

Configure secure access to your workloads using networking with Azure Virtual Network



Odbiorcy szkolenia

Szkolenie przeznaczone dla specjalistów IT, którzy zajmują się zagadnieniami bezpiecznego dostępu do obciążeń przy użyciu sieci wirtualnej platformy Azure oraz na co dzień wykonują zadania na platformie Azure. Szkolenie jest pomostem pomiędzy umiejętnościami na poziomie podstawowym a umiejętnościami stowarzyszonymi na poziomie podstawowym, co pomaga uczestnikom osiągnąć postęp na wielu stanowiskach IT, w tym zadania w zakresie infrastruktury i bezpieczeństwa dla administratorów i architektów. Kurs ma na celu przeciwiczenie konfiguracji i zabezpieczania zasobów sieciowych, w tym tworzenie i konfigurowanie sieci wirtualnych, routing sieciowy, strefy DNS, ustawienia DNS, sieciowe grupy zabezpieczeń i zaporę platformy Azure.



Korzyści

Nabycie wiedzy i umiejętności w zakresie konfiguracji i zarządzania sieciami wirtualnymi platformy Azure, w tym:

- Tworzenie i konfigurowanie sieci wirtualnych.
- Routing sieciowy.
- Strefy DNS.
- Ustawienia DNS.

- Sieciowe grupy zabezpieczeń.
- Zapora platformy Azure.



Program szkolenia

1. Konfiguracja sieci wirtualnych.
 - Planowanie sieci wirtualnych.
 - Tworzenie sieci wirtualnych.
 - Tworzenie podsieci.
 - Planowanie adresacji IP.
 - Tworzenie publicznego adresu IP.
 - Powiązanie publicznego adresu IP.
 - Alokacja lub przydzielanie prywatnych adresów IP.
2. Konfiguracja komunikacji równorzędnej sieci wirtualnej platformy Azure.
 - Wskazane przypadki wykorzystania komunikacji równorzędnej w sieci wirtualnej platformy Azure.
 - Wskazane przypadki wykorzystania tranzytu bramy i łączności.
 - Konfiguracja komunikacji równorzędnej sieci wirtualnej.
 - Rozszerzenie komunikacji równorzędnej za pomocą tras zdefiniowanych przez użytkownika i łączenia usług.
3. Zarządzanie i kontrolowanie przepływu ruchu we wdrożeniu platformy Azure za pomocą tras.
 - Identyfikacja możliwości routingu sieci wirtualnej platformy Azure.
 - Sieciowe urządzenie wirtualne (NVA).
4. Hostowanie domeny na platformie Azure DNS.
 - Azure DNS.
 - Konfiguracja Azure DNS do hostowania domeny.
5. Konfiguracja sieciowych grup zabezpieczeń.
 - Implementacja sieciowych grup zabezpieczeń.
 - Określenie reguły sieciowej grupy zabezpieczeń.
 - Określenie obowiązujących reguł sieciowej grupy zabezpieczeń.
 - Tworzenie reguły sieciowej grupy zabezpieczeń.
 - Implementacja grupy zabezpieczeń aplikacji.
6. Wprowadzenie do zapory platformy Azure.
 - Zapora platformy Azure.
 - Jak działa zapora platformy Azure.
 - Kiedy używać zapory platformy Azure.
 - Kiedy używać zapory platformy Azure w wersji Premium.
7. Projekt z przewodnikiem — konfiguracja bezpiecznego dostępu do obciążeń za pomocą usług sieci wirtualnej platformy Azure.
 - Ćwiczenie - Zapewnienie izolacji i segmentacji sieci dla aplikacji internetowej.

- Ćwiczenie – Kontrolowanie ruchu sieciowego do i z aplikacji internetowej.
- Ćwiczenie – Ochrona aplikacji internetowej przed złośliwym ruchem i blokowanie nieautoryzowanego dostępu.
- Ćwiczenie – Operacjonalizacja i egzekwowanie zasad filtrowania ruchu.
- Ćwiczenie – Rekordy i rozwiązywanie wewnętrznych nazw domen



Oczekiwane przygotowanie uczestnika

- Doświadczenie w korzystaniu z Azure Portal do tworzenia zasobów.
- Podstawowa wiedza na temat sieci korporacyjnych i koncepcji sieci w chmurze.
- Podstawowa wiedza na temat koncepcji bezpieczeństwa sieci, takich jak zapory ogniowe, routing i listy kontroli dostępu.



Szkolenie obejmuje

* **podręcznik** w formie elektronicznej dostępny na platformie:

<https://learn.microsoft.com/pl-pl/training/>

* dostęp do portalu słuchacza Altkom Akademii



Czas trwania

1 dni / 7 godzin

Język

- **Szkolenie:** polski
- **Materiały:** angielski