The DevOps Company

Microsoft Partner

SC-300T00
Microsoft Identity and Access Administrator

Sobre este curso.

El curso Microsoft Identity and Access Administrator explora cómo diseñar, implementar y operar los sistemas de administración de identidades y acceso de una organización mediante Azure AD. Aprenda a administrar tareas, como proporcionar acceso seguro con autenticación y autorización a las aplicaciones empresariales. También aprenderá a proporcionar experiencias sencillas y funcionalidades de administración de autoservicio para todos los usuarios. Por último, aprenda a crear el acceso adaptable y la gobernanza de las soluciones de administración de identidades y acceso, lo que garantiza que puede solucionar problemas, supervisar e informar sobre su entorno. El administrador de identidades y acceso puede ser una sola persona o un miembro de un equipo más grande. Obtenga información sobre cómo este rol colabora con muchos otros roles de la organización para impulsar proyectos de identidad estratégicos. El objetivo final es proporcionar conocimientos para modernizar las soluciones de identidad, implementar soluciones de identidad híbrida e implementar la gobernanza de identidades.

Duración.

4 Días.

Perfil del público.

Este curso está pensado para los administradores de identidad y acceso que planean realizar el examen de certificación asociado o que realizan tareas de administración de identidades y acceso en su trabajo diario. Este curso también sería útil para un administrador o ingeniero que quiera especializarse en proporcionar soluciones de identidad y sistemas de administración de acceso para soluciones basadas en Azure; desempeñando un papel integral en la protección de una organización.

Requisitos previos.

Antes de asistir a este curso, los estudiantes deben tener conocimientos en:

- Procedimientos recomendados de seguridad y requisitos de seguridad del sector, como la defensa en profundidad, el acceso con privilegios mínimos, la responsabilidad compartida y el modelo de confianza cero.
- Familiarizarse con conceptos de identidad como autenticación, autorización y Active Directory.
- Tener cierta experiencia en la implementación de cargas de trabajo de Azure Este curso no cubre los conceptos básicos de la administración de Azure, sino que el contenido del curso se basa en ese conocimiento al agregar información específica de seguridad.
- Cierta experiencia con Windows y sistemas operativos Linux y lenguajes de scripting es útil, pero no es necesario. Los laboratorios del curso pueden usar PowerShell y la CLI.

Examen.

SC-300: Microsoft Identity and Access Administrator.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Temario.

Módulo 1: Exploración de la identidad y Azure AD.

En este módulo se tratarán las definiciones y los servicios disponibles para la identidad proporcionada en Azure AD para Microsoft 365. Comenzará con la autenticación, la autorización y los tokens de acceso y, a continuación, creará en soluciones de identidad completas.

- Explicación del panorama de identidades.
- Exploración de confianza cero con identidad.
- Debate sobre la identidad como un plano de control.
- Exploración de por qué tenemos identidad.
- Definición de la administración de identidades.
- Contraste de la identidad descentralizada con sistemas de identidad central.
- Debate sobre soluciones de administración de identidades.
- Explicación de Azure AD de negocio a negocio.
- Comparación de proveedores de identidades de Microsoft.
- Definición de licencias de identidad.
- Exploración de la autenticación.
- Debate sobre la autorización.
- Explicación de la auditoría en la identidad.

Al final de este módulo, podrá:

- Definición de términos de identidad comunes y explicación de cómo se usan en Microsoft Cloud.
- Exploración de herramientas de administración comunes y las necesidades de una solución de identidad.
- Revisión del objetivo de confianza cero y cómo se aplica en la nube de Microsoft.
- Exploración de los servicios de identidad disponibles en Microsoft Cloud.

Módulo 2: Implementación de la configuración inicial de Azure Active Directory.

Aprenda a crear una configuración de Azure Active Directory inicial para asegurarse de que todas las soluciones de identidad disponibles en Azure están listas para su uso. En este módulo se explora cómo crear y configurar un sistema de Azure AD.

- Configuración de la personalización de marca de empresa.
- Configuración y administración de los roles de Azure Active Directory.
- Configuración de la delegación mediante unidades administrativas.
- Análisis de permisos de rol de Azure AD.
- Configuración y administración de dominios personalizados.
- Configuración para todo el inquilino.

