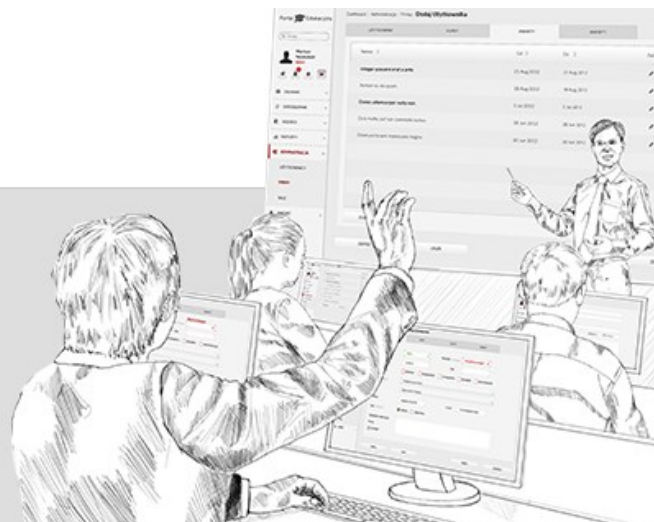


Zarządzanie infrastrukturą klucza publicznego na platformie Windows Server 2012



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

Uczestnicy podczas ćwiczeń praktycznych wdrażają rozwiązania oparte o certyfikaty dla aplikacji i usług sieciowych.

Warsztat skierowany jest do administratorów oraz specjalistów IT pracujących w systemach Windows Server 2008 lub Windows Server 2012, którzy chcą zdobyć wiedzę i umiejętności niezbędne, do planowania, instalacji i infrastruktury usług certyfikacyjnych w środowisku Windows 2012.



Czas trwania: 24 godziny



Zakres tematyczny:

1. Przegląd infrastruktury klucza publicznego

- Wprowadzenie do PKI
- Podstawy kryptografii
- Certyfikaty i urzędy certyfikacji

2. Projektowanie hierarchii urzędów certyfikacyjnych

- Identyfikacja wymagań i planowanie struktury CA dla domeny AD

3. Tworzenie hierarchii urzędów certyfikacji

- Konfiguracja pliku CAPolicy.inf
- Tworzenie autonomicznego głównego urzędu certyfikacji (Offline Root CA)
- Tworzenie podrzędnego urzędu certyfikacji przedsiębiorstwa (Sub Enterprise CA)
- Definiowanie ustawień publikacji list CRL i AIA
- Publikacja list CRL i AIA

4. Zarządzanie strukturą CA

- zatwierdzanie, odrzucanie żądań certyfikatów
- zarządzanie archiwizacją i odtwarzaniem bazy certyfikatów
- zarządzanie konfiguracją CA

5. Konfiguracja szablonów certyfikatów

- Przegląd szablonów
- Planowanie, wdrażanie i publikowanie szablonów

6. Konfiguracja dystrybucji certyfikatów

- Zarządzanie zmianami w istniejących certyfikatach.
- Konfiguracja automatycznego i ręcznego zatwierdzania żądań

7. Archiwizacja i odtwarzanie kluczy certyfikatów

8. Wdrażanie środowiska autoryzacji za pomocą kart czipowych (Smart Cards)

- Wstęp do usług autoryzacji przy pomocy SmartCard
- Tworzenie certyfikatów potrzebnych dla kart czipowych
- Zgłaszanie żądania dla karty czipowej
- Zatwierdzanie żądań certyfikatów dla SmartCard

9. Zabezpieczanie ruchu WEB przy pomocy SSL

- Podstawowe pojęcia
- Włączanie szyfrowania dla katalogów wirtualnych IIS
- Kojarzenie certyfikatów z kontami użytkowników w Active Directory
- Kojarzenie certyfikatów w IIS

10. Zabezpieczanie poczty elektronicznej

- Przegląd zagadnień związanych z szyfrowaniem poczty
- Szyfrowanie i podpisywanie cyfrowe poczty elektronicznej (MS Outlook 2013 i Exchange 2013)

11. Podpisywanie cyfrowe skryptów i aplikacji

12. Migracja usług certyfikatów z poprzednich wersji Windows Server