

## » Idź do

- Spis treści
- Przykładowy rozdział

## » Katalog książek

- Katalog online
- Zamów drukowany katalog

## » Twój koszyk

- Dodaj do koszyka

## » Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

## » Czytelnia

- Fragmenty książek online

## » Kontakt

Helion SA  
ul. Kościuszki 1c  
44-100 Gliwice  
tel. 032 230 98 63  
e-mail: helion@helion.pl  
© Helion 1991-2010

## Klastry pracy awaryjnej w środowisku Windows. Instalacja, konfiguracja i zarządzanie

Autor: Andrzej Szelaąg  
ISBN: 978-83-246-2609-0  
Format: 158×235, stron: 224



- Poznaj podstawy technologii klastrowej w oparciu o systemy firmy Microsoft
- Naucz się praktycznie wdrażać klastry pracy awaryjnej
- Dowiedz się, jak korzystać z zaawansowanych rozwiązań serwerowych

Zachowanie ciągłości procesów biznesowych dla wielu przedsiębiorstw stanowi jedną z najważniejszych kwestii, decydującą niejednokrotnie o ich istnieniu i powodzeniu na rynku w coraz bardziej zwirtualizowanym świecie. W firmach wymagających stałego dostępu do ważnych danych, usług lub aplikacji konieczne jest zapewnienie odpowiednich mechanizmów, gwarantujących ciągłość pracy systemów niezależnie od wszelkiego rodzaju awarii, które mogą czasami zdarzać się w bardziej rozbudowanej i skomplikowanej infrastrukturze informatycznej. Odpowiedzią na te potrzeby stała się technologia klastrowa, implementowana przez firmę Microsoft w jej serwerowych systemach operacyjnych.

Niestety, zagadnienia dotyczące technologii klastrowej i jej realizacji w środowiskach opartych na najnowszych serwerowych systemach operacyjnych firmy Microsoft nie należą do najprostszych w informatycznym świecie. Wszyscy zainteresowani mają też z pewnością świadomość tego, jak ważna w karierze każdego specjalisty IT może okazać się znajomość tej tematyki. To właśnie z myślą o takich osobach powstała książka "Klastry pracy awaryjnej w środowisku Windows. Instalacja, konfiguracja i zarządzanie". Informatycy, studenci kierunków informatycznych i amatorzy pragnący dowiedzieć się więcej na temat technologii klastrowej dostępnej w najbardziej zaawansowanych technologicznie serwerowych systemach operacyjnych z rodziny Windows Server 2008 R2 znajdą tu mnóstwo praktycznych informacji oraz poszerzą swoją wiedzę na temat klastrów pracy awaryjnej.

- Przegląd podstawowych pojęć i nowości związanych z technologią klastrową w środowisku opartym na systemach Windows Server 2008 R2
- Możliwości technologii klastrowej, oferowane przez systemy Windows Server 2008 R2
- Wdrażanie infrastruktury kluczy publicznych (PKI)
- Praktyczne przykłady wdrażania klastra pracy awaryjnej
- Konfigurowanie klastra pracy awaryjnej
- Zarządzanie klastrami pracy awaryjnej, infrastrukturą kluczy publicznych (PKI), rolami i funkcjami systemów Windows Server 2008 R2

**Poznaj od środka klastry pracy awaryjnej!  
Dołącz do najbardziej poszukiwanych na rynku specjalistów IT!**

# Spis treści

<b>Wstęp .....</b>	<b>7</b>
<b>Rozdział 1. Technologia klastrowa w systemach Windows Server 2008 R2 .....</b>	<b>13</b>
1.1. Czym jest klastrowa praca awaryjna? .....	14
1.2. Czym jest węzeł klastra praca awaryjna? .....	16
1.3. Jak działa klastrowa praca awaryjna i do czego można go wykorzystać? .....	17
1.4. Korzyści wynikające ze stosowania klastrów praca awaryjna .....	18
1.4.1. Wyższa dostępność .....	19
1.4.2. Lepsza skalowalność .....	20
1.4.3. Prostsze zarządzanie .....	20
1.5. Zmiany w klastrach praca awaryjna w systemach Windows Server 2008 R2 .....	20
1.5.1. Uproszczenie procesu instalacji .....	21
1.5.2. Udoskonalenia procesu konfiguracji .....	22
1.5.3. Zmiany i udoskonalenia interfejsów zarządzania .....	22
1.5.4. Ulepszenia sposobu współpracy klastra z magazynem .....	24
1.5.5. Udoskonalenia komunikacji sieciowej .....	26
1.5.6. Ulepszenia zabezpieczeń .....	27
<b>Rozdział 2. Klastrowa praca awaryjna w środowisku Windows Server 2008 R2 .....</b>	<b>29</b>
2.1. Informacje o środowisku klastra praca awaryjna .....	30
2.2. Przygotowanie do wdrożenia klastra praca awaryjna .....	35
2.3. Wymagania sprzętowe klastra praca awaryjna .....	36
2.4. Wymagania programowe klastra praca awaryjna .....	42
2.5. Wymagania sieciowe klastra praca awaryjna .....	48
<b>Rozdział 3. Wdrażanie Głównego Urzędu Certyfikacji w trybie offline .....</b>	<b>53</b>
3.1. Minimalne wymagania systemowe dla Głównego Urzędu Certyfikacji .....	54
3.2. Czynności przedinstalacyjne .....	55
3.3. CAPolicy.inf — plik konfiguracyjny dla Głównego Urzędu Certyfikacji .....	57
3.4. Instalowanie usług certyfikatów na Głównym Urzędzie Certyfikacji .....	58
3.5. Czynności poinstalacyjne .....	66
3.5.1. Skanowanie Głównego Urzędu Certyfikacji za pomocą narzędzia Analizator najlepszych rozwiązań .....	67
3.5.2. Skanowanie Głównego Urzędu Certyfikacji za pomocą modułu BestPractices środowiska Windows PowerShell .....	69
3.5.3. Sprawdzanie certyfikatu i konfiguracji Głównego Urzędu Certyfikacji za pomocą narzędzia CertUtil.exe .....	73

