CORSO SC-300

MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR

WIDEOFFICE
THE WORLD IS YOUR OFFICE

PRESENTAZIONE

L'obiettivo del corso **"SC-300 – Microsoft Identity and Access Administrator"** è fornire le conoscenze e le competenze necessarie per implementare soluzioni di **gestione delle identity basate su Microsoft Azure AD** e sulle relative tecnologie di gestione delle identità.

Questo corso descrive come **gestire le identity** per Azure AD, la **registrazione di applicazioni aziendali**, il **conditional access**, la **identity governance**.

Il contenuto di questo corso è in linea con le finalità dell'esame SC-300.

CERTIFICAZIONE

Il corso prepara all'esame **Esame SC-300: Microsoft Identity and Access Administrator**. Questo esame è parte dei requisiti per ottenere il badge **Microsoft Certified: Identity and Access Administrator Associate**.

DESTINATARI

- Cloud administrators
- IT security professionals
- Amministratori
- Tecnici

Ambito: Cloud

Vendor: Microsoft

+ Aula virtuale + one-to-one vILT + presenza in aula

Corso in italiano e materiale in inglese

Partecipanti: Min 4 Max 12

4 giorni (32 ore) 9-13/14-18

Docenti esperti Cloud Architect

Laboratorio: sì

Materiale su supporto elettronico

Attestato di partecipazione

FINALITÀ

- Configurare Azure Active Directory e personalizzare le impostazioni
- Gestire le identity interne ed esterne
- Implementare una soluzione ibrida di gestione delle identità
- Configurare e gestire l'autenticazione utente, inclusa l'MFA (autenticazione a più fattori)
- Controllare l'accesso alle risorse usando il Conditional Access
- Usare Azure AD Identity Protection per aumentare la security posture dell'organizzazione
- Registrare una nuova applicazione in Azure AD
- Pianificare e implementare l'accesso SSO per le applicazioni aziendali
- Monitorare e gestire le applicazioni aziendali
- Pianificare e implementare gli Access review
- Implementare il PIM (Privileged Identity Management)
- Concedere l'accesso agli utenti con Entitlement Management

PREPARAZIONE RACCOMANDATA

Si raccomanda a chi frequenta di avere:

- Comprensione delle tecnologie di virtualizzazione locali, tra cui: VMs, reti virtuali e hard disk virtuali.
- Comprensione delle configurazioni di rete, inclusi TCP/IP, Domain Name System (DNS), reti private virtuali (VPN), firewall e tecnologie di crittografia.
- Comprensione dei concetti di Active Directory, inclusi utenti, gruppi e controllo degli accessi basato sui ruoli.
- Comprensione della resilienza e del ripristino di emergenza, comprese le operazioni di backup e ripristino

PREZZI

Quota di partecipazione in aula: € **1.290 +IVA**

Sono disponibili sconti per partecipazioni in gruppo

Microsoft Partner

WIDEOFFICE
THE WORLD IS YOUR OFFICE

Via John F. Kennedy 7
10024 MONCALIERI (TO)
+39 011 627 2828
P.IVA IT09185850014
education@wideoffice.it
www.wideoffice.it

PROGRAMMA DEL CORSO SC-300

WIDEOFFICE
THE WORLD IS YOUR OFFICE

Modulo 1: Implementare una soluzione di gestione delle identità

- Implementare la configurazione iniziale di Azure AD
- Creare, configurare e gestire identità
- Implementare e gestire identità esterne
- Implementare e gestire l'identità ibrida
- Lab: Gestire i ruoli utente
- Lab: Impostazione delle proprietà a livello di tenant
- Lab: Assegnare le licenze agli utenti
- Lab: Ripristinare o rimuovere gli utenti eliminati
- Lab: Aggiungere gruppi in Azure AD
- Lab: Modificare le assegnazioni di licenze di gruppo
- Lab: Modificare le assegnazioni di licenze utente
- Lab: Configurare la collaborazione esterna
- Lab: Aggiungere utenti guest alla directory
- Lab: Esplorare gruppi dinamici

Modulo 2: Implementare una soluzione di gestione dell'autenticazione e degli accessi

- Proteggere l'utente di Azure AD con MFA
- Gestire l'autenticazione utente
- Pianificare, implementare e amministrare l'accesso condizionale
- Gestire Azure AD Identity Protection
- Lab: Configurare i criteri di registrazione dell'autenticazione di Azure AD MFA
- Lab: Abilitare i criteri di rischio di accesso
- Lab: Gestire i valori di blocco intelligente di Azure AD
- Lab: Configurare i controlli per le sessioni di autenticazione
- Lab: Implementare i criteri, i ruoli e le assegnazioni dell'accesso condizionale
- Lab: Usare le impostazioni predefinite per la sicurezza
- Lab: Configurare e distribuire la reimpostazione della password self-service (SSPR)
- Lab: Abilitare Azure AD MFA

Modulo 3: Implementare la gestione degli accessi per le app

- Pianificare e progettare l'integrazione di app aziendali per SSO
- Implementare e monitorare l'integrazione delle app aziendali per il Single Sign-On
- Implementare la registrazione delle app
- Lab: Implementare la gestione degli accessi per le app
- Lab: Creare un ruolo personalizzato per gestire la registrazione delle app
- Lab: Registrare un'applicazione
- Lab: Concedere a un'applicazione il consenso amministratore a livello di tenant
- Lab: Aggiungere ruoli app alle applicazioni e ricevere token

Modulo 4: Pianificare e implementare una strategia di governance delle identità

- Pianificare e implementare la gestione entitlement
- Pianificare, implementare e gestire le verifiche di accesso
- Pianificare e implementare l'accesso con privilegi
- Monitorare e gestire Azure AD
- Lab: Configurare PIM per i ruoli di Azure AD
- Lab: Assegnare un ruolo di Azure AD in PIM
- Lab: Assegnare ruoli di risorse di Azure AD in PIM
- Lab: Connettere i dati da Azure AD ad Azure Sentinel
- Lab: Creare verifiche di accesso per gruppi e app
- Lab: Gestire il ciclo di vita degli utenti esterni con la governance delle identità di Azure AD
- Lab: Aggiungere il report sull'accettazione delle condizioni per l'utilizzo
- Lab: Creare e gestire un catalogo di risorse con l'entitlement di Azure AD

SC-300 ver. 1.0