

Szkolenie: Microsoft
 SC-300T00 Microsoft Identity and Access Administrator


Cel szkolenia:

Szkolenie zapewnia wiedzę i umiejętności potrzebne do wdrażania rozwiązań do zarządzania tożsamościami opartych na usłudze Microsoft Azure AD i technologii połączonych tożsamości. Podczas szkolenia omówione zostaną zagadnienia z zakresu zawartości tożsamości dla usługi Azure AD, rejestracji aplikacji przedsiębiorstwa, dostępu warunkowego, zarządzania tożsamościami i innymi narzędziami tożsamości.

Po ukończeniu szkolenia, uczestnik będzie potrafił:

- Wdrażać rozwiązania do zarządzania tożsamościami
- Wdrażać rozwiązania do zarządzania uwierzytelnianiem i dostępem
- Implementować zarządzania dostępem dla aplikacji
- Zaplanować i wdrożyć swoją strategię określania tożsamości.

Grupa docelowa:

To szkolenie przeznaczone jest dla administratorów tożsamości i dostępu, którzy planują zdać odpowiedni egzamin certyfikacyjny lub którzy wykonują zadania administracyjne tożsamości i dostępu w codziennej pracy. Szkolenie jest również przydatne dla administratorów lub inżynierów, którzy chcą specjalizować się w dostarczaniu rozwiązań tożsamości i systemów zarządzania dostępem do rozwiązań opartych na platformie Azure; odgrywać integralną rolę w ochronie organizacji.

Plan szkolenia:

- Wdrażanie rozwiązania do zarządzania tożsamościami
 - Implementowanie wstępnej konfiguracji usługi Azure AD
 - Tworzenie, konfigurowanie i zarządzanie tożsamościami
 - Wdrażanie tożsamości zewnętrznych i zarządzanie nimi
 - Wdrażanie tożsamości hybrydowej i zarządzanie nią
- Wdrażanie rozwiązania do zarządzania uwierzytelnianiem i dostępem
 - Bezpieczny użytkownik usługi Azure AD za pomocą usługi MFA
 - Zarządzanie uwierzytelnianiem użytkowników
 - Planowanie, wdrażanie i administrowanie dostępem warunkowym
 - Zarządzanie ochroną tożsamości usługi Azure AD

- Implementowanie zarządzania dostępem dla aplikacji
 - Planowanie i projektowanie integracji przedsiębiorstwa dla SSO
 - Wdrażanie i monitorowanie integracji aplikacji dla przedsiębiorstw dla aplikacji SSO
 - Implementowanie rejestracji aplikacji
- Planowanie i wdrażanie strategii zarządzania tożsamością
 - Planowanie i wdrażanie zarządzania uprawnieniami
 - Planowanie, wdrażanie i zarządzanie przeglądami dostępu
 - Planowanie i wdrażanie uprzywilejowanego dostępu
 - Monitorowanie i obsługa usługi Azure AD

Wymagania:

Przed uczestnictwem w tym szkoleniu, kandydaci muszą posiadać:

- Znajomość najlepszych rozwiązań w zakresie zabezpieczeń i wymagań dotyczące zabezpieczeń w branży, takie jak dogłębna ochrona, najmniej uprzywilejowany dostęp, współużytkowana odpowiedzialność i model zerowego zaufania.
- Znajomość pojęć tożsamości, takimi jak uwierzytelnianie, autoryzacja i usługa active directory.
- Pewne doświadczenie wdrażania obciążeń platformy Azure. Szkolenie nie obejmuje podstaw administracji platformy Azure, zamiast tego zawartość szkolenia opiera się na tej wiedzy, dodając informacje specyficzne dla zabezpieczeń.
- Doświadczenie z systemami operacyjnymi Windows i Linux oraz językami skryptów są pomocne, ale nie są wymagane.

Poziom trudności



Certyfikaty:

Certyfikat ukończenia autoryzowanego szkolenia Microsoft.

Prowadzący:

Certyfikowany trener Microsoft.