3.6.	Konfigurowanie Głównego Urzędu Certyfikacji .....	74
3.6.1.	Ustawianie atrybutu DSConfigDN .....	75
3.6.2.	Konfigurowanie rozszerzeń Punkt dystrybucji listy CRL (CDP) i Dostęp do informacji o urządzeniach (AIA) .....	76
3.6.3.	Konfigurowanie okresu ważności wystawianych certyfikatów .....	80
3.6.4.	Włączanie dyskretnych podpisów w certyfikatach .....	82
3.6.5.	Konfigurowanie zdarzeń do inspekcji .....	82
3.6.6.	Konfigurowanie parametrów publikowania podstawowej listy odwołania certyfikatów (CRL) .....	85
3.6.7.	Publikowanie podstawowej listy CRL .....	87
3.7.	Eksportowanie certyfikatu i listy CRL Głównego Urzędu Certyfikacji .....	89
3.8.	Publikowanie certyfikatu i listy CRL Głównego Urzędu Certyfikacji w magazynie usługi Active Directory .....	89

<b>Rozdział 4.</b>	<b>Wdrażanie Podrzędnego Urzędu Certyfikacji na 1. węźle klastra pracy awaryjnej .....</b>	<b>93</b>
4.1.	Minimalne wymagania systemowe dla Podrzędnego Urzędu Certyfikacji .....	94
4.2.	Etapy wdrażania usług certyfikatów na 1. węźle klastra pracy awaryjnej .....	95
4.3.	CAPolicy.inf — plik konfiguracyjny dla Podrzędnego Urzędu Certyfikacji .....	96
4.4.	Konfigurowanie i instalowanie usług certyfikatów na 1. węźle klastra pracy awaryjnej .....	97
4.5.	Generowanie i eksportowanie certyfikatu cyfrowego dla Podrzędnego Urzędu Certyfikacji .....	107
4.6.	Dodawanie certyfikatu i listy CRL Głównego Urzędu Certyfikacji do magazynu Zaufane główne urzędy certyfikacji .....	111
4.7.	Instalowanie certyfikatu dla Podrzędnego Urzędu Certyfikacji na 1. węźle klastra pracy awaryjnej .....	114
4.8.	Konfigurowanie rozszerzeń CDP i AIA na 1. węźle klastra pracy awaryjnej .....	116
4.9.	Eksportowanie certyfikatu Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) .....	117

<b>Rozdział 5.</b>	<b>Wdrażanie Podrzędnego Urzędu Certyfikacji na 2. węźle klastra pracy awaryjnej .....</b>	<b>121</b>
5.1.	Etapy wdrażania usług certyfikatów na 2. węźle klastra pracy awaryjnej .....	122
5.2.	Importowanie certyfikatu Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) do magazynu Osobisty .....	124
5.3.	Konfigurowanie i instalowanie usług certyfikatów na 2. węźle klastra pracy awaryjnej .....	125

<b>Rozdział 6.</b>	<b>Wdrażanie klastra pracy awaryjnej w środowisku Windows Server 2008 R2 .....</b>	<b>131</b>
6.1.	Podstawowe wymagania dotyczące klastrów pracy awaryjnej .....	132
6.1.1.	Określenie statycznych adresów IP dla kart sieciowych na węzłach klastra pracy awaryjnej .....	133
6.1.2.	Określenie nazwy dla klastra pracy awaryjnej .....	133
6.1.3.	Określenie adresu IP dla klastra pracy awaryjnej .....	135
6.2.	Etapy wdrażania klastra pracy awaryjnej .....	135
6.3.	Instalowanie funkcji Klaster pracy awaryjnej .....	136
6.4.	Sprawdzanie poprawności konfiguracji klastra pracy awaryjnej .....	139
6.5.	Tworzenie dwuwęzłowego klastra pracy awaryjnej typu active/passive .....	151

