



# AZ-802T00

## Administer Windows Server



### Información general.

Este curso enseña a los profesionales de TI cómo desplegar, gestionar, asegurar y solucionar cargas de trabajo de Windows Server en entornos locales, híbridos y en la nube. El curso abarca Active Directory Domain Services, máquinas virtuales Hyper-V y Azure, redes locales e híbridas, almacenamiento y servicios de archivos, endurecimiento de la seguridad de Windows Server y monitorización y resolución de problemas. Destaca herramientas y tecnologías administrativas como Windows Admin Center, PowerShell, Azure Arc, Azure Monitor, Azure Update Manager y Microsoft Defender for Cloud.

### Duración.

5 Días.

### Perfil del público.

Este curso está dirigido a administradores de Windows Server que despliegan, implementan, gestionan y solucionan problemas de Windows Server como carga de trabajo en entornos locales, en la nube o híbridos. Los candidatos administran identidad, seguridad, computación, redes, almacenamiento y monitorización para Windows Server, y normalmente colaboran con arquitectos, administradores e ingenieros. Los candidatos deben tener experiencia administrando Windows Server utilizando tecnologías como Windows Admin Center, Hyper-V, PowerShell, Azure Arc, Azure Monitor, Azure Update Manager y Microsoft Defender for Cloud, y estar familiarizados con Active Directory Domain Services (AD DS).

### Examen.

AZ-802: Administering Windows Server.

### Temario.

#### **Ruta de aprendizaje: Implementación y administración de Active Directory Domain Services.**

Aprenda a implementar y administrar controladores de dominio de Active Directory Domain Services (AD DS), crear y administrar entidades de seguridad, configurar entornos de varios sitios, varios dominios y varios bosques, e implementar directivas de grupo basadas en dominios.

#### **Módulo 1: Implementación y administración de controladores de dominio de Active Directory Domain Services.**

Este módulo le presenta la topología de los controladores de dominio dentro de un entorno de Active Directory. También le inicia en la ruta de implementación, administración y migración de un controlador de dominio entre servidores.

- Definición de Active Directory Domain Services.
- Definición de bosques y dominios de Active Directory Domain Services.
- Implementación de controladores de dominio de Active Directory Domain Services.
- Migración de un controlador de dominio a un nuevo sitio.
- Administración de maestros de operaciones de Active Directory Domain Services.



## Módulo 2: Implementación y administración de controladores de dominio de Active Directory IaaS en Azure.

En este módulo, aprenderá a extender un entorno de Active Directory existente a Azure colocando máquinas virtuales IaaS configuradas como controladores de dominio en una subred de red virtual (VNet) de Azure especialmente configurada.

- Selección de una opción para implementar servicios de directorio e identidad mediante Active Directory Domain Services en Azure.
- Implementación y configuración de controladores de dominio de AD DS en máquinas virtuales de Azure.
- Instalación de un controlador de dominio de Active Directory de réplica en una máquina virtual de Azure.
- Instalación de un nuevo bosque de Active Directory en una VNet de Azure.

## Módulo 3: Administración de controladores de dominio de AD DS y roles FSMO.

Obtenga información sobre las tareas esenciales de administración y mantenimiento de los controladores de dominio de AD DS, incluida su implementación, copia de seguridad y recuperación, y administración del esquema. Conozca las consideraciones de diseño para el número, las funciones y la ubicación óptimos de los controladores de dominio.

- Implementación de controladores de dominio de AD DS.
- Mantenimiento de controladores de dominio de AD DS.
- Administración del rol de Catálogo global de AD DS.
- Administración de maestros de operaciones de AD DS.
- Administración del esquema de AD DS.

## Módulo 4: Creación y administración de objetos de Active Directory.

Este módulo se centra en las tareas asociadas a la creación y administración de objetos de Active Directory y controladores de dominio de servicios de dominio de AD.

- Definición de usuarios, grupos y equipos.
- Definición de unidades organizativas.
- Administración de objetos y sus propiedades en Active Directory.
- Creación de objetos en Active Directory.

- Configuración de objetos en Active Directory.
- Realización de tareas de administración masiva para cuentas de usuario.
- Mantenimiento de controladores de dominio de Active Directory Domain Services.

## Módulo 5: Implementación de identidad híbrida con Windows Server.

En este módulo, aprenderá a configurar un entorno de Azure para que se admitan las cargas de trabajo de IaaS de Windows que requieren Active Directory. También aprenderá a integrar el entorno de Active Directory Domain Services (AD DS) local en Azure.

- Selección de un modelo de integración de Microsoft Entra.
- Planificación de la integración de Microsoft Entra.
- Preparación del entorno local de Active Directory para la sincronización de directorios.
- Instalación y configuración de la sincronización de directorios con Microsoft Entra Connect.
- Implementación del inicio de sesión único de conexión directa.
- Habilitación del inicio de sesión de Microsoft Entra para máquinas virtuales Windows en Azure.
- Descripción de Microsoft Entra Domain Services.
- Implementación y configuración de Microsoft Entra Domain Services.
- Administración de Windows Server en un entorno de Microsoft Entra Domain Services.
- Creación y configuración de una instancia de Microsoft Entra Domain Services.
- Unión de una máquina virtual de Windows Server a un dominio administrado.

