ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 28 horas

SC-300 / Microsoft Identity and Access Administrator

El curso de administrador de identidades y acceso de Microsoft explora cómo diseñar, implementar y operar los sistemas de administración de identidades y acceso de una organización mediante Microsoft Entra ID. 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.

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.

Rol de trabajo: Ingeniero de Seguridad
Preparación para el examen: SC-300

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.

Módulos

Exploración de identidades en Microsoft Entra ID

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

- Introducción
- 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 Microsoft Entra 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
- Prueba de conocimientos
- Resumen

Implementación de la configuración inicial de Microsoft Entra ID

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

- Introducción
- Configuración de la marca de empresa
- Configuración y administración de roles de Microsoft Entra
- Ejercicio de administración de roles de usuarios
- Configuración de la delegación mediante unidades administrativas
- Analizar permisos de rol de Microsoft Entra
- Configuración y administración de dominios personalizados
- Configuración para todo el inquilino
- Ejercicio: configuración de propiedades para todo el inquilino
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Crear, configurar y administrar usuarios.
- Ejercicio: Asignar licencias a usuarios
- Ejercicio: Restaurar o quitar usuarios eliminados
- Crear, configurar y administrar grupos.
- Ejercicio: Adición de grupos en Microsoft Entra ID
- Configuración y administración del registro de dispositivos
- Administrar licencias
- Ejercicio: Cambiar las asignaciones de licencias de grupo
- Ejercicio: Cambiar las asignaciones de licencias de usuario
- Creación de atributos de seguridad personalizados
- Exploración de la creación automática de usuarios

- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Descripción del acceso de invitado y las cuentas de negocio a negocio
- Administración de la colaboración externa
- Ejercicio: Configurar la colaboración externa
- Invitación a usuarios externos, de forma individual y masiva
- Ejercicio: Agregar usuarios invitados a un directorio
- Ejercicio: Invitar a usuarios invitados de forma masiva
- Demostración: administración de usuarios invitados en Microsoft Entra ID
- Administración de cuentas de usuario externas en Microsoft Entra ID
- Administración de usuarios externos en cargas de trabajo de Microsoft 365
- Ejercicio: Explorar los grupos dinámicos
- Implementación y administración de Microsoft Entra Verified ID
- Configuración de proveedores de identidades
- Implementación de controles de acceso entre inquilinos
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Planear, diseñar e implementar Microsoft Entra Connect
- Implementación y administración de la sincronización de hash de contraseña (PHS)
- Implementación y administración de la autenticación de tránsito (PTA)
- Demostración: Administración de la autenticación transferida y el inicio de sesión único (SSO) de conexión directa
- Implementación y administración de la federación
- Solución de errores de sincronización
- Implementación de Microsoft Entra Connect Health
- Administrar Microsoft Entra Health
- Prueba de conocimientos
- Resumen y recursos

Protección de usuarios de Microsoft Entra con autenticación multifactor

Obtenga información sobre cómo usar la autenticación multifactor con Microsoft Entra ID para proteger las cuentas de usuario.

- Introducción
- ¿Qué es la autenticación multifactor de Microsoft Entra?
- Planificación de la implementación de la autenticación multifactor
- Ejercicio: Habilitación de la autenticación multifactor de Microsoft Entra
- Configurar los métodos de autenticación multifactor
- Resumen

Administrar la autenticación de usuarios

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

- Introducción
- 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
- Ejercicio configurar e implementar el autoservicio de restablecimiento de contraseña
- Implementación y administración de la protección de contraseñas
- Configuración de umbrales de bloqueo inteligente
- Ejercicio: administración de valores de bloqueo inteligente de Microsoft Entra
- Implementación de Kerberos y autenticación basada en certificados en Microsoft Entra ID
- Configuración de la autenticación de usuarios de Microsoft Entra para máquinas virtuales
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Planificación de los valores predeterminados de seguridad
- Ejercicio: uso de los valores predeterminados de seguridad
- Planificación de directivas de acceso condicional
- Implementación de controles y asignaciones de directivas de acceso condicional
- Ejercicio: implementación de roles 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
- Ejercicio: configuración de los controles de sesión de autenticación
- Implementación de la evaluación continua de acceso
- Prueba de conocimientos
- Resumen y recursos

Administrar Microsoft Entra Identity Protection

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

- Introducción
- Revisión de los conceptos básicos de Identity Protection
- Implementación y administración de directivas de riesgo de usuario
- Ejercicio: Habilitación de una directiva de riesgo de inicio de sesión
- Ejercicio para configurar la directiva de registro de autenticación multifactor de Microsoft Entra
- 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
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- 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
- Explorar la Administración de permisos de Microsoft Entra
- Prueba de conocimientos
- Resumen y recursos

Implementación y configuración de Acceso global seguro de Microsoft Entra

Acceso global seguro le permite colocar la identidad como equipo selector en el acceso a la red. Use los principios de Confianza cero para proteger los datos y las aplicaciones.