<b>Rozdział 7. Konfigurowanie klastra pracy awaryjnej typu active/passive .....</b>	<b>155</b>
7.1. Konfigurowanie wysokiej dostępności dla usług certyfikatów .....	156
7.2. Konfigurowanie rozszerzenia CDP dla klastra pracy awaryjnej .....	162
7.3. Tworzenie obiektu typu CRLDistributionPoint w magazynie usługi Active Directory dla klastra pracy awaryjnej .....	164
7.4. Zmiana uprawnień dla węzłów klastra pracy awaryjnej w usłudze Active Directory .....	165
7.5. Zmiana nazwy DNS w usłudze Active Directory dla klastra pracy awaryjnej .....	169
7.6. Testowanie klastra pracy awaryjnej dla usług certyfikatów .....	172
7.6.1. Przenoszenie sklastrowanej usługi certyfikatów pomiędzy węzłami klastra pracy awaryjnej .....	172
7.6.2. Instalowanie certyfikatu użytkownika w magazynie Osobisty z poziomu systemu Windows 7 .....	173
<b>Rozdział 8. Zarządzanie klastrem pracy awaryjnej, PKI, rolami i funkcjami .....</b>	<b>179</b>
8.1. Narzędzia do lokalnego zarządzania klastrem pracy awaryjnej i PKI .....	180
8.1.1. Konsola Menedżer klastra pracy awaryjnej (CluAdmin.msc) .....	181
8.1.2. Program narzędziowy Cluster.exe .....	183
8.1.3. Moduł FailoverClusters środowiska Windows PowerShell (PowerShell.exe) .....	185
8.1.4. Konsola Infrastruktura PKI przedsiębiorstwa (PKIView.msc) .....	187
8.1.5. Konsola Urząd certyfikacji (CertSrv.msc) .....	188
8.1.6. Konsola Certyfikaty (CertMgr.msc) .....	190
8.1.7. Konsola szablonów certyfikatów (CertTpl.msc) .....	192
8.1.8. Program narzędziowy CertUtil.exe .....	195
8.1.9. Program narzędziowy CertReq.exe .....	198
8.2. Narzędzia do zdalnego zarządzania klastrem pracy awaryjnej, PKI, rolami i funkcjami .....	199
8.2.1. Narzędzia administracji zdalnej serwera dla systemu Windows 7 (RSAT) .....	199
8.2.2. Zdalne zarządzanie klastrem pracy awaryjnej (CluAdmin.msc) .....	201
8.2.3. Zdalne zarządzanie Podrzednym Urzędem Certyfikacji w trybie online (CertSrv.msc) .....	203
8.2.4. Zdalne zarządzanie infrastrukturą kluczy publicznych (PKIView.msc) ...	205
8.2.5. Zdalne zarządzanie rolami i funkcjami systemu Windows Server 2008 R2 (WinRM.cmd) .....	208
8.3. Tworzenie konsoli głównej do zdalnego zarządzania klastrem pracy awaryjnej i PKI .....	210
<b>Bibliografia .....</b>	<b>215</b>
<b>Skorowidz .....</b>	<b>219</b>

## Rozdział 5.

# Wdrażanie Podrzędnego Urzędu Certyfikacji na 2. węźle klastra pracy awaryjnej

W tym rozdziale zostanie zaprezentowany szczegółowy proces instalacji oraz konfiguracji Podrzędnego Urzędu Certyfikacji na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, który będzie pracował w trybie online pod kontrolą serwerowego systemu operacyjnego Windows Server 2008 R2 Enterprise. Węzeł ten będzie pełnił (w przypadku awarii 1. węzła klastra pracy awaryjnej) funkcję Podrzędnego Urzędu Certyfikacji o nazwie *PUC01* oraz obsługiwał żądania użytkowników końcowych. Jego konfiguracja będzie różniła się nieco od konfiguracji 1. węzła, która została przedstawiona w rozdziale 4.

Z tego rozdziału dowiesz się, jak wygląda przebieg wdrażania usług certyfikatów na 2. węźle klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, podzielony na następujące etapy:

- ◆ sprawdzenie, czy udostępnione na macierzy pamięci masowej SAN iSCSI dyski klastrowe *Dysk 1* i *Dysk 2* są dostępne i znajdują się w stanie online,
- ◆ przygotowanie pliku konfiguracyjnego *CAPolicy.inf* oraz umieszczenie go w lokalizacji *%SYSTEMROOT%* (zwykle *C:\Windows*). Plik ten można skopiować z 1. węzła dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, tj. z serwera klastrowanego *SRV01*.
- ◆ zaimportowanie do lokalnego magazynu certyfikatów *Zaufane główne urzędy certyfikacji* certyfikatu cyfrowego i podstawowej listy CRL Głównego Urzędu Certyfikacji,

- ◆ zaimportowanie do lokalnego magazynu certyfikatów *Osobisty* certyfikatu cyfrowego Podrzednego Urzedu Certyfikacji (z kluczem prywatnym), tj. pliku z rozszerzeniem \*.p12,
- ◆ skonfigurowanie i zainstalowanie roli *Uslugi certyfikatow w usłudze Active Directory* na potrzeby środowiska dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive*, które zostało przedstawione w rozdziale 2.,
- ◆ skonfigurowanie (z wykorzystaniem skryptu) dwóch rozszerzeń: *Punkt dystrybucji listy CRL (CDP)* oraz *Dostęp do informacji o urzędach (AIA)*.

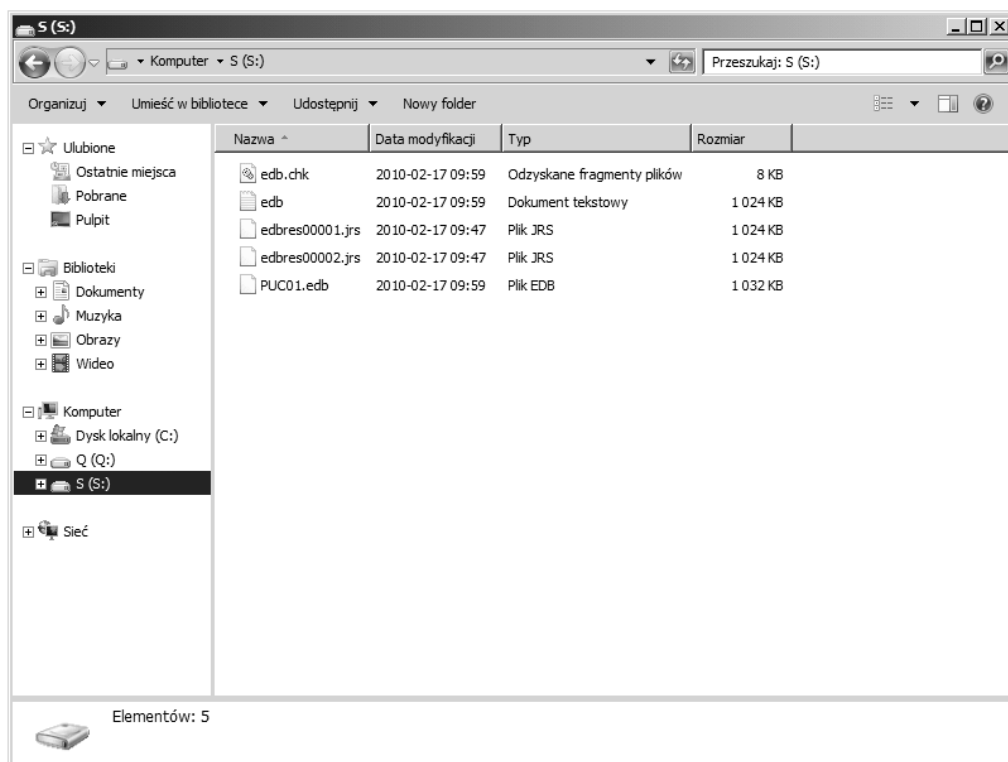
## 5.1. Etapy wdrażania uslug certyfikatow na 2. węzle klastra pracy awaryjnej