## Módulo 6: Creación y configuración de objetos de directiva de grupo en Active Directory.

Este módulo se centra en los objetos de directiva de grupo, incluido su uso para aplicar una directiva de contraseñas específica y en todo el dominio.

- Definición de objetos de directiva de grupo.
- Implementación del alcance y la herencia de los objetos de directiva de grupo.





- Definición de objetos de directiva de grupo basados en dominio.
- Creación y configuración de un objeto de directiva de grupo basado en dominio.
- Configuración de una directiva de contraseña de dominio.
- Configuración y aplicación de una directiva de contraseña específica.

## **Módulo 7: Implementación de objetos de directiva de grupo.**

Aprenda a implementar objetos de directiva de grupo (GPO) en Active Directory Domain Services (AD DS).

- Definición de GPO.
- Implementación del alcance y la herencia de los GPO.
- Definición de GPO basados en dominios.
- Creación y configuración de un GPO basado en dominios.
- Definición del almacenamiento de GPO.
- Definición de plantillas administrativas.

## **Módulo 8: Administración de características avanzadas de AD DS.**

Aprenda sobre tareas de administración avanzadas de AD DS, incluida la creación de relaciones de confianza, la implementación de bosques de entorno administrativo de seguridad mejorada (ESAE), la supervisión y solución de problemas de replicación de AD DS y la creación de particiones personalizadas de AD DS.

- Creación de relaciones de confianza.
- Implementación de bosques ESAE.
- Supervisión y solución de problemas de AD DS.
- Creación de particiones de AD DS personalizadas.

## **Ruta de aprendizaje: Administración de instancias y cargas de trabajo de Windows Server en un entorno híbrido.**

Aprenda a configurar la administración remota de servidores Windows mediante Windows Admin Center, PowerShell, SSH y Escritorio remoto, y a administrar las cargas de trabajo de Windows Server mediante Azure Arc, Azure Update Manager y Azure Automation.

## **Módulo 9: Administración y gestión remota de máquinas virtuales IaaS de Windows Server.**

Usted es capaz de utilizar herramientas y técnicas adecuadas para administrar de forma remota máquinas virtuales de IaaS con Windows. También podrá restringir las conexiones administrativas a dichas máquinas virtuales.

- Selección de la herramienta de administración remota adecuada.
- Administración de máquinas virtuales de Windows con Azure Bastion.
- Creación de un host de Azure Bastion.
- Configuración de la administración justo a tiempo.

## **Módulo 10: Descripción de las herramientas de administración de Windows Server.**

Seleccione la herramienta de administración de Windows Server más adecuada para una situación determinada y aprenda a usarla.

- Exploración de Windows Admin Center.
- Uso del Administrador del servidor.
- Lista de herramientas de administración remota del servidor.
- Uso de Windows PowerShell.
- Uso de Windows PowerShell para administrar de forma remota un servidor.

## **Módulo 11: Administración necesaria en Windows Server.**

Optimice la administración de los entornos de Windows Server con Just Enough Administration (JEA). Limite las operaciones con privilegios a un conjunto de cmdlets, parámetros y variables de PowerShell especificados, y limite qué usuarios pueden conectarse a los puntos de conexión de JEA.

- Explicación del concepto de Just Enough Administration (JEA).
- Definición de las funciones de rol para un punto de conexión JEA.
- Creación de un archivo de configuración de sesión para registrar un punto de conexión JEA.
- Descripción de cómo funcionan los puntos de conexión JEA para limitar el acceso a una sesión de PowerShell.
- Creación y conexión a un punto de conexión JEA.

**Demostración: Conexión a un punto de conexión JEA.**

## **Módulo 12: Realización de administración segura de Windows Server.**

Comprenda el principio de privilegios mínimos, sepa cuándo usar estaciones de trabajo de acceso privilegiado y sea capaz de identificar cuentas con privilegios integradas.

- Definición de la administración con privilegios mínimos.
- Implementación de privilegios delegados.
- Uso de estaciones de trabajo de acceso privilegiado.
- Uso de servidores de salto.

## **Módulo 13: Uso de técnicas avanzadas de comunicación remota de Windows PowerShell.**

Este módulo cubre algunas técnicas avanzadas útiles que ayudan a superar las limitaciones de la comunicación remota básica de Windows PowerShell.

- Revisión de las técnicas comunes de comunicación remota de Windows PowerShell.
- Envío de parámetros a equipos remotos en Windows PowerShell.
- Configuración de protección de acceso a variables, alias y funciones mediante el modificador de ámbito.
- Habilitación de la comunicación remota de saltos múltiples en Windows PowerShell.

## **Módulo 14: Administración de uno o varios equipos mediante la comunicación remota de Windows PowerShell.**

En este módulo se explica cómo usar la comunicación remota para realizar la administración en equipos remotos.

- Revisión de la característica de comunicación remota de Windows PowerShell.
- Comparación de la comunicación remota con la conectividad remota.
- Revisión de la característica de seguridad de comunicación remota de Windows PowerShell.
- Habilitación de la comunicación remota con Windows PowerShell.

- Uso de la comunicación remota uno a uno y de uno a varios mediante Windows PowerShell.
- Comparación de la salida remota con la salida local.