Ejercicios:

- Administración de roles de usuarios.
- Configuración de propiedades para todo el inquilino.

Al final de este módulo, podrá:

- Implementar la configuración inicial de Azure Active Directory.
- Crear, configurar y administrar identidades.
- Implementar y administrar identidades externas (excepto escenarios B2C).
- Implementar y administrar una identidad híbrida.

Módulo 3: Crear, configurar y administrar identidades.

El acceso a las cargas de trabajo basadas en la nube debe controlarse de forma centralizada al proporcionar una identidad definitiva para cada usuario y recurso. Puede asegurarse de que los empleados y los proveedores tengan el acceso suficiente para realizar su trabajo.

- Crear, configurar y administrar usuarios.
- Creación, configuración y administración de grupos.
- Configuración y administración del registro de dispositivos.
- Administrar licencias.
- Creación de atributos de seguridad personalizados.
- Exploración de la creación automática de usuarios.

Ejercicios:

- Asignar licencias a usuarios.
- Restaurar o quitar usuarios eliminados.
- Agregar grupos en Azure Active Directory.
- Cambiar las asignaciones de licencias de grupo.
- Cambiar las asignaciones de licencias de usuario.

Al término de este módulo, podrá:

- Crear, configurar y administrar usuarios.
- Crear, configurar y administrar grupos.
- Administrar licencias.
- Explicación de los atributos de seguridad personalizados y el aprovisionamiento automático de usuarios.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Módulo 4: Implementación y administración de identidades externas.

La posibilidad de invitar a usuarios externos a usar los recursos de Azure de la empresa es una gran ventaja, pero debe hacerlo de manera segura. Explore cómo habilitar la colaboración externa segura.

- Descripción del acceso de invitado y las cuentas de negocio a negocio.
- Administración de la colaboración externa.
- Invitación a usuarios externos, de forma individual y masiva.
- Administrar cuentas de usuario externas en Azure Active Directory.
- Administración de usuarios externos en cargas de trabajo de Microsoft 365.
- Implementación de controles de acceso entre inquilinos.
- Configuración de proveedores de identidades.
- Implementación y administración de Entra Verified ID.

Ejercicios:

- Configurar la colaboración externa.
- Agregar usuarios invitados a un directorio.
- Invitar a usuarios invitados de forma masiva.
- Explorar los grupos dinámicos.

Demostración:

- Administración de los usuarios invitados en Azure Active Directory.

Al final de este módulo, podrá:

- Administrar la configuración de colaboración externa en Azure Active Directory.
- Invitar a usuarios externos (de forma individual o masiva).
- Administrar cuentas de usuario externas en Azure Active Directory.
- Configurar proveedores de identidades (sociales y SAML/ WS-Fed).

Módulo 5: Implementación y administración de una identidad híbrida.

Crear una solución de identidad híbrida para usar su instancia local de Active Directory puede ser todo un desafío. Consulte cómo puede implementar una solución de identidad híbrida segura.

- Planificación, diseño e implementación de Azure Active Directory Connect.
- Implementación y administración de la sincronización de hash de contraseña (PHS).
- Implementación y administración de la autenticación de tránsito (PTA).
- Implementación y administración de la federación.
- Solución de errores de sincronización.
- Implementación de Azure Active Directory Connect Health.
- Administración de Azure Active Directory Connect Health.

Demostración:

- Administración de la autenticación transferida y el inicio de sesión único (SSO) de conexión directa.

Al final de este módulo, podrá hacer lo siguiente:

- Planeación, diseño e implementación de Azure Active Directory Connect (AADC).
- Administración de Azure Active Directory Connect (AADC).
- Administración de la sincronización de hash de contraseña (PHS).
- Administración de la autenticación de tránsito (PTA).
- Administración del inicio de sesión único de conexión directa (SSO de conexión directa).
- Administración de la federación excluyendo las implementaciones manuales de ADFS.
- Solución de errores de sincronización.
- Implementación y administración de Azure Active Directory Connect Health.

Módulo 6: Protección de usuarios de Azure Active Directory con Multi-Factor Authentication.

Obtenga información sobre cómo usar la autenticación multifactor con Azure AD para proteger las cuentas de usuario.

- ¿Qué es Azure AD Multi-Factor Authentication?
- Planificación de la implementación de la autenticación multifactor.
- Configuración de métodos de autenticación multifactor.

