SC-300: Microsoft Identity and Access Administrator

Introducción

En presente curso proporciona al candidato los conocimientos y las habilidades necesarias para implementar soluciones de administración de identidades basadas en Microsoft Azure AD y tecnologías de identidad conectadas.

El curso incluye contenido de identidades para Azure AD, registro de aplicaciones empresariales, acceso condicional, gobiernanza de identidades y otras herramientas de identidad.

El perfil laboral de *Microsoft Identity and Access Administrator* se encarga de diseñar, implementar y operar los sistemas de administración de acceso e identidad de una organización mediante Azure AD, realizando tareas tales como:

- Proporcionar autenticación segura y acceso de autorización a aplicaciones empresariales.
- Proporcionar experiencias perfectas y capacidades de gestión de autoservicio para todos los usuarios.
- Resolución de problemas, monitoreo y generación de informes para el entorno de identidad y acceso

Audiencia y prerequisistos

Este curso está dirigido a administradores de sistemas y a ingenieros que tengan que especializarse en proporcionar soluciones de identidad y sistemas de gestión de acceso para soluciones basadas en Azure.

Prerrequisitos

Para un mayor aprovechamiento del curso, es recomendable que el alumno tenga los siguientes conocimientos:

- Comprensión fundamental de los productos de identidad, cumplimiento y seguridad de Microsoft equivalentes a haber realizado el curso Microsoft Security, Compliance, and Identity Fundamentals.
- Mejores prácticas de seguridad y sus requisitos en la industria tales como la defensa en profundidad, el acceso con menos privilegios, la responsabilidad compartida y el modelo de confianza cero.
- Familiaridad con conceptos de identidad como autenticación, autorización y directorio activo.
- Experiencia básica en la implementación de cargas de trabajo, gestión de identidades y gobernanza en Azure. Este curso no cubre los conceptos básicos de la administración de Azure, su contenido se basa en ese conocimiento y agrega información específica de seguridad.

Se recomienda tener cierta experiencia con los sistemas operativos Windows, Linux y los lenguajes de secuencias de comandos, pero no es necesario. Los laboratorios del curso pueden usar PowerShell y la CLI.

Objetivos

Una vez finalizado el curso el alumno habrá adquirido los siguientes conocimientos y habilidades:

- Implementar una solución de gestión de identidades
- Implementar soluciones de gestión de acceso y autenticación
- Implementar la gestión de acceso para aplicaciones
- Planificar e implementar una estrategia de gobernanza de la identidad

Temario

Módulo 1: Implementar una solución de gestión de identidades

- Implementar la configuración inicial de Azure AD
- Crear, configurar y administrar identidades
- Implementar y administrar identidades externas
- Implementar y administrar la identidad híbrida

Laboratorio: Administrar roles de usuario

Laboratorio: Configuración de propiedades para todo el inquilino (tenant)

Laboratorio: Asignar licencias a usuarios

Laboratorio: Restaurar o eliminar usuarios eliminados

Laboratorio: Añadir grupos en Azure AD

Laboratorio: Cambiar asignaciones de licencias de grupo

Laboratorio: Cambiar asignaciones de licencias de usuario

Laboratorio: Configurar la colaboración externa

Laboratorio: Agregar usuarios invitados al directorio

Laboratorio: Explorar grupos dinámicos

Módulo 2: Implementar una solución de gestión de acceso y autenticación

- Proteger al usuario de Azure AD con MFA
- Gestionar la autenticación de usuarios
- Planificar, implementar y administrar el acceso condicional
- Administrar la protección de identidades de Azure AD

Laboratorio: Habilitación de Azure AD MFA

Laboratorio: Configurar e implementar el restablecimiento de contraseña de autoservicio (SSPR)

Laboratorio: Trabajar con valores predeterminados de seguridad

Laboratorio: Implementar políticas, roles y asignaciones de acceso condicional

Laboratorio: Configurar controles de sesión de autenticación

Laboratorio: Administrar los valores de bloqueo inteligente de Azure AD

Laboratorio: Habilitar la política de riesgo de inicio de sesión

Laboratorio: Configurar las políticas de registro de autenticación multifactor (MFA) de Azure AD

Módulo 3: Implementar la gestión de acceso para aplicaciones

- Planificar y diseñar la integración de la empresa para SSO
- Implementar y monitorear la integración de aplicaciones empresariales para SSO
- Implementar el registro de la aplicación

Laboratorio: Implementar la gestión de acceso para aplicaciones

Laboratorio: Crear un rol personalizado para el registro de aplicaciones de administración

Laboratorio: Registrar una aplicación

Laboratorio: Otorgar el consentimiento de administrador de todo inquilino para una aplicación

Laboratorio: Agregar roles de aplicaciones a aplicaciones y recibir tokens

Módulo 4: Planificar e implementar una estrategia de gobernanza de la identidad

- Planificar e implementar la gestión de derechos
- Planificar, implementar y administrar revisiones de acceso
- Planificar e implementar el acceso privilegiado
- Supervisar y mantener Azure AD

Laboratorio: Creación y administración de un catálogo de recursos con derechos de Azure AD

Laboratorio: Añadir informes de aceptación de los términos de uso

Laboratorio: Administrar el ciclo de vida de los usuarios externos con la gobernanza de identidades de Azure AD

Laboratorio: Crear revisiones de acceso para grupos y aplicaciones

Laboratorio: Configurar PIM para roles de Azure AD

Laboratorio: Asignar roles de Azure AD en PIM

Laboratorio: Asignar roles de recursos de Azure en PIM

Laboratorio: Conectar datos de Azure AD a Azure Sentinel

Duración y Desarrollo

25 horas teórico-practicas
Del 30 de septiembre al 4 de octubre de 9 a 14 horas
Modalidad presencial-virtual

Coste y Condiciones

Curso enmarcado en el Digital Tatent Hub. Gratuito para empresas socias de GAIA. Otro tipología de empresas pueden ponerse en contacto con dth-academy@gaia.es

Si cancelas tu inscripción con un margen mínimo de 4 días laborables previos al inicio del curso, no se aplicará ninguna penalización. En caso de cancelar tu inscripción con un margen menor a 4 días laborables, se estudiará el % de penalización aplicable. No informar, y/o no presentarse a la formación puede suponer un cargo de entre 150-300€.