## **Módulo 15: Administración de cargas de trabajo híbridas con Azure Arc.**

Aprenderá a describir Azure Arc, a implementar Azure Arc con instancias de servidor locales, a implementar políticas de Azure con Azure Arc y a utilizar el control de acceso basado en roles (RBAC) para restringir el acceso a los datos de Log Analytics.

- Descripción de Azure Arc.
- Incorporación de instancias de Windows Server.
- Conexión de máquinas híbridas a Azure desde Azure Portal.
- Uso de Azure Arc para administrar instancias de Windows Server.
- Restricción de acceso con RBAC.

## **Módulo 16: Administración de actualizaciones de Azure.**

Administre las actualizaciones del sistema operativo para las máquinas virtuales de Azure y los servidores habilitados para Azure Arc mediante Azure Update Manager.

- Descripción de Azure Update Manager.
- Preparación de las máquinas para Azure Update Manager.
- Implementación de actualizaciones.
- Evaluación de las actualizaciones.
- Administración de actualizaciones a escala.

## **Módulo 17: Automatización de la configuración de máquinas virtuales IaaS de Windows Server.**

Aprenda a implementar extensiones de configuración de estado deseado (DSC), implementarlas para remediar servidores no conformes y utilizar la extensión de script personalizado.

- Descripción de Azure Automation.
- Implementación de Azure Automation con DSC.
- Corrección de servidores que no cumplen las normas.
- Descripción de las extensiones de script personalizadas.
- Configuración de una máquina virtual mediante DSC.





## **Módulo 18: Aplicación de la configuración de seguridad de las máquinas virtuales con Azure Machine Configuration.**

Audite y aplique la configuración de seguridad del sistema operativo en MVs de Azure y servidores habilitados para Arc mediante Azure Machine Configuration. Aplique directivas de línea base de seguridad de Windows y Linux integradas, configure los modos de auditoría y cumplimiento, y cree configuraciones de máquinas personalizadas para requisitos de seguridad específicos de la organización.

- Exploración de las funciones y los modos de extensión de Azure Machine Configuration.
- Aplicación de directivas de línea base de seguridad integradas.
- Creación y asignación de configuraciones de máquinas personalizadas.

## **Módulo 19: Exploración de Azure Automation con DevOps.**

Aprenda a implementar Azure Automation con DevOps mediante runbooks, webhooks y flujos de trabajo de PowerShell. Comprenda cómo crear cuentas de automatización, administrar recursos compartidos, integrarse con sistemas de control de código fuente y planificar la administración de la nube híbrida en Azure y entornos locales.

- Creación de cuentas de automatización.
- ¿Qué es un runbook?.
- Comprensión de los recursos compartidos de automatización.
- Exploración de la galería de runbooks.
- Examen de los webhooks.
- Exploración de la integración del control de código fuente.
- Exploración de los flujos de trabajo de PowerShell.
- Creación de un flujo de trabajo.
- Exploración de la administración híbrida.
- Examen de los puntos de control y el procesamiento paralelo.

## **Ruta de aprendizaje: Administración de MVs.**

Aprenda a administrar máquinas virtuales invitadas y Hyper-V, lo que incluye la configuración, las redes, la replicación y la alta disponibilidad, y a administrar máquinas virtuales con Windows Server en Azure, lo que incluye la configuración de almacenamiento, capacidad, disponibilidad y redes.

## **Módulo 20: Configuración y administración de máquinas virtuales de Hyper-V.**

Obtenga información sobre cómo configurar y administrar máquinas virtuales de Hyper-V en Windows Server.

- Lista de las versiones de configuración de las máquinas virtuales.
- Lista de las versiones de generación de las máquinas virtuales.
- Lista de los tipos y formatos de VHD disponibles.
- Creación y configuración de máquinas virtuales.
- Determinación de las opciones de almacenamiento para las máquinas virtuales.
- Definición de VHD y conjuntos de VHD compartidos.
- Implementación de clústeres invitados con VHDX compartido.

## **Módulo 21: Configuración y administración de Hyper-V.**

Obtenga información sobre la virtualización y el rol Microsoft Hyper-V en Windows Server. Conozca las prácticas recomendadas para preparar hosts de Hyper-V, además de las características de redes de Hyper-V y la implementación de la virtualización anidada.

- Definición de Hyper-V.
- Definición de Administrador de Hyper-V.
- Configuración de hosts de Hyper-V mediante procedimientos recomendados.
- Configuración de redes de Hyper-V.
- Evaluación de las funciones de red avanzadas de Hyper-V.
- Definición de virtualización anidada.

## **Módulo 22: Protección de cargas de trabajo de Hyper-V.**

Obtenga información sobre cómo proteger las cargas de trabajo de Hyper-V en Windows Server, instalar y configurar el Servicio de protección de host (HGS), los modos de atestación disponibles con HGS y la creación e implementación de máquinas virtuales (VM) blindadas.

- Definición de tejido protegido.
- Definición de Servicio de protección de host.
- Exploración de la atestación de confianza mediante TPM.
- Definición de KPS.
- Determinación de las características clave de las MVs blindadas.

- Comparación de las máquinas virtuales con cifrado compatible y las protegidas en un tejido protegido.
- Implementación de una máquina virtual blindada.