Ejercicio:

- Habilitación de Azure AD Multi-Factor Authentication.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

En este módulo, aprenderá a:

- Entender Azure AD Multi-Factor Authentication (Azure AD MFA).
- Crear un plan para implementar Azure AD MFA.
- Activar Azure AD MFA para usuarios y aplicaciones específicas.

Módulo 7: Administrar la autenticación de usuarios.

Hay varias opciones para la autenticación en Azure AD. Aprenda a implementar y administrar las autenticaciones correctas para los usuarios en función de las necesidades empresariales.

- Administrar FIDO2 y métodos de método de autenticación sin contraseña.
- Exploración de la aplicación Authenticator y tokens de OATH.
- Implementar una solución de autenticación basada en Windows Hello para empresas.
- Implementación y administración de la protección de contraseñas.
- Configuración de umbrales de bloqueo inteligente.
- Implementación de Kerberos y autenticación basada en certificados en Azure AD.
- Configuración de la autenticación de usuarios de Azure AD para máquinas virtuales.

Ejercicios:

- Configurar e implementar el autoservicio de restablecimiento de contraseña.
- Administración de los valores de bloqueo inteligente de Azure Active Directory.

Al final de este módulo, podrá:

- Administrar métodos de autenticación (FIDO2/sin contraseña)
- Implementar una solución de autenticación basada en Windows Hello para empresas
- Configurar e implementar el autoservicio de restablecimiento de contraseña
- Implementación y administración de la protección de contraseñas
- Implementación y administración de restricciones de inquilino

Módulo 8: Planificación, implementación y administración del acceso condicional.

El acceso condicional proporciona una gran granularidad de control sobre qué usuarios pueden realizar actividades concretas, acceder a recursos y garantizar que los datos y los sistemas sean seguros.

- Planificación de los valores predeterminados de seguridad.
- Planificación de directivas de acceso condicional.
- Implementación de controles y asignaciones de directivas de acceso condicional.
- Prueba de las directivas de acceso condicional y solución de problemas relacionados.
- Implementación de controles de aplicación.
- Implementación de la administración de sesiones.
- Implementación de la evaluación continua de acceso.

Ejercicios:

- Uso de los valores predeterminados de seguridad.
- Implementación de roles y asignaciones de directivas de acceso condicional.
- Configuración de los controles de sesión de autenticación.

Al final de este módulo, podrá:

- Planear e implementar los valores predeterminados de seguridad.
- Planear directivas de acceso condicional.
- Implementar controles y asignaciones de directivas de acceso condicional (destino, aplicaciones y condiciones).
- Probar las directivas de acceso condicional y solucionar los problemas relacionados.
- Implementar controles de aplicación.
- Implementar la administración de sesiones.
- Configurar umbrales de bloqueo inteligente.

Módulo 9: Administración de Azure AD Identity Protection.

La protección de la identidad de un usuario mediante la supervisión de sus patrones de uso e inicio de sesión garantizará una solución de nube segura. Explore cómo diseñar e implementar Azure AD Identity Protection.

- Revisión de los conceptos básicos de Identity Protection.
- Implementación y administración de directivas de riesgo de usuario.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado.
- Implementación de la seguridad para las identidades de carga de trabajo.
- Explorar Microsoft Defender for Identity.

Ejercicios:

- Habilitación de una directiva de riesgo de inicio de sesión.
- Configuración de la directiva de registro de autenticación multifactor de Azure Active Directory.

Al final de este módulo, podrá hacer lo siguiente:

- Implementar y administrar directivas de riesgo de usuario, de inicio de sesión y de autenticación multifactor.
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado.

Módulo 10: Implementación de la administración del acceso para recursos de Azure.

Explore cómo usar roles integrados de Azure, identidades administradas y directivas de RBAC para controlar el acceso a recursos de Azure. La identidad es la clave para proteger las soluciones.

- Asignación de roles de Azure.
- Configuración de roles personalizados de Azure.
- Creación y configuración de identidades administradas.
- Acceso a recursos de Azure con identidades administradas.
- Análisis de permisos de rol de Azure.
- Configuración de directivas de RBAC de Azure Key Vault.
- Recuperación de objetos de Azure Key Vault.
- Exploración de la administración de permisos de Entra (CloudKnox).

