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

Autor: Andrzej Szeląg
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

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 Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym), tj. pliku z rozszerzeniem **.p12*,
- 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.,
- skonfigurowanie (z wykorzystaniem skryptu) dwóch rozszerzeń: *Punkt dystrybucji listy CRL (CDP)* oraz *Dostęp do informacji o urzędach (AIA)*.

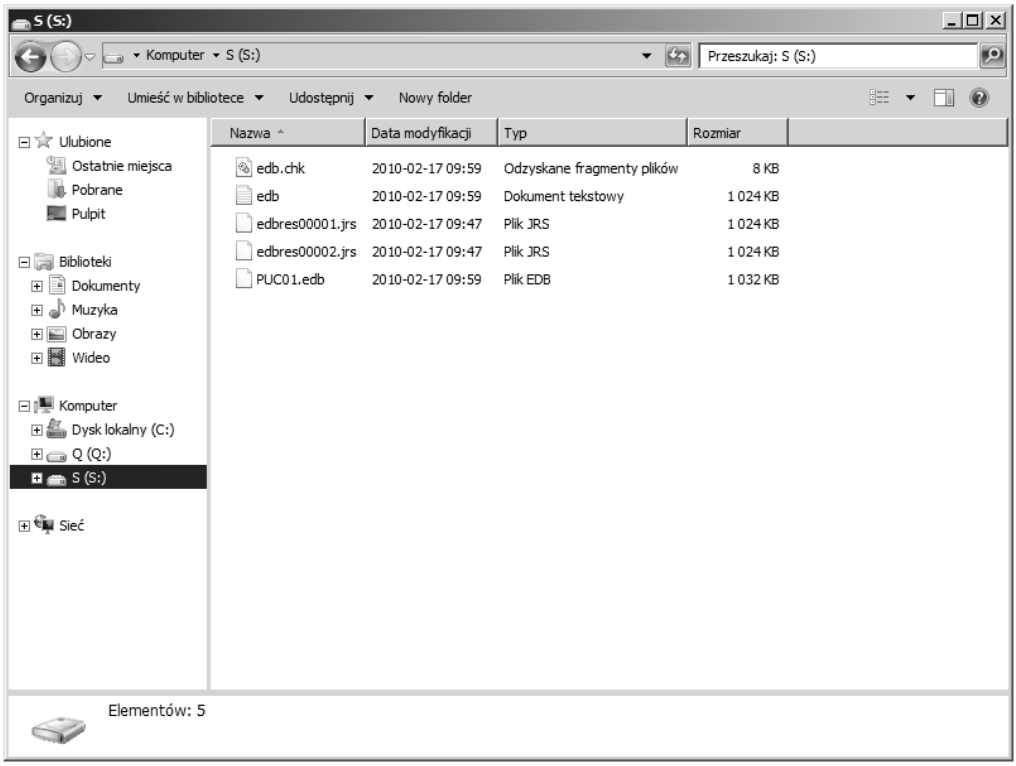
5.1. Etapy wdrażania usług certyfikatów na 2. węźle klastra pracy awaryjnej

Wdrażanie usług certyfikatów na 2. węźle dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, pracującego pod kontrolą serwerowego systemu operacyjnego Windows Server 2008 R2 Enterprise, składa się z kilku kroków (etapów), które należy wykonać w takiej kolejności, w jakiej zostały przedstawione poniżej.

Etap 1. Sprawdzenie, czy udostępnione na macierzy pamięci masowej SAN iSCSI dyski klastrowe *Dysk 1* i *Dysk 2* są dostępne dla 2. węzła klastra pracy awaryjnej dla usług certyfikatów typu *active/passive* oraz znajdują się w stanie online. Można tu wykorzystać (jak w poprzednim rozdziale) program narzędziowy *DiskPart.exe* lub konsolę graficzną *Zarządzanie dyskami*. Na dysku klastrowym *S* powinny być pliki, które zostały utworzone podczas uruchamiania usługi certyfikatów 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 dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, tj. z serwera klastrowanego *SRV01*. Ten krok należy wykonać samodzielnie.