### **Módulo 23: Implementación de alta disponibilidad de máquinas virtuales de Windows Server.**

Obtenga información sobre la funcionalidad principal, los beneficios, los casos de uso y la implementación de máquinas virtuales (VM) de Microsoft Hyper-V de alta disponibilidad en Windows Server.

- Selección de opciones de alta disponibilidad para Hyper-V.
- Consideración del equilibrio de carga de red para máquinas virtuales Hyper-V.
- Implementación de la migración en vivo de máquinas virtuales Hyper-V.
- Implementación de la migración de almacenamiento de máquinas virtuales Hyper-V.

### **Módulo 24: Ejecución de contenedores en Windows Server.**

Obtenga información sobre los contenedores de Hyper-V y Windows Server, los modos de aislamiento asociados, la ejecución de contenedores y la preparación del host de Windows Server para ejecutar cargas de trabajo en contenedores. Conozca Docker, la preparación de Windows Server para ejecutar cargas de trabajo de contenedores y la administración de contenedores.

- Definición de contenedores.
- Lista de diferencias entre contenedores y máquinas virtuales.
- Definición de contenedores de Windows Server y Hyper-V y modos de aislamiento.
- Exploración de Docker.
- Preparación de un host de Windows Server 2019 para la implementación de contenedores.
- Seguridad, almacenamiento y redes con contenedores de Windows.

### **Módulo 25: Planificación e implementación de máquinas virtuales IaaS de Windows Server.**

Usted es capaz de describir la informática y el almacenamiento de Azure en relación con las máquinas virtuales de Azure, e

implementar máquinas virtuales de Azure mediante Azure Portal, la CLI de Azure o plantillas.

- Descripción de los procesos de Azure.
- Descripción del almacenamiento en máquinas virtuales.
- Implementación de máquinas virtuales de Azure.
- Creación de una máquina virtual de Windows mediante el portal.
- Creación de una máquina virtual de Windows mediante la CLI de Azure.
- Implementación de máquinas virtuales de Azure mediante plantillas.
- Descripción de opciones de optimización de administración adicionales.

### **Módulo 26: Implementación de escalado y alta disponibilidad con máquinas virtuales de Windows Server.**

Aprenda a implementar el escalado para conjuntos de escalado de máquinas virtuales y máquinas virtuales con equilibrio de carga. Además, aprenda a implementar Azure Site Recovery.

- Descripción de conjuntos de escalado de máquinas virtuales.
- Implementación de escalado.
- Implementación de máquinas virtuales con equilibrio de carga.
- Creación de un conjunto de escalado de máquinas virtuales en Azure Portal.
- Descripción de Azure Site Recovery.
- Implementación de Azure Site Recovery.

### **Módulo 27: Implementación de direccionamiento IP y enrutamiento de máquinas virtuales IaaS de Windows Server.**

En este módulo, aprenderá a administrar redes virtuales (VNETs) de Microsoft Azure y la configuración de direcciones IP para máquinas virtuales (VM) de infraestructura como servicio (IaaS) de Windows Server.

- Implementación de una red virtual.
- Implementación del direccionamiento IP de la máquina virtual IaaS.
- Asignación y administración de direcciones IP.





- Configuración de una dirección IP privada para una máquina virtual mediante Azure Portal.
- Creación de una máquina virtual con una dirección IP pública estática mediante Azure Portal.
- Implementación de enrutamiento IP en una máquina virtual de IaaS.
- Implementación de IPv6 para máquinas virtuales de IaaS de Windows Server.

## Módulo 28: Implementación de seguridad de red de máquinas virtuales IaaS de Windows Server.

En este módulo, se centrará en cómo mejorar la seguridad de la red para las máquinas virtuales (VM) de infraestructura como servicio (IaaS) de Windows Server y cómo diagnosticar problemas de seguridad de la red con esas máquinas virtuales.

- Implementación de grupos de seguridad de red y máquinas virtuales de Windows IaaS.
- Implementación de Azure Firewall y máquinas virtuales de Windows IaaS.
- Implementación de Windows Firewall con máquinas virtuales de Windows Server IaaS.
- Elección de la solución de filtrado adecuada.
- Implementación y configuración del firewall de Azure mediante Azure Portal.
- Captura del tráfico de red con Network Watcher.
- Registro del tráfico de red hacia y desde una máquina virtual mediante Azure Portal.

## Módulo 29: Administración y gestión remota de máquinas virtuales IaaS de Windows Server.

Usted es capaz de utilizar herramientas y técnicas adecuadas para administrar de forma remota máquinas virtuales de IaaS con Windows. También podrá restringir las conexiones administrativas a dichas máquinas virtuales.

- Selección de la herramienta de administración remota adecuada.
- Administración de máquinas virtuales de Windows con Azure Bastion.
- Creación de un host de Azure Bastion.
- Configuración de la administración justo a tiempo.

## Ruta de aprendizaje: Implementación y administración de una infraestructura de red local e híbrida.

Aprenda a implementar la resolución de nombres local e híbrida, incluida la integración de DNS con Active Directory, zonas DNS, reenvío, directivas y DNSSEC, y administrar el direccionamiento IP mediante DHCP en escenarios locales e híbridos.

## Módulo 30: Implementación de DNS de Windows Server.

Aprenda a implementar y configurar la resolución de nombres con el DNS de Windows Server.

- Explora la arquitectura DNS.
- Trabajo con zonas y registros DNS.
- Instalar y configurar el rol DNS.
- Implementar el reenvío DNS.

