

kod szkolenia: SC-300 / PL DL 4d

Microsoft Identity and Access Administrator

Autoryzowane szkolenie Microsoft Identity and Access Administrator **SC-300** szkolenie w formule Distance Learning.
Docelowa grupa odbiorców.:

- **Administrator**
- **Specjalista IT**
- **Specjalista** ds. bezpieczeństwa
- **Inżynier** ds. bezpieczeństwa

Zobacz film: <https://youtu.be/RVkfN1DyxQc>



Przeznaczenie szkolenia

Szkolenie skierowane do osób, które są zainteresowane poznaniem czym jest:

- Wdrażanie rozwiązań do zarządzania tożsamością
- Wdrażanie rozwiązań do uwierzytelniania i zarządzania dostępem
- Wdrażanie zarządzania dostępem do aplikacji
- Planowanie i wdrażanie strategii zarządzania tożsamością

Kurs SC-300 jest przeznaczony dla:

- administratorów tożsamości i dostępu, którzy planują przystąpić do powiązanego egzaminu certyfikacyjnego lub którzy wykonują zadania administracyjne związane z tożsamością i dostępem w swojej codziennej pracy.
- administratora lub inżyniera, który chce specjalizować się w dostarczaniu rozwiązań do obsługi tożsamości i systemów zarządzania dostępem do rozwiązań opartych na platformie Azure; odgrywanie integralnej roli w ochronie organizacji.



Korzyści wynikające z ukończenia szkolenia

- Implementuj rozwiązanie do zarządzania tożsamością
- Implementuj rozwiązania do uwierzytelniania i zarządzania dostępem

- Wdrażaj zarządzanie dostępem do aplikacji
- Planuj i wdrażaj strategię zarządzania tożsamością

Ten kurs zapewnia IT Identity and Access Professional, wraz z IT Security Professional, wiedzę i umiejętności potrzebne do wdrożenia rozwiązań do zarządzania tożsamością opartych na Microsoft Azure AD i połączonych technologiach tożsamości. Ten kurs obejmuje zawartość tożsamości dla usługi Azure AD, rejestrację aplikacji dla przedsiębiorstw, dostęp warunkowy, nadzór nad tożsamością i inne narzędzia do zarządzania tożsamością



Metoda egzaminowania

Egzamin w formie **on-line**. Zapis na stronie <https://home.pearsonvue.com/Clients/Microsoft.aspx>



Opis egzaminu

Po kursie **SC-300** można przystąpić do certyfikowanego egzaminu: w autoryzowanym centrum egzaminacyjnym, online będąc monitorowanym przez zewnętrznego egzaminatora. Szczegóły na <https://docs.microsoft.com/pl-pl/learn/certifications/exams/sc-300>



Oczekiwane przygotowanie słuchaczy

- Podstawowa znajomość platformy Microsoft 365
- Podstawowa wiedza na temat produktów firmy Microsoft związanych z zabezpieczeniami, zgodnością i tożsamością
- Średnio zaawansowana znajomość systemu Windows 10
- Znajomość usług platformy Azure
- Podstawowe rozumienie koncepcji skryptowych
- Pewne doświadczenie z systemami operacyjnymi Windows i Linux
- Umiejętność korzystania z anglojęzycznych materiałów
- szkolenia poprzedzające: **SC-200, AZ-900, MS-900**

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego

ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć.

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na:

<https://www.altkomakademia.pl/distance-learning/#FAQ>



Język szkolenia

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

Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie:

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

* dostęp do portalu słuchacza Altkom Akademii

Metoda szkolenia:

- teoria
- demo
- laboratoria indywidualne
- 50% teoria
- 50% praktyka

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

1: Wdrożenie rozwiązania do zarządzania tożsamością

- Zaimplementuj wstępną konfigurację usługi Azure AD
- Twórz, konfiguruj i zarządzaj tożsamościami
- Wdrażaj tożsamości zewnętrzne i zarządzaj nimi

- Wdrażaj tożsamość hybrydową i zarządzaj nią

2: Wdrożenie rozwiązania do uwierzytelniania i zarządzania dostępem

- Zabezpiecz użytkownika usługi **Azure AD** za pomocą **usługi MFA**
- Zarządzaj uwierzytelnianiem użytkowników
- Planuj, wdrażaj i zarządzaj dostępem warunkowym
- Zarządzaj ochroną tożsamości w usłudze Azure AD

3: Wdrażanie zarządzania dostępem do aplikacji

- Zaplanuj i zaprojektuj integrację przedsiębiorstwa pod kątem rejestracji jednokrotnej
- Wdrażaj i monitoruj integrację aplikacji korporacyjnych na potrzeby logowania jednokrotnego
- Wdrożenie rejestracji aplikacji

4: Planowanie i wdrażanie strategii zarządzania tożsamością

- Planuj i wdrażaj zarządzanie uprawnieniami
- Planuj, wdrażaj i zarządzaj przeglądami dostępu
- Planuj i wdrażaj uprzywilejowany dostęp
- Monitoruj i utrzymuj usługę Azure AD