Al final de este módulo, podrá:

- Configuración y uso de roles de Azure en Azure AD
- Configuración de una identidad administrada y asignación a recursos de Azure.
- Análisis de los permisos de rol concedidos o heredados por un usuario.
- Configuración del acceso a los datos en Azure Key Vault mediante la directiva de RBAC.

Módulo 11: Planeación y diseño de la integración de aplicaciones empresariales para SSO.

La implementación de aplicaciones empresariales permite controlar qué usuarios pueden acceder a las aplicaciones, iniciar sesión fácilmente en las aplicaciones con inicio de sesión único y proporcionar informes de uso integrados.

- Descubrimiento de aplicaciones mediante Microsoft Defender for Cloud Apps y el informe de aplicaciones de Servicios de federación de Active Directory (AD FS).
- Configuración de conectores en aplicaciones.
- Diseño e implementación de roles de administración de aplicaciones.
- Configuración de aplicaciones SaaS integradas previamente (Galería).
- Implementación y administración de directivas para aplicaciones de OAuth.

Ejercicios:

- Implementación de la administración de acceso para aplicaciones.
- Creación de un rol personalizado para administrar el registro de aplicaciones.

Al final de este módulo, podrá:

- Descubrir aplicaciones mediante MCAS o el informe de aplicación de ADFS.
- Diseñar e implementar la administración de acceso para las aplicaciones.
- Diseñar e implementar roles de administración de aplicaciones.
- Configurar aplicaciones SaaS integradas previamente (Galería).

Módulo 12: Implementación y supervisión de la integración de aplicaciones empresariales para el inicio de sesión único.

La implementación y supervisión de las aplicaciones empresariales en las soluciones de Azure puede garantizar la seguridad. Vea cómo implementar aplicaciones locales y basadas en la nube para los usuarios.

- Implementar personalizaciones de tokens.
- Implementación y configuración de las opciones de consentimiento.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

- Integración de las aplicaciones locales con el proxy de aplicación de Azure Active Directory.
- Integración de aplicaciones SaaS personalizadas para el inicio de sesión único.
- Implementación del aprovisionamiento de usuarios de aplicaciones.
- Supervisión y auditaría del acceso a aplicaciones integradas de Azure Active Directory.
- Creación y administración de colecciones de aplicaciones.

Al final de este módulo, podrá:

- Implementar personalizaciones de tokens.
- Implementación y configuración de las opciones de consentimiento.
- Integrar las aplicaciones locales con Azure AD Application Proxy.
- Integrar las aplicaciones SaaS personalizadas para el inicio de sesión único.
- Implementar el aprovisionamiento de usuarios de aplicaciones.
- Supervisar y auditar el acceso a las aplicaciones empresariales de Azure Active Directory o el inicio de sesión en ellas.

Módulo 13: Implementación del registro de aplicaciones.

La línea de negocio que se desarrolló internamente debe registrarse en Azure AD y asignarse a los usuarios para obtener una solución segura de Azure. Explore cómo implementar el registro de aplicaciones.

- Planear la estrategia de registro de la aplicación de línea de negocio.
- Implementación de registros de aplicaciones.
- Configuración de los permisos de la aplicación.
- Implementación de la autorización de la aplicación.
- Administración y supervisión de aplicaciones con la gobernanza de aplicaciones.

Ejercicios:

- Registro de una aplicación.
- Concesión del consentimiento del administrador para todo el inquilino a una aplicación.
- Adición de roles de aplicación a tokens de aplicación y de recepción.

Al final de este módulo, podrá hacer lo siguiente:

- Planear la estrategia de registro de la aplicación de línea de negocio.
- Implementar registros de aplicaciones.
- Configuración de los permisos de la aplicación.
- Planear y configurar permisos de aplicación de varios niveles.

Módulo 14: Planificación e implementación de la administración de derechos.

Cuando usuarios nuevos o usuarios externos se unen a su sitio, es necesario asignarles rápidamente acceso a las soluciones de Azure. Explore cómo autorizar a los usuarios para que accedan a su sitio y sus recursos.

- Definición de los paquetes de acceso.
- Configuración de la administración de derechos.
- Configuración y administración de organizaciones conectadas.
- Revisión de derechos por usuario.