## Módulo 31: Implementación de DNS para máquinas virtuales IaaS de Windows Server.

En este módulo, aprenderá a configurar DNS para máquinas virtuales IaaS de Windows Server, elegir la solución de DNS adecuada para las necesidades de su organización y ejecutar un servidor DNS en una máquina virtual IaaS de Azure de Windows Server.

- Entender Azure DNS.
- Implementar Azure DNS.
- Crea una zona DNS Azure y un registro usando el portal Azure.
- Implementar DNS con máquinas virtuales Azure IaaS.
- Implementar DNS de horizonte dividido en Azure.
- Solucionar problemas DNS.

## Módulo 32: Protección de DNS de Windows Server.

Aprenda a proteger DNS de Windows Server para ayudar a proteger la infraestructura de resolución de nombres de la red y también aprenda a implementar directivas DNS.

- Implementar DNS de horizonte dividido.
- Crear políticas DNS.
- Implementar políticas DNS.

- DNS seguro de Windows Server.
- Implementar DNSSEC.

### Módulo 33: Implementación y administración de DHCP.

Aprenda a implementar la configuración IP automática con el Protocolo de configuración dinámica de host (DHCP) en Windows Server 2019.

- Utiliza DHCP para simplificar la configuración de IP.
- Instalar y configurar el rol DHCP.
- Configurar opciones DHCP.
- Configurar los ámbitos DHCP.
- Selecciona opciones de alta disponibilidad DHCP.
- Implementar conmutación por error DHCP.

### Módulo 34: Implementación de la administración de direcciones IP.

Aprenda a implementar IPAM para ayudar a administrar los servidores DHCP y DNS de su organización y para administrar el espacio de direcciones IP.

- Definir la gestión de direcciones IP.
- Despliegue de la gestión de direcciones IP.
- Administrar la gestión de direcciones IP.
- Configurar opciones de gestión de direcciones IP.
- Gestionar zonas DNS con Gestión de Direcciones IP.
- Gestionar servidores DHCP con gestión de direcciones IP.
- Utiliza la Gestión de Direcciones IP para gestionar la direccionamiento IP.

### Módulo 35: Implementación de direccionamiento IP y enrutamiento de máquinas virtuales IaaS de Windows Server.

En este módulo, aprenderá a administrar redes virtuales (VNets) de Microsoft Azure y la configuración de direcciones IP para máquinas virtuales (VM) de infraestructura como servicio (IaaS) de Windows Server.

- Implementar una red virtual.
- Implementar direccionamiento IP de VM IaaS.
- Asignar y gestionar direcciones IP.

- Configura una dirección IP privada para una máquina virtual usando el portal de Azure.
- Crea una máquina virtual con una dirección IP pública estática usando el portal de Azure.
- Implementar enrutamiento IP de máquinas virtuales IaaS.
- Implementar IPv6 para máquinas virtuales IaaS de Windows Server.

### Ruta de aprendizaje: Administración de servicios de archivos y almacenamiento.

Aprenda a configurar y administrar Azure Files y Azure File Sync, administrar recursos compartidos de archivos de Windows Server, incluidos DFS y SMB a través de QUIC, y configurar el almacenamiento de Windows Server, incluidos Storage Spaces, Storage Spaces Direct, Storage Replica, Data Deduplication e iSCSI.

### Módulo 36: Implementación de una infraestructura de servidor de archivos híbrida.

En este módulo, aprenderá a implementar Azure File Sync, migrar desde DFS y usar Storage Migration Services para migrar servidores de archivos a Azure.

- Describe los servicios de archivos de Azure.
- Configurar archivos Azure.
- Configurar la conectividad a Azure Files.
- Describe Azure File Sync.
- Implementar Azure File Sync.
- Despliega Azure File Sync y Azure File Sync 2.
- Gestionar la estratificación en la nube.
- Migrar de DFSR a Azure File Sync.

### Módulo 37: Administración de servidores de archivos de Windows Server.

Obtenga información sobre la funcionalidad principal de la función de servidor de archivos de Windows Server y cómo configurar y administrar esa funcionalidad principal.

- Defina el sistema de archivos de Windows Server.
- Enumera los beneficios y usos del Gestor de Recursos de Servidor de Archivos.
- Defina la PYME y sus consideraciones de seguridad.





- Configurar el protocolo SMB.
- Definir el servicio de copia en sombra de volumen.

### **Módulo 38: Implementación de Espacios de almacenamiento y Espacios de almacenamiento directo.**

Obtenga información sobre la funcionalidad principal, las ventajas, los casos de uso y la implementación de Storage Spaces y Storage Spaces Direct en Windows Server.

- Definir la arquitectura de los Espacios de Almacenamiento y sus componentes.
- Enumera las funcionalidades, beneficios y casos de uso de los Espacios de Almacenamiento.
- Implementar espacios de almacenamiento.
- Enumera las funcionalidades, componentes, beneficios y casos de uso de Storage Spaces Direct.
- Implementar Storage Spaces Direct.

### **Módulo 39: Implementación de deduplicación de datos de Windows Server.**

Obtenga información sobre la funcionalidad principal, las ventajas, los casos de uso y la implementación de la deduplicación de datos en Windows Server.