Wdrażanie uslug certyfikatow na 2. węzle dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive*, pracujacego pod kontrola serwerowego systemu operacyjnego Windows Server 2008 R2 Enterprise, sklada sie z kilku krokow (etapow), które należy wykonać w takiej kolejności, w jakiej zostały przedstawione ponizej.

**Etap 1.** Sprawdzenie, czy udostępnione na macierzy pamieci masowej SAN iSCSI dyski klastrowe *Dysk 1* i *Dysk 2* są dostępane dla 2. węzła klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive* oraz znajduja sie w stanie online. Można tu wykorzystać (jak w poprzednim rozdziale) program narzedziowy *DiskPart.exe* lub konsolę graficzną *Zarządzanie dyskami*. Na dysku klastrowym *S* powinny być pliki, które zostały utworzone podczas uruchamiania uslugi certyfikatow na 1. serwerze klastrowanym *SRV01* (rysunek 5.1). Ten krok należy wykonać samodzielnie.

**Etap 2.** Przygotowanie pliku konfiguracyjnego *CAPolicy.inf* oraz umieszczeniu go w lokalizacji *%SYSTEMROOT%* (zwykle *C:\Windows*). Plik ten można skopiować z 1. węzła dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive*, tj. z serwera klastrowanego *SRV01*. Ten krok należy wykonać samodzielnie.

**Etap 3.** Zaimportowanie do lokalnego magazynu certyfikatow *Zaufane glowne urzedy certyfikacji* certyfikatu cyfrowego i podstawowej listy CRL Glownego Urzedu Certyfikacji. Można tu wykorzystać program narzedziowy *CertUtil.exe* (wraz z przełącznikiem *-addstore*). Ten krok należy wykonać samodzielnie, zgodnie z informacjami przedstawionymi w poprzednim rozdziale.



**Rysunek 5.1.** Zawartość udostępnionego dysku klastrowego S (na serwerze SRV02)

**Etap 4.** Zaimportowanie do lokalnego magazynu certyfikatów *Osobisty* certyfikatu cyfrowego Podrzednego Urzędu Certyfikacji (z kluczem prywatnym), tj. pliku z rozszerzeniem \*.p12. Ten krok zostanie przedstawiony szczegółowo w dalszej części rozdziału.

**Etap 5.** Skonfigurowanie i zainstalowanie roli *Usługi certyfikatów* w usłudze *Active Directory* na potrzeby środowiska dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, które zostało przedstawione w rozdziale 2. Ten krok zostanie szczegółowo przedstawiony w dalszej części tego rozdziału.

**Etap 6.** Skonfigurowanie (z wykorzystaniem skryptu) dwóch rozszerzeń: *Punkt dystrybucji listy CRL (CDP)* oraz *Dostęp do informacji o urządach (AIA)*. Ten krok należy wykonać samodzielnie, wykorzystując skrypt `PUC01_skrypt01.cmd`, którego zawartość została przedstawiona w poprzednim rozdziale.

## 5.2. Importowanie certyfikatu Podrzednego Urzedu Certyfikacji (z kluczem prywatnym) do magazynu Osobisty

Aby z poziomu 2. wężla dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive* *zaimportowac certyfikat cyfrowy Podrzednego Urzedu Certyfikacji* (z kluczem prywatnym) do jego lokalnego magazynu certyfikatow *Osobisty*, nalezy wykonac (jako administrator domenowy) komende `CertUtil.exe -importPFX A:\CA\PUC01.p12`. Gdy zostanie wprowadzone poprawne haslo, pojawi sie komunikat, ktorego tresc przedstawiono na listingu 5.1.

