WIDEOFFICE
THE WORLD IS YOUR OFFICE

CORSO SC-300
MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR

Ambito:	Durata:	Vendor:	Modalità:
Cloud	4 giorni	Microsoft	Virtual classroom, one-to-one

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.

DESTINATARI

Questo corso è indirizzato a cloud administrator e ad IT Security Professional che intendono sostenere l'esame di certificazione associato o che eseguono attività di amministrazione delle identità e degli accessi nel proprio lavoro quotidiano. Questo corso è utile anche per un amministratore o un tecnico che vuole specializzarsi nell'offerta di soluzioni di gestione delle identità e sistemi di gestione degli accessi per soluzioni basate su Azure.

MODALITÀ FORMATIVE

Questo corso viene offerto in tre modalità:

- In aula virtuale, live con istruttore da remoto;
- One-to-one come formazione individuale, live con istruttore da remoto;
- In aula con presenza dell'istruttore (ILT) – al momento non attivabile;

Il corso è erogabile in lingua italiana e inglese ma il materiale del corso è sempre fornito in lingua inglese.

Il numero massimo di partecipanti ad un'edizione del corso è 12, il minimo per attivare il corso è 4. In ogni modalità è previsto l'accesso con un account personale al lab online e lo svolgimento di una serie di esercizi teorici e pratici.

FINALITÀ DEL CORSO

Alla fine del corso i partecipanti saranno in grado di:

- 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

DURATA E PREZZI

- Durata: 4 giorni (32 ore)
- Quota di partecipazione in aula: € 1.290+IVA
- Sono disponibili sconti per partecipazioni in gruppo;
- Per un preventivo sulla formazione one-to-one e altre opzioni contattateci

NOTE

- Salvo diversamente concordato, l'orario di svolgimento è: 09-13 / 14-18
- Periodo: schedulazione bimestrale
- Il corso viene erogato esclusivamente con docenti dotati di esperienza come Cloud Architect
- Il laboratorio (su richiesta) sarà accessibile con l'account utilizzato durante la formazione per 30 giorni dopo la fine del corso, in modo da poter preparare al meglio l'esame di certificazione. In questo periodo un docente sarà disponibile via mail o sessione remota su appuntamento.
- Il materiale didattico è realizzato da Wideoffice e viene fornito su supporto elettronico.

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.

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 DR, comprese le operazioni di backup e ripristino

NOTE INTEGRATIVE

- Non è ammesso registrare le lezioni, né audio né audio/video

SEDI DEI CORSI

- Moncalieri (Torino) – via John Kennedy, 7 – 10024 – al momento non utilizzabile
- Torino – via Val della Torre, 3 – 10149 – al momento non utilizzabile

Microsoft Partner

citrix Partner Silver Solution Advisor

ARGOMENTI

GIORNO 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 i dynamic groups

GIORNO 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

GIORNO 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

GIORNO 4

Pianificare e implementare una strategia di governance delle identità

- Pianificare e implementare la gestione degli entitlement
- Pianificare, implementare e gestire gli Access Reviews
- Pianificare e implementare l'accesso con PIM
- 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 di Azure AD ad Azure Sentinel
- Lab: Creare Access Review 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 dei Terms of Use
- Lab: Creare e gestire un catalogo di risorse con l'entitlement di Azure AD

WIDEOFFICE.IT - Via John F. Kennedy 7 - 10024 MONCALIERI (TO) - Tel. +39 011 627 28 28 - P.IVA IT09185850014 - education@wideoffice.it - www.wideoffice.it