- Definir la arquitectura, los componentes y la funcionalidad de la Deduplicación de Datos.
- Definir los casos de uso e interoperabilidad de la deduplicación de datos.
- Implementar la deduplicación de datos.
- Gestionar y mantener la deduplicación de datos.

### **Módulo 40: Implementación de iSCSI de Windows Server.**

Obtenga información sobre la funcionalidad principal, las ventajas, los casos de uso y la implementación de la interfaz de sistemas de computadoras pequeñas de Internet (iSCSI) en Windows Server 2019.

- Enumera las funcionalidades, componentes y casos de uso de iSCSI.
- Enumera las consideraciones para implementar iSCSI.

- Implementar iSCSI.
- Configurar alta disponibilidad para iSCSI.

### **Módulo 41: Implementación de réplica de almacenamiento de Windows Server.**

Obtenga información sobre la funcionalidad principal, las ventajas, los casos de uso y la implementación de la réplica de almacenamiento en Windows Server.

- Enumera las funcionalidades y componentes de Réplica de Almacenamiento.
- Examina los requisitos previos para implementar Storage Replica.
- Implementa la réplica de almacenamiento usando el Centro de Administración de Windows.
- Implementa la réplica de almacenamiento usando Windows PowerShell.

### **Ruta de aprendizaje: Infraestructura segura de Windows Server.**

Aprenda a proteger el sistema operativo Windows Server mediante Exploit Protection, Windows Defender Application Control, Credential Guard, líneas base de seguridad de OSConfig, LAPS y Microsoft Defender for Servers, y asegure los servicios de dominio de Active Directory, incluidas las políticas de contraseñas, la protección de contraseñas de Microsoft Entra y el refuerzo de los controladores de dominio.

### **Módulo 42: Endurecimiento de Windows Server.**

Aprenda a reforzar la configuración de seguridad del entorno de su sistema operativo Windows Server. Proteja el acceso administrativo a las estaciones de trabajo de acceso privilegiado (PAW), aplique líneas base de seguridad y asegure los controladores de dominio y el tráfico SMB.

- Describe la solución local de administrador de contraseñas.
- Configurar estaciones de trabajo de acceso privilegiado.
- Controladores de dominio seguros.
- Analizar la configuración de seguridad con Security Compliance Toolkit.
- Tráfico seguro para pymes.

### **Módulo 43: Administración de Microsoft Defender para Endpoints.**

Este módulo explora el uso de Microsoft Defender para punto de conexión para proporcionar protección adicional y monitorear dispositivos frente a amenazas.

- Explora Microsoft Defender para Endpoint.
- Examina las principales capacidades de Microsoft Defender para Endpoint.
- Explora el Control de Aplicaciones y la Protección de Dispositivos de Windows Defender.
- Explora Microsoft Defender Application Guard.
- Examinar Windows Defender Exploit Guard.
- Explora Windows Defender System Guard.

### **Módulo 44: Administración de Microsoft Defender en el cliente de Windows.**

Este módulo explica las características de seguridad integradas en los clientes de Windows y cómo implementarlas usando directivas.

- Explora el Centro de Seguridad de Windows.
- Explorar Windows Defender Credential Guard.
- Gestionar el antivirus Microsoft Defender.
- Gestionar el cortafuegos de Windows Defender.
- Explora el cortafuegos de Windows Defender con seguridad avanzada.

### **Módulo 45: Comprensión de la configuración de seguridad de directivas de grupo de Active Directory.**

Aprenda qué hace cada directiva de seguridad de directiva de grupo, en qué escenario del mundo real se aplica y cómo configurar, auditar y administrar configuraciones de seguridad a gran escala en entornos de Active Directory.

- Configurar políticas de cuenta.
- Asignar derechos de usuario.
- Configurar opciones de seguridad.
- Configurar la política de auditoría.
- Grupos seguros, servicios, registros, archivos y registros.
- Despliegue políticas de seguridad de red y aplicaciones.
- Diseñar, desplegar y gestionar configuraciones de seguridad a gran escala.

### **Módulo 46: Administración de la seguridad en Active Directory.**

Este módulo se centra en mantener la seguridad dentro de un entorno de Active Directory. Abarca desde la administración de permisos hasta los métodos de autenticación y la identificación de cuentas problemáticas.

- 
- Configurar derechos de cuenta de usuario.
- Configurar los derechos de cuenta de usuario para restringir el acceso.
- Delegar permisos en Active Directory.
- Proteger las cuentas de usuario con el grupo de Usuarios Protegidos.
- Describe la Guardia de Credenciales de Windows Defender.
- Bloquear autenticación NTLM de Windows.
- Localiza cuentas problemáticas.

### **Módulo 47: Comprensión de las cuentas de servicio de Windows Server.**

Las cuentas de servicio proporcionan el contexto de seguridad que usan los servicios de Windows, las tareas programadas y las aplicaciones para acceder a recursos locales y de red. Aprenda qué son las cuentas de servicio, los problemas que causan y cómo elegir y configurar el tipo de cuenta local o administrada correcta en Windows Server 2025.

- Comprender los tipos de cuentas de servicio local.
- Comprender los tipos de cuentas de servicios gestionados.
- Mejores prácticas para cuentas de servicio.