**Listing 5.1.** *Wynik wykonania komendy `CertUtil.exe -importPFX A:\CA\PUC01.p12` (na serwerze SRV02)*

```
Wprowadz haslo PFX:
Certyfikat "CN=PUC01, DC=EA, DC=local" zostal dodany do magazynu.
CertUtil: polecenie -importPFX zostalo wykonane pomyslnie.
```

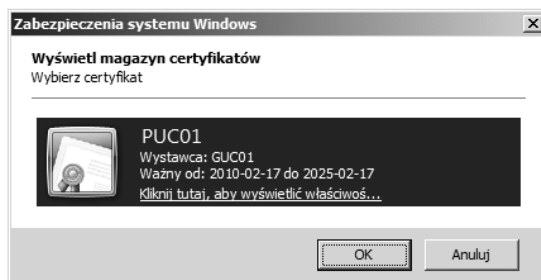


Uwaga

Przed *zaimportowaniem* z poziomu 2. wężla dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive* certyfikatu cyfrowego Podrzednego Urzedu Certyfikacji (z kluczem prywatnym) do jego lokalnego magazynu certyfikatow *Osobisty* nalezy *zaimportowac certyfikat cyfrowy oraz podstawowal liste CRL Glownego Urzedu Certyfikacji do lokalnego magazynu certyfikatow *Zaufane glowne urzedy certyfikacji**. Mozna tu wykorzystac program narzedziowy `CertUtil.exe` (wraz z przełącznikiem `-addstore`). Powyzsze czynnosci uzytkownik powinien wykonac samodzielnie, zgodnie z informacjami przedstawionymi w poprzednim rozdziale.

O tym, czy faktycznie certyfikat cyfrowy Podrzednego Urzedu Certyfikacji (z kluczem prywatnym) zostal dodany do lokalnego magazynu certyfikatow *Osobisty* 2. wężla dwuwęzlowego klastra pracy awaryjnej dla uslug certyfikatow typu *active/passive*, mozna sie przekonac, wykonujac np. komende `CertUtil.exe -viewstore My PUC01`. W rezultacie powinno sie pojawic okno podobne do przedstawionego na rysunku 5.2.

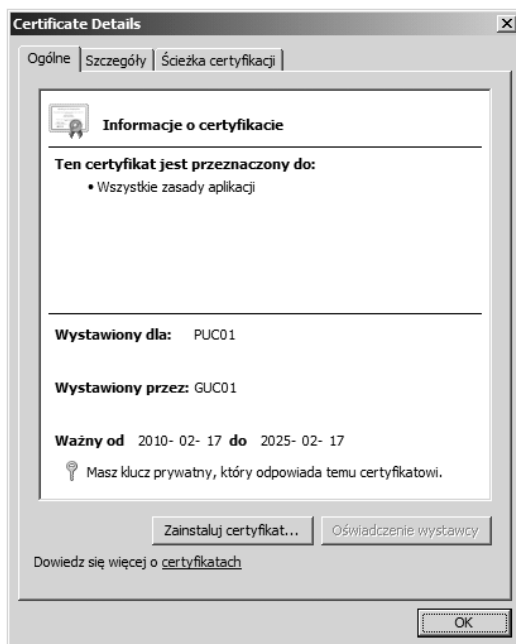
**Rysunek 5.2.**  
*Wynik wykonania komendy `CertUtil.exe -viewstore My PUC01` (na serwerze SRV02)*





Po kliknięciu certyfikatu cyfrowego *PUC01* (rysunek 5.2) można wyświetlić jego szczegółowe informacje. Warto się tutaj upewnić, czy na zakładce *Ogólne* znajduje się informacja o tym, że certyfikat ma klucz prywatny (rysunek 5.3). Certyfikat ten będzie potrzebny podczas konfigurowania roli *Usługi certyfikatów w usłudze Active Directory* na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*.

**Rysunek 5.3.**  
Zakładka *Ogólne*  
certyfikatu  
Podrzednego  
Urzędu Certyfikacji  
(z kluczem prywatnym)  
na serwerze *SRV02*



Uwaga

Certyfikat cyfrowy Podrzednego Urzędu Certyfikacji (z kluczem prywatnym) można wyświetlić także z poziomu konsoli graficznej *Certyfikaty* (dla komputera lokalnego).

## 5.3. Konfigurowanie i instalowanie usług certyfikatów na 2. węźle klastra pracy awaryjnej

Aby poprawnie skonfigurować i zainstalować usługi certyfikatów na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, trzeba wykonać przedstawione poniżej kroki (jako administrator domenowy) na serwerze klastrowanym *SRV02*.

Aby skonfigurować i zainstalować na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive* rolę *Usługi certyfikatów w usłudze Active*

*Directory*, należy wykonać kroki podobne do opisanych w przypadku instalacji tej roli na 1. węźle tego typu klastra (z małymi wyjątkami, o których będzie mowa w tym rozdziale).

