



# AZ-1003

## Secure storage for Azure Files and Azure Blob Storage



### Información general.

En esta ruta de aprendizaje, practicará el almacenamiento de datos empresariales de forma segura mediante Azure Blob Storage y Azure Files. Las aptitudes validadas incluyen la creación de cuentas de almacenamiento, contenedores de almacenamiento y recursos compartidos de archivos. Además, la configuración del cifrado y las redes para mejorar la posición de seguridad.

### Duración.

1 Día.

### Requisitos previos.

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

- Experimentar con el uso de Azure Portal para crear recursos.
- Conocimientos básicos de datos no estructurados, como blobs y archivos.
- Conocimientos básicos de conceptos de seguridad, como identidades, permisos y cifrado.
- Conocimientos básicos de conceptos de red, como redes virtuales y subredes.

### Examen.

Applied Skills Assessment.

### Temario.

#### Módulo 1: Creación de una cuenta de Azure Storage.

Cree una cuenta de Azure Storage con las opciones que respondan a sus necesidades empresariales.

- Determinación del número de cuentas de almacenamiento necesarias.
- Elección de la configuración de la cuenta.
- Elección de una herramienta de creación de cuentas.

**Ejercicio: creación de una cuenta de almacenamiento mediante Azure Portal.**

#### Módulo 2: Configuración de Azure Blob Storage.

Descubra cómo configurar Azure Blob Storage, incluidos los niveles y la replicación de objetos.

- Implementación de Azure Blob Storage.
- Creación de contenedores de blobs.
- Asignación de niveles de acceso de blob.
- Adición de reglas de administración del ciclo de vida de los blobs.
- Determinación de la replicación de objetos de blob.
- Cargar blobs.
- Determinación de los precios de Blob Storage.

#### Módulo 3: Configurar la seguridad de Azure Storage.

Aprenda a configurar características comunes de seguridad de Azure Storage, como las firmas de acceso al almacenamiento.

- Revisión de las estrategias de seguridad de Azure Storage.
- Creación de firmas de acceso compartido.
- Identificación de parámetros de URI y SAS.



- Determinación del cifrado de Azure Storage.
- Creación de claves administradas por el cliente.
- Aplicar procedimientos recomendados de seguridad para Azure Storage.

#### **Módulo 4: Protección y aislamiento del acceso a recursos de Azure mediante grupos de seguridad de red y puntos de conexión de servicio.**

Los grupos de seguridad de red y los puntos de conexión de servicio ayudan a proteger las máquinas virtuales y los servicios de Azure contra el acceso de red no autorizado.

- Uso de grupos de seguridad de red para controlar el acceso a la red.
- Protección del acceso de red a servicios PaaS mediante puntos de conexión de servicio de red virtual.

##### **Ejercicios:**

- Creación y administración de grupos de seguridad de red.
- Restricción del acceso a Azure Storage mediante puntos de conexión de servicio.

#### **Módulo 5: Azure Files y Azure Blobs (Proyecto guiado).**

En este módulo, practicará el almacenamiento de datos empresariales de forma segura mediante Azure Blob Storage y Azure Files. El laboratorio combina aprendizaje y práctica.

##### **Ejercicios:**

- Provisión de almacenamiento para las pruebas y el entrenamiento del departamento de TI.
- Provisión de almacenamiento para el sitio web público.
- Provisión de almacenamiento privado para documentos internos de la empresa.
- Provisión de almacenamiento de archivos compartidos para las oficinas de la empresa.
- Provisión de almacenamiento para una nueva aplicación de empresa.