### **Módulo 48: Protección de cuentas de usuario de Windows Server.**

Proteja su entorno de Active Directory asegurando las cuentas de usuario con el principio de privilegios mínimos y colocándolas en el grupo de usuarios protegidos. Aprenda cómo limitar el alcance de autenticación y remediar cuentas potencialmente inseguras.

- Configurar derechos de cuenta de usuario.
- Proteger las cuentas de usuario con el grupo de Usuarios Protegidos.
- Describe la Guardia de Credenciales de Windows Defender.
- Autenticación NTLM por bloques.
- Localiza cuentas problemáticas.





## Módulo 49: Administración de controles de seguridad para identidades y accesos.

Este módulo se enfoca en administrar de manera efectiva los controles de seguridad en Microsoft Entra ID asegurando las identidades, la autenticación y la autorización para proteger usuarios, grupos e identidades externas contra amenazas, a la par de asegurar un acceso perfecto a los recursos.

- Benchmark de seguridad en la nube de Microsoft: Gestión de identidades y acceso privilegiado.
- ¿Qué es Microsoft Entra ID?
- Usuarios seguros de Microsoft Entra.
- Crear un nuevo usuario en Microsoft Entra ID.
- Grupos seguros de Microsoft Entra.
- Recomendación cuándo usar identidades externas.
- Identidades externas seguras.
- Implementar la Protección de Identidad Microsoft Entra.
- Microsoft Entra Connect.
- Microsoft Entra Cloud Sync.
- Opciones de autenticación.
- Sincronización de hash de contraseña con Microsoft Entra ID.
- Autenticación de paso de Microsoft Entra.
- Federación con Microsoft Entra ID.
- ¿Qué es la autenticación de Microsoft Entra?
- Implementar autenticación multifactor (MFA).
- Autenticación por Kerberos.
- Gestor de Red de Área Local de Nueva Tecnología (NTLM).
- Opciones de autenticación sin contraseña para Microsoft Entra ID.
- Implementar autenticación sin contraseña.
- Implementar protección por contraseña.
- Inicio de sesión único con Microsoft Entra ID.
- Implementar el inicio de sesión único (SSO).
- Integrar proveedores de inicio de sesión único (SSO) e identidad.
- Introducción a Microsoft Entra Verified ID.
- Configurar el ID verificado de Microsoft Entra.
- Recomendación y aplica protocolos modernos de autenticación.
- Azure Management Groups.
- Configura permisos de rol de Azure para grupos de gestión, suscripciones, grupos de recursos y recursos.
- Azure role-based access control.
- Azure Roles integrados.
- Asignar permisos de rol a Azure para grupos de gestión, suscripciones, grupos de recursos y recursos.

- Roles integrados en Microsoft Entra.
- Asignar roles integrados en Microsoft Entra ID.
- Control de acceso basado en roles de Microsoft Entra.
- Crea y asigna un rol personalizado en Microsoft Entra ID.
- Seguridad Zero Trust.
- Microsoft Entra Privileged Identity Management.
- Configurar la gestión de identidad privilegiada.
- Gobernanza de Microsoft Entra ID.
- Gestión del ciclo de vida de la identidad.
- Flujos de trabajo del ciclo de vida.
- Gestión de derechos.
- Delegación y roles en la gestión de derechos.
- Reseñas de Access.
- Configura la gestión de roles y revisiones de acceso utilizando la gobernanza de Microsoft Entra ID.
- Implementar políticas de acceso condicional para recursos en la nube en Azure.
- Resumen de Azure Lighthouse.

## Módulo 50: Supervisión y gobernanza de la seguridad.

Este módulo explora de manera integral el monitoreo y la gobernanza de la seguridad en entornos de Azure DevOps. Aprenda a implementar la seguridad en los flujos de trabajo, configurar Microsoft Defender for Cloud para la protección contra amenazas y el cumplimiento de normativas, gestionar Azure Policy para la aplicación del gobierno, y proteger recursos mediante bloqueos de recursos, así como implementar Microsoft Defender for Identity y la integración con GitHub Advanced Security.

- Implementar la seguridad de la tubería.
- Explora Microsoft Defender para la Nube.
- Examinar escenarios de uso de Microsoft Defender para la nube.
- Explore Azure Policy.
- Entiende las políticas.
- Explora iniciativas.
- Explorar bloqueos de recursos.
- Entiende Microsoft Defender for Identity.
- Integra la seguridad avanzada de GitHub con Microsoft Defender para la Nube.
- Configurar la seguridad avanzada de GitHub para GitHub y Azure DevOps.

## **Ruta de aprendizaje: Supervisión y solución de problemas en entornos de Windows Server.**

Aprenda a usar herramientas, procesos y prácticas recomendadas de supervisión y solución de problemas para optimizar el rendimiento de las aplicaciones y la disponibilidad de su entorno de Windows Server, así como de sus máquinas virtuales IaaS de Windows Server e instancias híbridas.

### **Módulo 51: Supervisión de máquinas virtuales IaaS de Windows Server e instancias híbridas.**

Aprenda a supervisar las máquinas virtuales de Azure y los servidores habilitados para Azure Arc mediante el agente de Azure Monitor y las reglas de recopilación de datos.