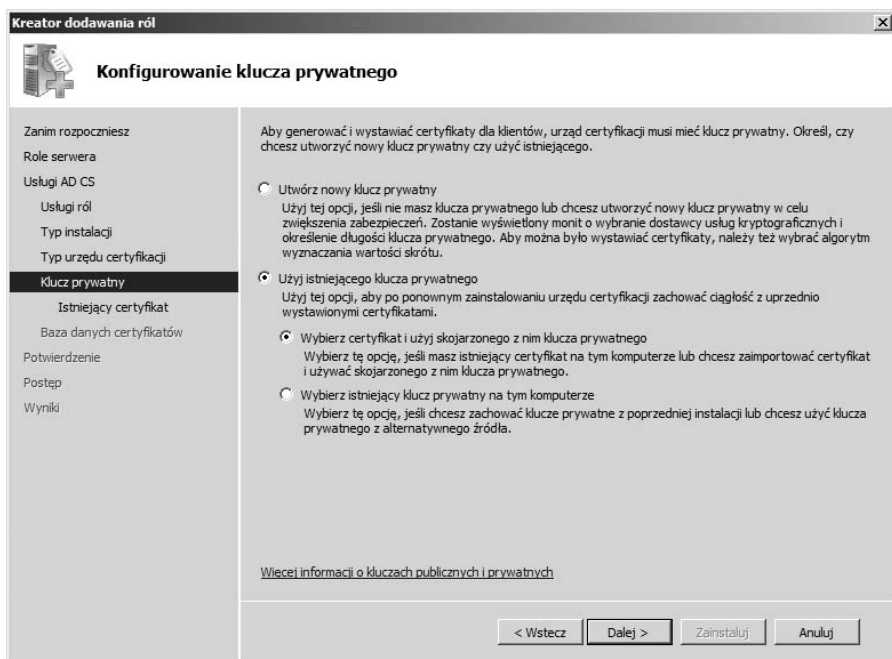
1. Uruchomić konsolę graficzną *Menedżer serwera* (np. za pomocą komendy `ServerManager.msc`).
2. W lewym panelu konsoli *Menedżer serwera* wybrać gałąź *Role*.
3. W prawym panelu konsoli kliknąć odnośnik *Dodaj rolę*, co spowoduje uruchomienie narzędzia graficznego *Kreator dodawania ról*, w którym należy (po zapoznaniu się z podstawowymi informacjami) kliknąć przycisk *Dalej*.
4. Na stronie *Wybieranie ról serwera* zaznaczyć opcję *Usługi certyfikatów w usłudze Active Directory*, a następnie kliknąć przycisk *Dalej*.
5. Po zapoznaniu się z informacjami znajdującymi się na stronie *Wprowadzenie do Usług certyfikatów w usłudze Active Directory* należy kliknąć przycisk *Dalej*.
6. Na stronie *Wybieranie usług ról* należy upewnić się, czy zaznaczona jest opcja *Urząd certyfikacji*, a następnie kliknąć przycisk *Dalej*.
7. Na stronie *Określanie typu instalacji* należy zaznaczyć pierwszą opcję *Przedsiębiorstwo*, a następnie kliknąć przycisk *Dalej*.
8. Na stronie *Określanie typu urzędu certyfikacji* należy upewnić się, czy zaznaczona jest druga z opcji, tj. *Podrzędny urząd certyfikacji*, a następnie kliknąć przycisk *Dalej*.
9. Na stronie *Konfigurowanie klucza prywatnego*, która została przedstawiona na rysunku 5.4, należy zaznaczyć opcje: *Użyj istniejącego klucza prywatnego* oraz *Wybierz certyfikat i użyj skojarzonego z nim klucza prywatnego*. Powyższe ustawienia należy zatwierdzić przyciskiem *Dalej*.



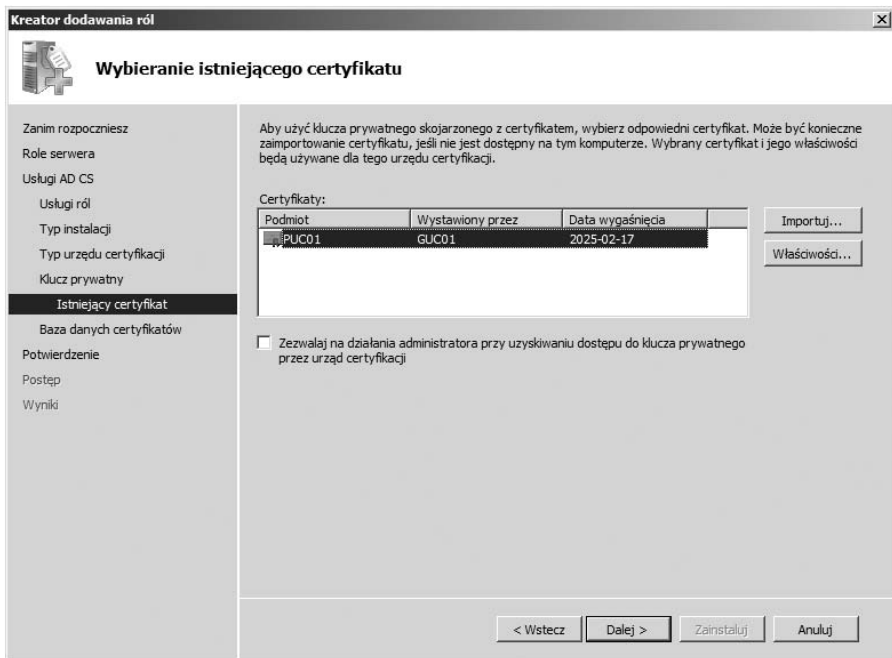
Uwaga

Jeżeli przed rozpoczęciem na 2. węźle klastra pracy awaryjnej instalacji roli *Usługi certyfikatów w usłudze Active Directory* nie zostanie zaimportowany certyfikat cyfrowy *Podrzednego Urzędu Certyfikacji* (z kluczem prywatnym) do lokalnego magazynu certyfikatów *Osobisty*, to nie będzie on widoczny w oknie *Certyfikaty*, które jest dostępne z poziomu strony *Wybieranie istniejącego certyfikatu*.

