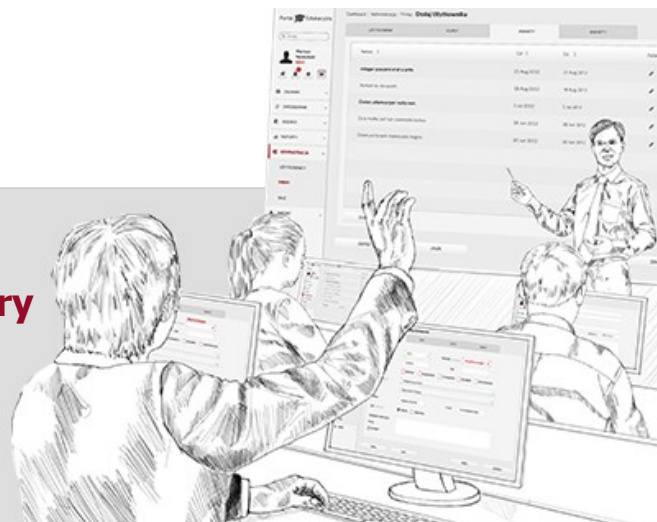


Usługi certyfikatów w Active Directory na Windows Server 2016



Autor i trener



Trener Tomasz Gniadek

Administrator i certyfikowany trener firmy Microsoft.



Od ponad 16 lat aktywnie szkoli na rynku IT, od 2003 roku dzieli się wiedzą jako certyfikowany trener Microsoft.

Specjalizuje się w technologiach związanych z Windows Server, Exchange Server i bazami danych SQL Server. Potwierdza to uzyskanymi certyfikatami MCSE Server Infrastructure, MCITP Database Administrator i MCITP Enterprise Messaging Administrator.

Posiada również 7-letnią praktykę jako administrator i wdrożeniowiec. Pomaga firmom w zaplanowaniu i modernizacji ich środowisk IT. Dzięki codziennej pracy jako administrator ma stały kontakt z najnowszymi technologiami nie tylko w teorii, ale również w praktyce.

Opis warsztatów

Ćwiczenia praktyczne, podczas których uczestnicy wdrażają rozwiązania oparte o certyfikaty dla aplikacji i usług sieciowych.



Czas trwania: 16 godzin



Wymagania wstępne:

- Doświadczenie w planowaniu i posługiwaniu się zagadnieniami AD DS w Windows Server 2012 lub Windows Server 2016.

- Doświadczenie w pracy i konfigurowaniu środowiska opartego o Windows Server 2012 lub Windows Server 2016.
- Praktyczna wiedza na temat podstaw zagadnień sieciowych, włączając protokoły TCP/IP i usługi DNS, DHCP.
- Praktyczna wiedza podstaw wirtualizacji na platformie Microsoft Hyper-V.
- Doświadczenie w obsłudze stacji klienckich opartych na systemach operacyjnych Windows 7, Windows 8.1 lub Windows 10.



Dla kogo:

Warsztaty skierowane są do administratorów oraz specjalistów IT, pracujących w systemach Windows Server 2012 lub Windows Server 2016, którzy chcą zdobyć wiedzę i umiejętności niezbędne do instalacji i konfiguracji infrastruktury usług certyfikacyjnych w środowisku Windows Server 2016.



Zakres tematyczny:

1) Architektura infrastruktury klucza publicznego

2) Tworzenie hierarchii urzędów certyfikacji

- a. Tworzenie autonomicznego głównego urzędu certyfikacji (Offline Root CA)
- b. Tworzenie podrzędnego urzędu certyfikacji przedsiębiorstwa (Sub Enterprise CA)
- c. Kopia zapasowa i odzyskiwanie usług CA

3) Zarządzanie odwoływaniem certyfikatów

- a. Odrzucanie żądań certyfikatów
- b. Definiowanie ustawień publikacji list CRL
- c. Instalacja i konfiguracja usługi Online Responder

4) Zarządzanie rejestracją certyfikatów

- a. Konfiguracja szablonów certyfikatów
- b. Konfiguracja automatycznego i ręcznego zatwierdzania żądań
- c. Zarządzanie odnawianiem certyfikatów
- d. Archiwizacja i odtwarzanie kluczy prywatnych certyfikatów

5) Używanie certyfikatów dla kart czipowych (Smart Cards)

- a. Wstęp do usług autoryzacji przy pomocy SmartCard
- b. Szablony certyfikatów wydawanych dla kart czipowych
- c. Zgłaszanie żądań certyfikatu z użyciem agenta rejestracji

6) Zabezpieczanie komunikacji http przy pomocy certyfikatów

- a. Konfiguracja szablonu certyfikatu
- b. Rejestracja certyfikatu na serwerze WWW
- c. Kojarzenie certyfikatów w IIS

7) Migracja usług certyfikatów z poprzednich wersji Windows Server 2008 lub Windows Server 2012