- Introducción
- Exploración del acceso seguro global
- Implementación y configuración de Acceso a Internet de Microsoft Entra
- Implementación y configuración de Acceso privado de Microsoft Entra
- Exploración del uso del panel para impulsar el acceso seguro global
- Creación de redes remotas para su uso con Acceso global seguro
- Uso del acceso condicional con Acceso global seguro
- Exploración de registros y opciones de supervisión con Acceso global seguro
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- 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
- Ejercicio: Implementación de la administración de acceso para aplicaciones
- Diseño e implementación de roles de administración de aplicaciones
- Ejercicio: Creación de un rol personalizado para administrar el registro de aplicaciones
- Configuración de aplicaciones SaaS preintegradas de la galería
- Implementación y administración de directivas para aplicaciones de OAuth
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Implementar personalizaciones de tokens
- Implementación y configuración de las opciones de consentimiento
- Integrar las aplicaciones locales con Application Proxy de Microsoft Entra
- Integración de aplicaciones SaaS personalizadas para el inicio de sesión único

- Implementación del aprovisionamiento de usuarios basado en aplicaciones
- Supervisar y auditar el acceso a las aplicaciones empresariales integradas en Microsoft Entra
- Creación y administración de colecciones de aplicaciones
- Prueba de conocimientos
- Resumen y recursos

Implementación del registro de aplicaciones

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

- Introducción
- Planear la estrategia de registro de la aplicación de línea de negocio.
- Implementación de registros de aplicaciones
- Registro de una aplicación
- Configuración del permiso para una aplicación
- Concesión del consentimiento del administrador para todo el inquilino a aplicaciones
- Implementación de la autorización de la aplicación
- Ejercicio para añadir roles de aplicación a una aplicación y recibir tokens
- Administración y supervisión de aplicaciones mediante la gobernanza de aplicaciones
- Prueba de conocimientos
- Resumen y recursos

Registro de aplicaciones con Microsoft Entra ID

Explore las opciones de valor y configuración al registrar una aplicación en Microsoft Entra para asegurarse de que los datos y la infraestructura están protegidos.

- Introducción
- Planeamiento para el registro de aplicaciones
- Exploración de objetos de aplicación y entidades de servicio
- Crear registros de aplicaciones
- Configuración de la autenticación de aplicaciones
- Configurar permisos de API
- Creación de roles de aplicación
- Prueba de conocimientos
- Resumen

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.

- Introducción
- Definición de los paquetes de acceso
- Ejercicio: creación y administración de un catálogo de recursos con la administración de derechos de Microsoft Entra
- Configuración de la administración de derechos
- Ejercicio: adición del informe de aceptación de los términos de uso
- Ejercicio: administración del ciclo de vida de los usuarios externos con la gobernanza de identidades de Microsoft Entra
- Configuración y administración de organizaciones conectadas
- Revisión de derechos por usuario
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Planear revisiones de acceso

- Crear revisiones de acceso para grupos y aplicaciones
- Crear y configurar revisiones de acceso mediante programación
- Supervisar los resultados de la revisión de acceso
- Automatizar las tareas de administración de revisiones de acceso
- Configurar revisiones de acceso periódicas
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- Definición de una estrategia de acceso con privilegios para usuarios administrativos
- Configurar Privileged Identity Management para recursos de Azure
- Ejercicio de configuración de Privileged Identity Management para roles de Microsoft Entra
- Ejercicio para asignar roles de Microsoft Entra en Privileged Identity Management
- Ejercicio: asignación de roles de recursos de Azure en Privileged Identity Management
- Planeamiento 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
- Prueba de conocimientos
- Resumen y recursos

Supervisión y mantenimiento de Microsoft Entra ID

Los registros de auditoría y diagnóstico de Microsoft Entra ID proporcionan una vista enriquecida de cómo los usuarios acceden a la solución de Azure. Obtenga información sobre cómo supervisar, solucionar problemas y analizar los datos de inicio de sesión.

- Introducción
- Análisis e investigación de los registros de inicio de sesión para solucionar problemas de acceso
- Revisión y supervisión de los registros de auditoría de Microsoft Entra
- Ejercicio: conexión de datos de Microsoft Entra ID a Microsoft Sentinel
- Exportación de registros a la información de seguridad de terceros y al sistema de administración de eventos
- Análisis de libros e informes de Microsoft Entra
- Supervisión de la posición de seguridad con la puntuación de seguridad de la identidad
- Prueba de conocimientos
- Resumen y recursos

Explorar las muchas características de administración de permisos de Microsoft Entra

Mientras profundizamos en las características de Administración de permisos de Microsoft Entra, usamos el marco de detección, corrección, supervisión como guía para ayudar a ver cómo las características de administración de permisos establecidas pueden beneficiar a su organización.

- Introducción
- Una experiencia completa para todos los entornos en la nube
- Obtención de información de nivel general en el panel Administración de permisos
- Comprobación de conocimientos: Conclusiones
- Profundización en la pestaña Análisis
- Comprobación de conocimientos: Análisis
- Desarrollar una mejor comprensión de su entorno con informes

- Análisis de datos históricos con la pestaña Auditoría
- Actuar sobre los resultados con la pestaña Corrección de administración de permisos
- Comprobación de conocimientos: Corrección
- Adoptar un enfoque más proactivo para la administración con supervisión continua
- Comprobación de conocimientos: Supervisión
- Administración del acceso a la Administración de permisos de Microsoft Entra
- Resumen