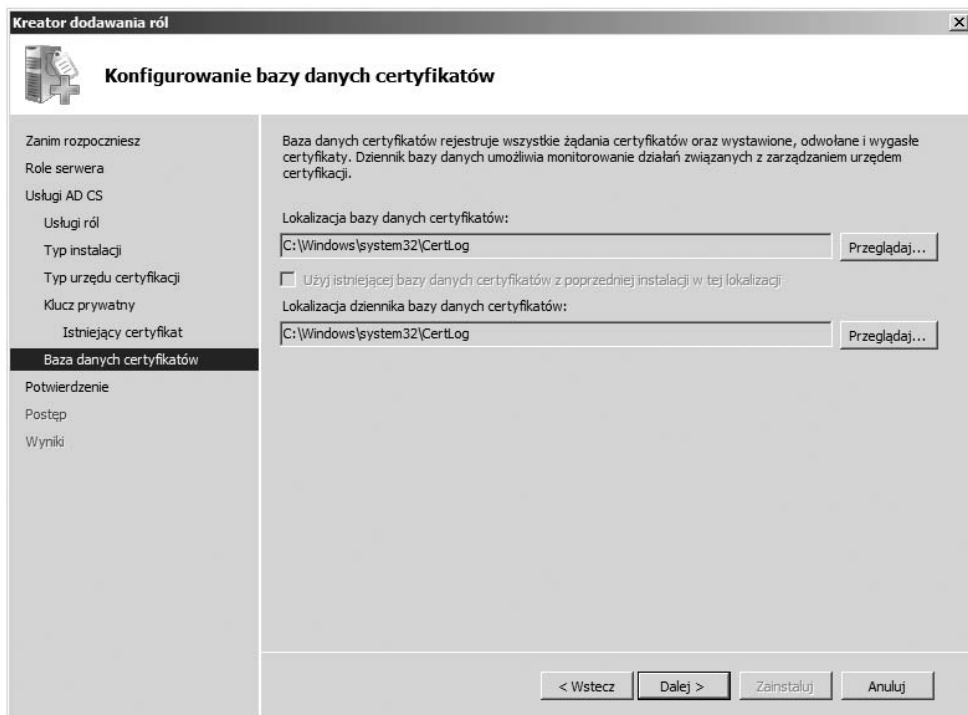
10. Na stronie *Wybieranie istniejącego certyfikatu* należy zaznaczyć (rysunek 5.5) certyfikat cyfrowy *PUC01* (z kluczem prywatnym) i kliknąć przycisk *Dalej*.
11. Na stronie *Konfigurowanie bazy danych certyfikatów*, którą przedstawia rysunek 5.6, należy zmienić domyślne ścieżki dla lokalizacji bazy danych certyfikatów cyfrowych oraz jej dziennika transakcyjnego na lokalizację *S*, tj. na udostępniony dysk klastrowy, znajdujący się na macierzy pamięci masowej SAN iSCSI.
12. Przy próbie zmiany lokalizacji bazy danych certyfikatów cyfrowych i jej dziennika transakcyjnego powinno pojawić się ostrzeżenie, które przedstawia rysunek 5.7. Narzędzie *Kreator dodawania ról* wyświetli ostrzeżenie



**Rysunek 5.4.** Strona Konfigurowanie klucza prywatnego dla Podrzednego Urzędu Certyfikacji (na serwerze SRV02)



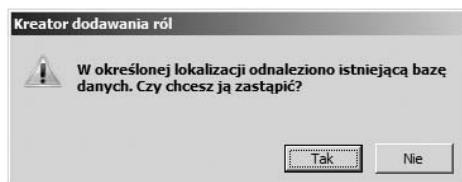
**Rysunek 5.5.** Strona Wybieranie istniejącego certyfikatu dla Podrzednego Urzędu Certyfikacji (na serwerze SRV02)



**Rysunek 5.6.** Strona Konfigurowanie bazy danych certyfikatów dla Podrzednego Urzędu Certyfikacji (na serwerze SRV02) przed zmianami

**Rysunek 5.7.**

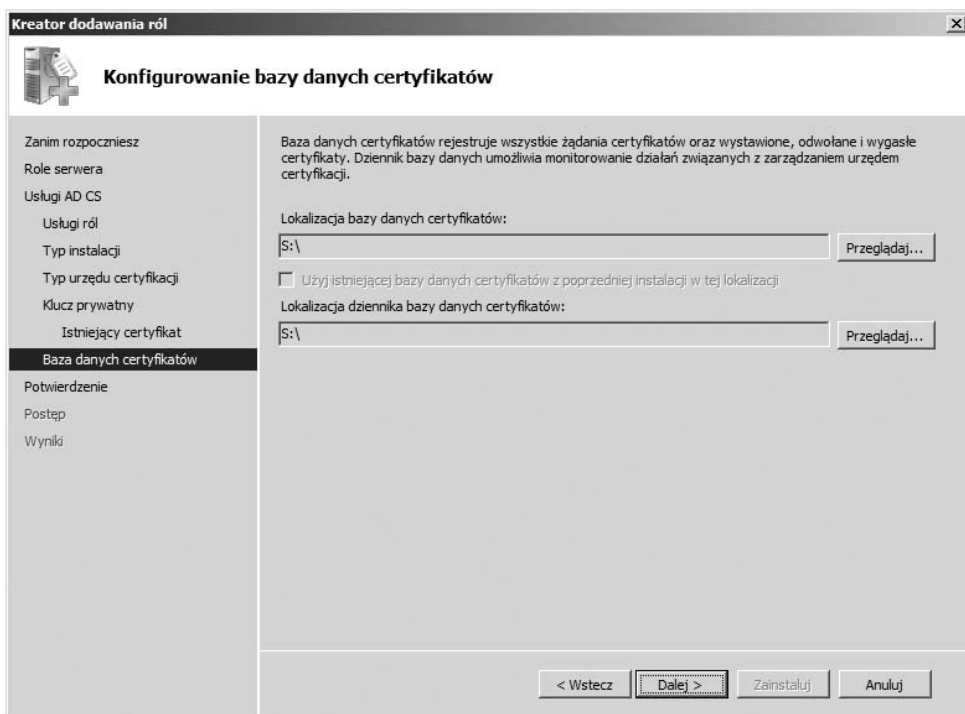
*Ostrzeżenie o zastąpieniu istniejącej bazy danych certyfikatów (na serwerze SRV02)*



