

SC-300T00 Microsoft Identity and Access Administrator

Czas trwania: 4 dni

Dla kogo:

Szkolenie skierowane do administratorów tożsamości i dostępu, którzy wykonują zadania administracyjne dotyczące zarządzania tożsamością oraz dostępem w swojej codziennej pracy.

Wymagania wstępne:

- Bardzo dobra praktyczna wiedza w zakresie bezpieczeństwa i branżowych wymagań bezpieczeństwa, takich jak dogłębna ochrona, najmniej uprzywilejowany dostęp, wspólna odpowiedzialność i model zerowego zaufania
- Znajomość pojęć dotyczących tożsamości, takie jak uwierzytelnianie, autoryzacja i usługa Active Directory
- Doświadczenie we wdrażaniu obciążeń platformy Azure.
- Doświadczenie z systemami operacyjnymi Windows i Linux oraz językami skryptowymi jest pomocne, ale nie jest wymagane.

Szkolenie przygotowuje do egzaminu:

SC-300 Microsoft Identity and Access Administrator

Zakres tematyczny:

1. **Wdrożenie rozwiązania do zarządzania tożsamością**
 - implementacja wstępnej konfiguracji usługi Azure AD
 - tworzenie, konfiguracja i zarządzanie tożsamościami
 - wdrażanie tożsamości zewnętrznych i zarządzanie nimi
 - wdrażanie tożsamości hybrydowej i zarządzanie nią
2. **Wdrożenie rozwiązania do uwierzytelniania i zarządzania dostępem**
 - zabezpieczanie użytkownika usługi Azure AD za pomocą usługi MFA
 - zarządzanie uwierzytelnianiem użytkowników
 - planowanie, wdrażanie i zarządzanie dostępem warunkowym
 - zarządzanie ochroną tożsamości w usłudze Azure AD
3. **Wdrażanie zarządzania dostępem do aplikacji**
 - planowanie i projektowanie integracji przedsiębiorstwa pod kątem SSO
 - wdrażanie i monitorowanie integracji aplikacji korporacyjnych na potrzeby logowania jednokrotnego
 - wdrożenie rejestracji aplikacji
4. **Planowanie i wdrażanie strategii zarządzania tożsamością**
 - planowanie i wdrażanie zarządzania uprawnieniami
 - planowanie, wdrażanie i zarządzanie przeglądami dostępu
 - planowanie i wdrażanie uprzywilejowanego dostępu
 - monitorowanie i utrzymanie usługi Azure AD