Etap 3. Zaimportowanie do lokalnego magazynu certyfikatów *Zaufane główne urzędy certyfikacji* certyfikatu cyfrowego i podstawowej listy CRL Głównego Urzędu Certyfikacji. Można tu wykorzystać program narzędziowy *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 Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym), tj. pliku z rozszerzeniem **.p12*. Ten krok zostanie przedstawiony szczegółowo w dalszej części tego 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 urzędach (AIA)*. Ten krok należy wykonać samodzielnie, wykorzystując skrypt *PUC01_skrypt01.cmd*, którego zawartość została przedstawiona w poprzednim rozdziale.

5.2. Importowanie certyfikatu Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) do magazynu Osobisty

Aby z poziomu 2. węzła dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu active/passive *zaimportować certyfikat cyfrowy Podrzędnego Urzędu Certyfikacji* (z kluczem prywatnym) do jego lokalnego magazynu certyfikatów *Osobisty*, należy wykonać (jako administrator domenowy) komendę `CertUtil.exe -importPFX A:\CA\PUC01.p12`. Gdy zostanie wprowadzone poprawne hasło, pojawi się komunikat, którego treść przedstawiono na listingu 5.1.

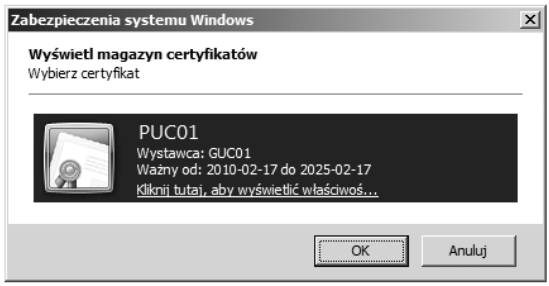
Listing 5.1. *Wynik wykonania komendy CertUtil.exe -importPFX A:\CA\PUC01.p12 (na serwerze SRV02)*

```
Wprowadź hasło PFX:
Certyfikat "CN=PUC01, DC=EA, DC=local" został dodany do magazynu.
CertUtil: polecenie -importPFX zostało wykonane pomyślnie.
```


Uwaga

Przed zaimportowaniem z poziomu 2. węzła dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive* certyfikatu cyfrowego Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) do jego lokalnego magazynu certyfikatów *Osobisty* należy zaimportować certyfikat cyfrowy oraz podstawową listę CRL Głównego Urzędu Certyfikacji do lokalnego magazynu certyfikatów *Zaufane główne urzędy certyfikacji*. Można tu wykorzystać program narzędziowy *CertUtil.exe* (wraz z przełącznikiem `-addstore`). Powyższe czynności użytkownik powinien wykonać samodzielnie, zgodnie z informacjami przedstawionymi w poprzednim rozdziale.

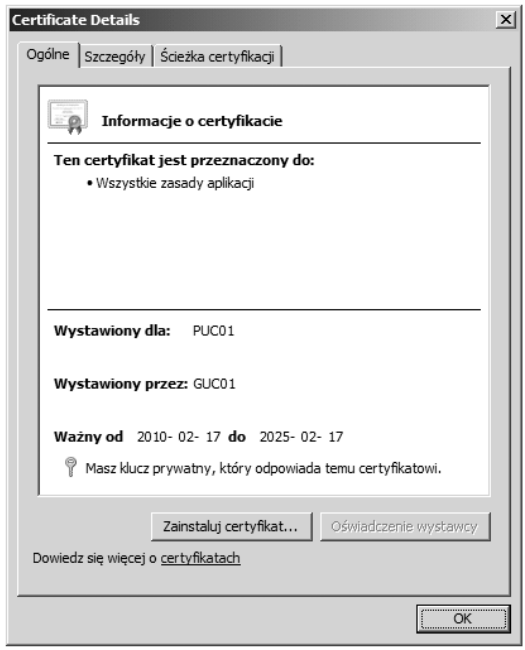
O tym, czy faktycznie certyfikat cyfrowy Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) został dodany do lokalnego magazynu certyfikatów *Osobisty* 2. węzła dwuwęzłowego klastra pracy awaryjnej dla usług certyfikatów typu *active/passive*, można się przekonać, wykonując np. komendę `CertUtil.exe -viewstore My PUC01`. W rezultacie powinno się pojawić 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 Podrzędnego Urzędu Certyfikacji (z kluczem prywatnym) na serwerze SRV02*




Uwaga

Certyfikat cyfrowy Podrzędnego 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*