informujące o tym, że w określonej lokalizacji (na udostępnionym dysku klastrowym *S*) istnieje baza danych. Jest to baza danych certyfikatów Podrzednego Urzędu Certyfikacji. W poprzednim rozdziale została utworzona na udostępnionym dysku klastrowym *S* baza danych (podczas uruchamiania na 1. węźle klastra pracy awaryjnej usługi certyfikatów *CertSvc*). Na tym etapie należy kliknąć przycisk *Tak*. Ustawienia końcowe dla lokalizacji bazy danych certyfikatów i jej dziennika powinny być podobne do tych, które zostały przedstawione na rysunku 5.8. Jeżeli tak faktycznie jest, to należy kliknąć przycisk *Dalej*.

**13.** Na stronie *Potwierdzenie opcji instalacji* należy kliknąć przycisk *Zainstaluj*.

Gdy zostaną wykonane powyższe kroki, rozpocznie się proces instalowania roli *Usługi certyfikatów w usłudze Active Directory* na 2. węźle dwuwęzłowego klastra pracy awaryjnej typu *active/passive*. Jego poszczególne etapy będą



**Rysunek 5.8.** Strona Konfigurowanie bazy danych certyfikatów dla Podrzednego Urzędu Certyfikacji (na serwerze SRV02) po zmianach

wyświetlane na bieżąco na stronie *Postęp instalacji*, której tutaj nie przedstawiono. Proces instalacyjny usług certyfikatów może trwać kilka minut; po jego zakończeniu wyświetli się strona *Wyniki instalacji*, informująca o pomyślnym zainstalowaniu powyższej roli.

**14.** Zamknąć okno narzędzia *Kreator dodawania ról*, klikając przycisk *Zamknij*.

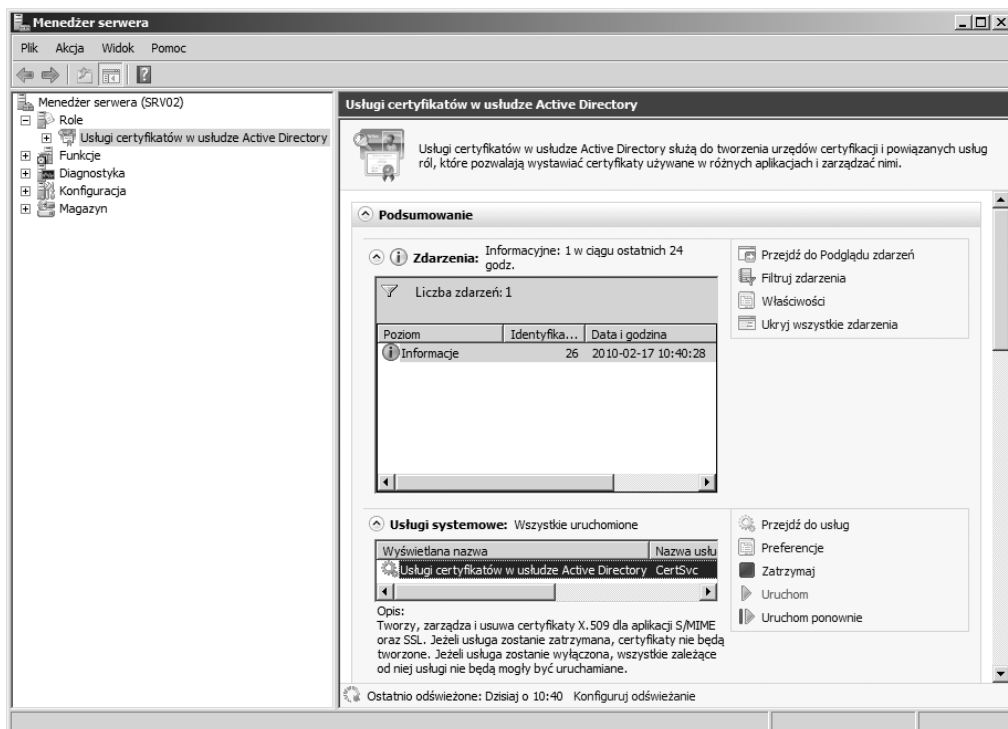
Wykonanie powyższych kroków sprawi, że konsola *Menedżer serwera* na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive* zmieni wygląd na podobny do tego z rysunku 5.9.



Uwaga

Po zainstalowaniu na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive* roli *Usługi certyfikatów w usłudze Active Directory* należy pamiętać o tym, aby następnie skonfigurować m.in. dwa ważne rozszerzenia: *Punkt dystrybucji listy CRL (CDP)* i *Dostęp do informacji o urzędach (AIA)*. Można wykorzystać do tego celu skrypt *PUC01\_skrypt01.cmd*, którego zawartość została przedstawiona w rozdziale 4. Można też rozważyć skonfigurowanie inspekcji, jeżeli zajdzie taka potrzeba, czy innych ustawień.

Mając zainstalowane i skonfigurowane role *Usługi certyfikatów w usłudze Active Directory* na obu węzłach dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, można przystąpić do wdrażania tego typu klastra zgodnie z informacjami przedstawionymi w następnym rozdziale.



**Rysunek 5.9.** Gałąź Usługi certyfikatów w usłudze Active Directory po zainstalowaniu roli Usługi certyfikatów w usłudze Active Directory (na serwerze SRV02)