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: 7 horas

AZ-2001 / Implement security through a pipeline using Azure DevOps

Esta ruta de aprendizaje le ayuda a prepararse para la evaluación Implementación de la seguridad a través de una canalización mediante Azure DevOps. Aprenda a configurar y proteger Azure Pipelines. También tendrá oportunidades para poner en práctica las aptitudes. Estas aptitudes incluyen la configuración del acceso seguro a los recursos de canalización, la configuración y la validación de permisos, la configuración de un proyecto y una estructura de repositorio, la ampliación de una canalización, la configuración de canalizaciones para usar variables y parámetros de forma segura y la administración de identidades para proyectos, canalizaciones y agentes.

Perfil del Público

Está dirigido a desarrolladores de software, ingenieros DevOps, y profesionales de seguridad que buscan integrar prácticas de seguridad en sus procesos de desarrollo y operaciones. Este curso es ideal para aquellos que desean aprender a implementar y automatizar medidas de seguridad en un pipeline de CI/CD utilizando Azure DevOps, asegurando que las aplicaciones sean seguras desde la fase de desarrollo hasta la producción. Es especialmente útil para equipos de desarrollo y operaciones que buscan mejorar la seguridad y cumplimiento sin comprometer la agilidad y eficiencia en el desarrollo de software.

Requisitos Previos

- Una suscripción de Azure. Tiene que traer su propia suscripción.
- Conocimientos básicos de Azure DevOps.
- Conocimientos básicos de conceptos de seguridad, como identidades y permisos.
- Experiencia con el uso de Azure Portal para crear recursos como Azure Key Vault y establecer permisos.

Módulos

Configuración de una estructura de proyecto y repositorio para admitir canalizaciones seguras

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de configurar una estructura de proyecto y de repositorio segura para admitir canalizaciones en Azure DevOps. En él se tratan los conceptos básicos y los procedimientos recomendados para organizar la estructura de proyecto y repositorio y mover el repositorio de seguridad fuera del proyecto de aplicación.

- Introducción
- Organización de la estructura de proyecto y repositorio
- Configuración de proyectos y repositorios seguros
- Laboratorio: Configurar una estructura de proyecto y repositorio para admitir canalizaciones seguras
- Prueba de conocimientos
- Resumen

Configuración del acceso seguro a los recursos de canalización

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de la seguridad de las canalizaciones y a proteger los recursos de canalización mediante Azure DevOps. En él se tratan conceptos básicos y procedimientos recomendados para grupos de agentes seguros, variables secretas, archivos y almacenamiento, conexiones de servicio, entornos y repositorios.

- Introducción
- Configurar grupos de agentes
- Uso de variables de secreto y grupos de variables
- Descripción de archivos seguros
- Configuración de conexiones de servicio
- Administración de entornos
- Repositorios seguros
- Laboratorio: Configurar agentes y grupos de agentes para canalizaciones seguras
- Prueba de conocimientos
- Resumen

Administración de la identidad para proyectos, canalizaciones y agentes

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de administrar la identidad de proyectos, canalizaciones y agentes en Azure DevOps. En él se tratan los conceptos básicos y los procedimientos recomendados para configurar un grupo hospedado por Microsoft, agentes para proyectos e identidades de agente y también para configurar el ámbito de una conexión de servicio y convertirlo en una identidad administrada.

- Introducción
- Configuración de un grupo hospedado por Microsoft
- Configuración de agentes para proyectos
- Configuración de identidades de agente
- Configuración del ámbito de una conexión de servicio
- Descripción y conversión en una identidad administrada
- Laboratorio: Administrar la identidad para proyectos y canalizaciones4
- Prueba de conocimientos
- Resumen

Configuración y validación de permisos

En él se tratan conceptos básicos y procedimientos recomendados para configurar y validar permisos de usuario, permisos de canalización, comprobaciones de aprobación y rama, y auditoría y administración de permisos.

- Introducción
- Configuración y validación de permisos de usuario
- Configuración y validación de permisos de canalización
- Configuración y validación de comprobaciones de aprobación y rama
- Administración y auditoría de permisos
- Laboratorio: Configurar y validar permisos
- Prueba de conocimientos
- Resumen

Extensión de una canalización para usar varias plantillas

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de extender una canalización a varias plantillas y cómo hacerlo mediante Azure DevOps. En él se tratan conceptos básicos y procedimientos recomendados para crear plantillas anidadas, volver a escribir la canalización de implementación principal, configurar la canalización y la aplicación para usar tokenización, quitar secretos de texto sin formato, restringir el registro de agentes e identificar y quitar condicionalmente las tareas de script.

- Introducción
- Creación de una plantilla anidada

- Reescritura de la canalización de implementación principal
- Configuración de la canalización y la aplicación para usar la tokenización
- Eliminación de secretos de texto sin formato9 min.
- Restricción del registro del agente
- Identificación y eliminación condicional de tareas de script
- Laboratorio: Extender una canalización para usar varias plantillas
- Prueba de conocimientos
- Resumen

Configuración del acceso seguro a Azure Repos desde canalizaciones

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de proteger el acceso a Azure Repos desde canalizaciones y cómo hacerlo mediante Azure DevOps. En él se tratan los conceptos básicos y los procedimientos recomendados para proteger el acceso a paquetes, secretos de credenciales, secretos para servicios y Azure Key Vault.

- Introducción
- Configuración del acceso con canalizaciones a paquetes
- Configuración del acceso con canalizaciones a secretos de credenciales
- Configuración del acceso con canalizaciones a secretos para servicios
- Uso de Azure Key Vault para proteger secretos
- Exploración y protección de los archivos de registro
- Laboratorio: Integrar Azure Key Vault con Azure Pipelines
- Prueba de conocimientos
- Resumen

Configuración de canalizaciones para usar variables y parámetros de forma segura

Este módulo está diseñado para ayudar a los alumnos a comprender la importancia de configurar canalizaciones para usar variables y parámetros de forma segura en Azure DevOps. En él se tratan los conceptos básicos y los procedimientos recomendados para garantizar que los parámetros y las variables conserven su tipo, identificar y restringir el uso poco seguro de parámetros y variables, mover los parámetros a un archivo YAML que proteja su tipo, limitar las variables que se pueden establecer en tiempo de cola y validar que las variables obligatorias están presentes y establecidas correctamente.

- Introducción
- Garantía de los tipos de parámetros y variables
- Identificación y restricción del uso no seguro de parámetros y variables
- Traslado de parámetros a un archivo YAML
- Limitación de las variables de tiempo en cola
- Validación de las variables obligatorias
- Laboratorio: Configurar canalizaciones para usar variables y parámetros de forma segura
- Prueba de conocimientos
- Resumen