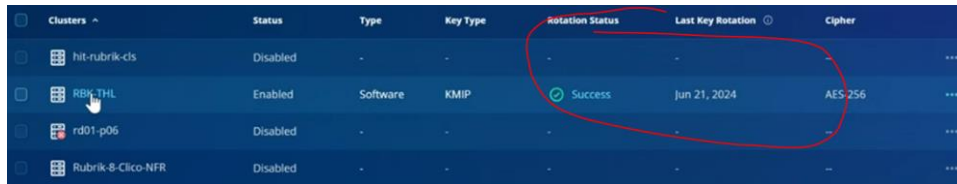
SQL_LDT							
Restrict Update: ☐ Learn Mode: ☐							
ApplyKey effect for Deny rules.. Remove							
Security Rules Key Rules							
0 Selected 5 results 5 Security Rules ⌵ ⌴ ⌶ ⌷ + Add Security Rule							
Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	⚙
▶ 1				key_op	permit,applykey	No	
▶ ☐ 2		SQL_DBAdmin		all_ops	permit,audit,applykey	Yes	...
▶ ☐ 3			SQLSERVER	all_ops	permit,audit,applykey	Yes	...
▶ ☐ 4		Serv_Admin		read,f_i	permit,audit	Yes	...
▶ ☐ 5				all_ops	deny,audit	Yes	...
5 Security Rules 10 per page ▾							

Dostęp do pliku kontrolowany przez CTE



Nauczki...

- Przed wdrożeniem upewnij się czy rozwiązanie backupu (tu:Rubrik) i CM posiada odpowiednią licencję i zasoby do wdrożenia szyfrowania.
- Rubrik (v9.1.x) w integracji KMIP nie obsługuje kluczy ECC, na razie tylko RSA 2K+.
- Po udanej integracji Rubrik-CipherTrust zrotuj klucz!



Clusters	Status	Type	Key Type	Rotation Status	Last Key Rotation	Cipher
hit-rubrik-cls	Disabled	-	-	-	-	---
RBK-THL	Enabled	Software	KMIP	Success	Jun 21, 2024	AES-256
rd01-p06	Disabled	-	-	-	-	---
Rubrik-S-Clico-NFR	Disabled	-	-	-	-	---

- Zawsze sprawdzaj aktualną dokumentację, podręcznik integracji może być leciwy.



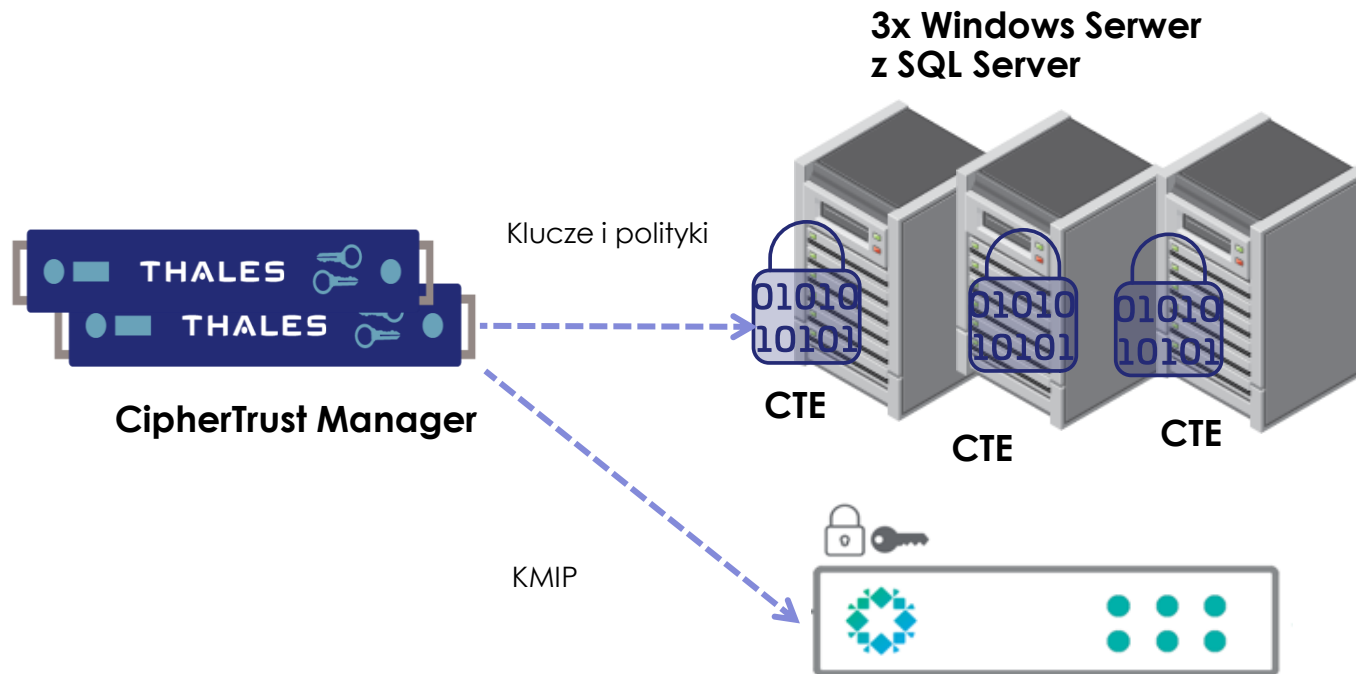
CryptoPanel



podsumowanie



Architektura rozwiązania



Podsumowanie, czyli co potrzeba... (ceny SRP, netto w €)

- 2x CM
- 3x CTE
- 1x KMIP
- ...jako abonament na rok z opieką:

2x Virtual CipherTrust Manager,k170v, Term Based , Enhanced Support	6 520,00	976-000012-001-000
1x CipherTrust Flex Ability, Term Based , Enhanced Support	171,00	976-000010-001-000
3x CipherTrust Flex Connector - Basic, Term Based , Enhanced support	1 700,00	976-000002-001-000



CryptoPanel



CryptoPanel



A teraz quiz