Ejercicios:

- Creación y administración de un catálogo de recursos con derechos de Azure AD.
- Adición del informe de aceptación de los términos de uso.
- Administración del ciclo de vida de los usuarios externos con Azure AD Identity Governance.

Al final de este módulo, podrá:

- Definir catálogos.
- Revisar paquetes de acceso.
- Planear, implementar y administrar los derechos.
- Implementar y administrar las condiciones de uso.
- Administrar el ciclo de vida de los usuarios externos en la configuración de Azure AD Identity Governance.

Módulo 15: Planeamiento, implementación y administración de la revisión de acceso.

Una vez implementada la identidad, es necesario un control adecuado con revisiones de acceso para conseguir una solución segura. Explore cómo planear e implementar revisiones de acceso.

- Planear revisiones de acceso.
- Crear revisiones de acceso para grupos y aplicaciones.
- Creación y configuración de programas de revisión de acceso.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

- Supervisar los resultados de la revisión de acceso.
- Automatizar las tareas de administración de revisiones de acceso.
- Configurar revisiones de acceso periódicas.

Al final de este módulo, podrá:

- Planear revisiones de acceso.
- Crear revisiones de acceso para grupos y aplicaciones.
- Supervisar los resultados de la revisión de acceso.
- Administrar licencias para revisiones de acceso.
- Automatizar tareas de administración para la revisión de acceso.
- Configurar revisiones de acceso periódicas.

Módulo 16: Planificación e implementación de acceso con privilegios.

Es necesario asegurarse de que los roles administrativos están protegidos y administrados para aumentar la seguridad de la solución de Azure. Explore cómo usar PIM para proteger sus datos y recursos.

- Definición de una estrategia de acceso con privilegios para usuarios administrativos.
- Configurar Privileged Identity Management para recursos de Azure.
- Planificación y configuración de grupos de acceso con privilegios.
- Análisis del historial de auditoría e informes de Privileged Identity Management.
- Crear y administrar cuentas de acceso de emergencia.

Ejercicios:

- Configuración de Privileged Identity Management para los roles de Azure Active Directory.
- Asignación de roles de Azure Active Directory en Privileged Identity Management.
- Asignación de roles de recursos de Azure en Privileged Identity Management.

Al final de este módulo, podrá:

- **D**efinir una estrategia de acceso con privilegios para usuarios administrativos (recursos, roles, aprobaciones y umbrales).
- Configuración de Privileged Identity Management para roles de Azure AD.
- Configurar Privileged Identity Management para recursos de Azure.
- Asignación de roles.
- Administrar solicitudes de PIM.
- Analizar el historial de auditorías y los informes de PIM.
- Crear y administrar cuentas de acceso de emergencia.

Módulo 17: Supervisión y mantenimiento de Azure Active Directory.

Los registros de auditoría y diagnóstico de Azure AD proporcionan una vista completa de cómo los usuarios obtienen acceso a la solución de Azure. Obtenga información sobre cómo supervisar, solucionar problemas y analizar los datos de inicio de sesión.

- Análisis e investigación de los registros de inicio de sesión para solucionar problemas de acceso.
- Revisión y supervisión de los registros de auditoría de Azure Active Directory.
- Exportación de registros a la información de seguridad de terceros y al sistema de administración de eventos.
- Análisis de libros e informes de Azure Active Directory.
- Supervisión de la posición de seguridad con la puntuación de seguridad de la identidad.

Ejercicio:

- Conexión de datos de Azure Active Directory a Microsoft Sentinel.

Al término de este módulo, sabrá hacer lo siguiente:

- Análisis e investigación de los registros de inicio de sesión para solucionar problemas de acceso.
- Revisar y supervisar los registros de auditoría de Azure AD.
- Habilitar e integrar los registros de diagnóstico de Azure AD con Log Analytics o Azure Sentinel.
- Exportación del inicio de sesión y de registros de auditoría a un SIEM (administración de eventos e información de seguridad) de terceros.
- Revisión de la actividad de Azure AD mediante Log Analytics o Azure Sentinel, excepto el uso de KQL (Lenguaje de consulta Kusto).
- Analizar libros o informes de Azure Active Directory.
- Configuración de notificaciones.