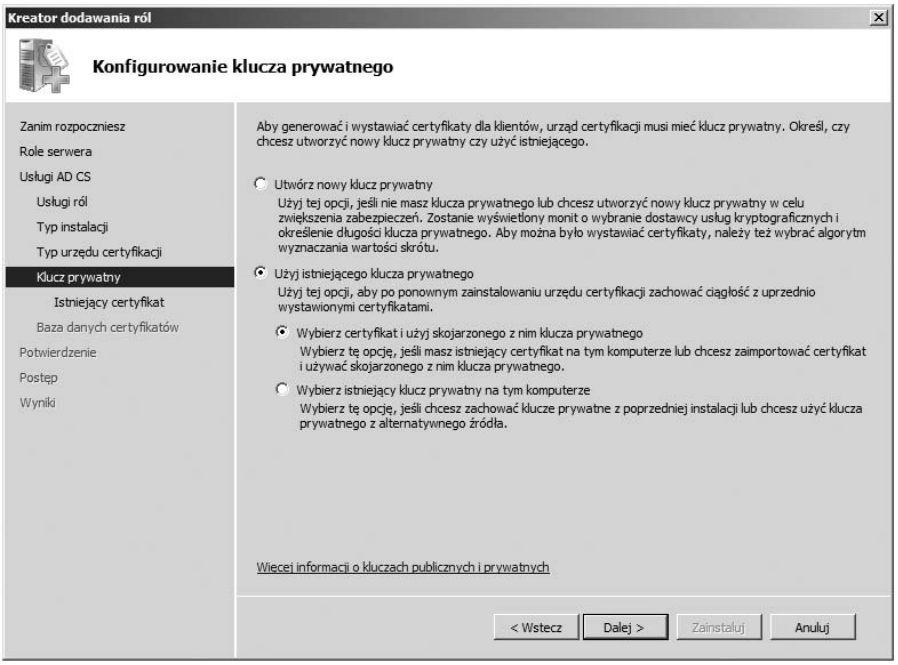
Directory, należy wykonać kroki podobne do opisanych w przypadku instalacji tej roli na 1. węźle tego typu klastra (z małymi wyjątkami, o których będzie mowa w tym rozdziale).

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 role*, 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*.

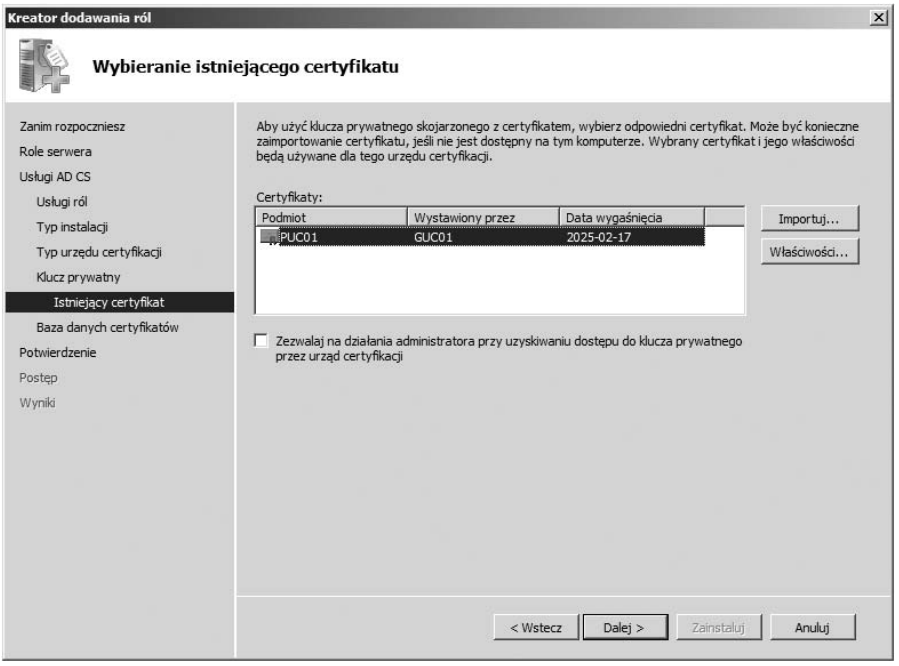

Uwaga

Jeżeli przed rozpoczęciem na 2. węźle klastra pracy awaryjnej instalacji roli *Usługi certyfikatów w usłudze Active Directory* nie zostanie zaimportowany certyfikat cyfrowy Podrzędnego 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*.