- Habilitar Azure Monitor for Virtual Machines.
- Monitorizar una VMs de Azure con Azure Monitor.
- Habilitar Azure Monitor en escenarios híbridos.
- Recopilar datos de un ordenador con Windows en un entorno híbrido.
- Integrar Azure Monitor con Microsoft Operations Manager.

### **Módulo 52: Supervisión de máquinas virtuales de Azure con Azure Monitor.**

Aprenda a supervisar sus máquinas virtuales de Azure utilizando Azure Monitor para recopilar y analizar métricas y registros del host y el cliente de la máquina virtual.

- Monitorizar los datos del host de la VM.
- Utiliza Metrics Explorer para ver métricas detalladas del host.
- Recopila contadores de rendimiento del cliente utilizando insights de VM.
- Recopilar los registros de eventos del cliente de la VM.

### **Módulo 53: Supervisión del rendimiento de Windows Server.**

Aprenda a usar una gama de herramientas de Windows Server para monitorear el sistema operativo y las aplicaciones en un equipo servidor. También aprenderá a configurar su sistema para optimizar la eficiencia y resolver problemas.

- Utiliza el Monitor de Rendimiento para identificar problemas de rendimiento.

- Utiliza Monitor de Recursos para revisar el uso actual de recursos.
- Revisa la fiabilidad con Reliability Monitor.
- Implementar una metodología de monitorización del rendimiento.
- Utiliza conjuntos de recopiladores de datos para analizar el rendimiento de los servidores.
- Monitorizar los servicios de infraestructura de red.
- Monitorizar máquinas virtuales que ejecutan Windows Server.
- Monitorizar el rendimiento con Windows Admin Center.
- Utiliza System Insights para ayudar a predecir problemas futuros de capacidad.
- Optimizar el rendimiento de Windows Server.

### **Módulo 54: Administración y supervisión de registros de eventos de Windows Server.**

Conozca cómo el Visor de eventos proporciona una ubicación conveniente y accesible para observar los eventos que ocurren. Acceda a la información de eventos de manera rápida y sencilla. Aprenda a interpretar los datos en el registro de eventos.

- Describe los registros de eventos de Windows Server.
- Utiliza el Centro de Administración de Windows para revisar registros.
- Utiliza Server Manager para revisar registros.
- Utiliza vistas personalizadas.
- Implementar suscripciones al registro de eventos.

### **Módulo 55: Implementación de auditoría y diagnóstico de Windows Server.**

Aprenda a realizar auditorías y diagnósticos en su entorno de Windows Server para cumplir con regulaciones, verificar la actividad de los usuarios y solucionar problemas. Implemente mejores prácticas de seguridad a través de auditorías periódicas de su entorno de red para recibir alertas tempranas sobre posibles actividades maliciosas.

- Describe las categorías básicas de auditoría.
- Describe categorías avanzadas.
- Registro de acceso de usuario.
- Habilitar la configuración y la recogida de eventos de arranque.



## **Módulo 56: Solución de problemas de redes locales e híbridas.**

Aprenda a solucionar problemas de conectividad local y conectividad de red híbrida. Diagnostique problemas comunes con DHCP, resolución de nombres, configuración de IP y enrutamiento que pueden causar problemas de confiabilidad y conectividad en un entorno local y en uno híbrido.

- Diagnosticar problemas de DHCP y DNS.
- Diagnosticar problemas de configuración de IP.
- Diagnosticar problemas de enrutamiento.
- Utiliza Packet Monitor para ayudar a diagnosticar problemas de red.
- Utiliza Azure Network Watcher para ayudar a diagnosticar problemas de red.

## **Módulo 57: Solución de problemas de máquinas virtuales de Windows Server en Azure.**

Aprenda a solucionar los problemas de configuración que afectan la conectividad con sus máquinas virtuales alojadas en Azure (VM). Explore enfoques para resolver problemas de inicio de la máquina virtual, extensiones, rendimiento, almacenamiento y cifrado.

- Resolución de problemas en el despliegue de MVs.
- Solucionar problemas en el inicio de una máquina virtual.
- Solucionar problemas de extensiones de máquinas virtuales.
- Solucionar problemas de conectividad de máquinas virtuales.
- Solucionar problemas en el rendimiento de las máquinas virtuales.
- Solucionar problemas de almacenamiento de máquinas virtuales.

## **Módulo 58: Administración de actualizaciones de Windows Server.**

Aprenda a usar Windows Server Update Services (WSUS) para implementar actualizaciones del sistema operativo en los equipos de su red. Seleccione la opción de implementación adecuada y combine WSUS con Microsoft Azure Update Management para administrar las actualizaciones del servidor.

- Explorar Windows Update.
- Descripción de las opciones de despliegue de servidores de Windows Server Update Services.

- Definir el proceso de gestión de actualizaciones de Windows Server Update Services.
- Describe el proceso de gestión de actualizaciones.

## **Módulo 59: Solución de problemas de Active Directory.**

Aprenda a solucionar fallas del servicio de AD DS o problemas de rendimiento degradado. Descubra cómo recuperar objetos de seguridad eliminados y la base de datos de AD DS, y cómo solucionar problemas de autenticación híbrida.

- Recuperar objetos de la papelera de reciclaje de AD.
- Recuperar la base de datos de AD DS.
- Recuperar SYSVOL.
- Resolución de problemas de replicación de AD DS.
- Solucionar problemas de autenticación híbrida.