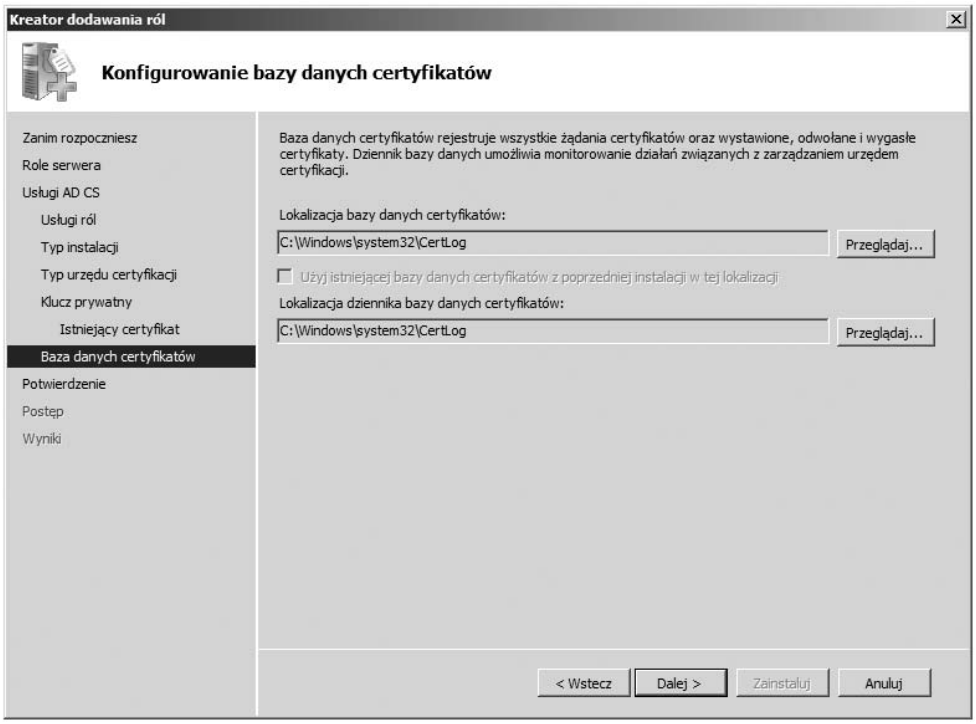
10. Na stronie *Wybieranie istniejącego certyfikatu* należy zaznaczyć (rysunek 5.5) certyfikat cyfrowy *PUC01* (z kluczem prywatnym) i kliknąć przycisk *Dalej*.
11. Na stronie *Konfigurowanie bazy danych certyfikatów*, którą przedstawia rysunek 5.6, należy zmienić domyślne ścieżki dla lokalizacji bazy 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 Podrzędnego Urzędu Certyfikacji (na serwerze SRV02)*

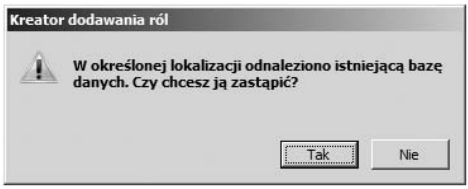


Rysunek 5.5. *Strona Wybieranie istniejącego certyfikatu dla Podrzędnego Urzędu Certyfikacji (na serwerze SRV02)*



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

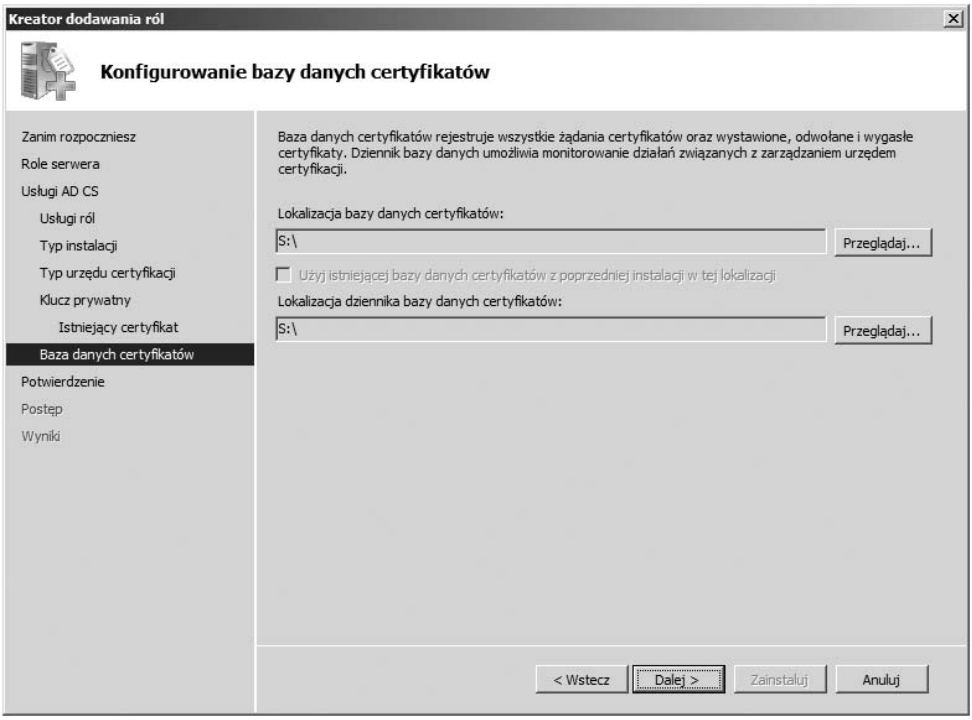
Rysunek 5.7. *Ostrzeżenie o zastąpieniu istniejącej bazy danych certyfikatów (na serwerze SRV02)*



informujące o tym, że w określonej lokalizacji (na udostępnionym dysku klastrowym *S*) istnieje baza danych. Jest to baza danych certyfikatów Podrzędnego 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 *Potwierdzanie 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 Podrzędnego 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.

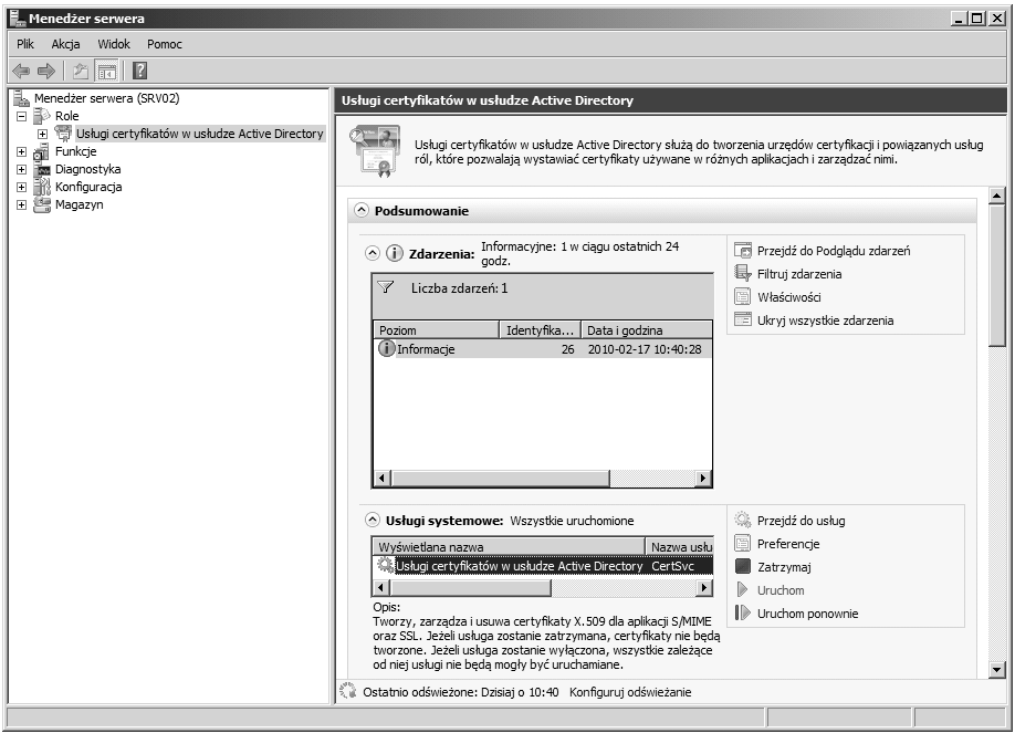
14. Zamknąć okno narzędzia *Kreator dodawania ról*, klikając przycisk *Zamknij*.

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)*