AZ-802 · CHEAT SHEET · CERTIFYDECK

Microsoft Certified: Windows Server Administrator Associate

Dominios, pesos oficiales y habilidades clave del temario de AZ-802, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 120 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Deploy and manage AD DS

20–25%

Deploy and manage AD DS domain controllers

- Un controlador de dominio se despliega en dos pasos: instalar el rol AD DS (Install-WindowsFeature) y promoverlo con el asistente o con los cmdlets ADDSDeployment (Install-ADDSForest, Install-ADDSDomain, Install-ADDSDomainController y sus cmdlets Test). Para sucursales con WAN lenta se usa instalar desde medios (IFM); la base de datos, SYSVOL y los registros van en rutas que no sean el sistema.
- Los controladores de dominio en máquinas virtuales de Azure guardan NTDS.dit, registros y SYSVOL en un disco de datos con la caché del host en None, usan IP privada estática sin IP pública, Azure Bastion para administrarlos y zonas de disponibilidad. Se apagan desde el sistema invitado, no desde el portal, y se crea un sitio de AD DS para las subredes de Azure.
- Un RODC guarda una copia de solo lectura del directorio, replica en un solo sentido y no puede ser el primer DC de un bosque o dominio. Se puede preconfigurar su cuenta con Add-ADDSReadOnlyDomainControllerAccount (el sitio debe existir y antes debe haberse ejecutado adprep /rodcprep) y adjuntar después el servidor con Install-ADDSDomainController -UseExistingAccount, de modo que un administrador local instale el rol.
- La directiva de replicación de contraseñas (PRP) de un RODC tiene listas de permitidos y denegados; denegar prevalece y lo que no figura en ninguna lista no se almacena en caché. Se gestiona con Add-ADDomainControllerPasswordReplicationPolicy, se precargan contraseñas con Sync-ADObject -PasswordOnly y se audita con Get-ADDomainControllerPasswordReplicationPolicyUsage. Si roban un RODC, se borra su cuenta y se restablecen las contraseñas en caché.
- Cada bosque tiene un maestro de esquema y un maestro de nomenclatura de dominios, y cada dominio un maestro RID, un maestro de infraestructura y un emulador de PDC; un RODC no puede tener ninguno. Los roles se transfieren con los complementos, ntdsutil o Move-ADDirectoryServerOperationMasterRole, y solo se asumen con ntdsutil o con -Force; el antiguo titular no debe volver sin reinstalarse y limpiar sus metadatos.

Configure and manage multi-site, multi-domain, and multi-forest environments

- Las confianzas de bosque son transitivas entre todos los dominios de los dos bosques, pero no se extienden a un tercer bosque; las externas y de acceso directo no son transitivas y las de territorio conectan con dominios Kerberos v5 ajenos a AD DS. Antes de una confianza de bosque hace falta resolución DNS entre bosques. La autenticación selectiva exige que se permita explícitamente a los objetos de cada bosque autenticarse en los equipos y servicios.
- Habilitar el filtrado de SID (quarantine) bloquea los SID ajenos; Netdom trust /enablesidhistory permite el historial de SID (migración). Permitir autenticación selectiva exige que se permita explícitamente a los objetos de cada bosque autenticarse en los equipos y servicios.
- Los vínculos de sitio definen coste y programación entre sitios. Los vínculos son transitivos por defecto (Puentear todos los vínculos de sitio); en redes no totalmente enrutadas se desactiva y se crean puentes. Un DC se mueve con Move-ADDirectoryServerToSite y los sitios se crean con New-ADReplicationSite, New-ADReplicationSubnet y New-ADReplicationSiteLink. El KCC crea objetos de conexión entre DC del mismo sitio y puentes de expansión entre sitios.
- Elevar el nivel funcional del bosque o dominio habilita características nuevas y no se puede bajar. Los sufijos de UPN alternativos permiten iniciar sesión con nombres cortos; los sufijos de nombre de entidad principal (SPN) alternativos, con Set-ADForest -SPNSuffixes, evitan errores de Kerberos cuando el nombre DNS del servicio no coincide con el dominio.
- La replicación depende de la red (RPC por el puerto 135), DNS, autenticación y hora. Se diagnostica con el registro Directory Service, repadmin /showrepl, Get-ADReplicationFailure y Get-ADReplicationPartnerMetadata.

Create and manage AD DS security principals

- Los grupos de seguridad se usan en las DACL y los de distribución solo para correo. Los globales contienen cuentas de su dominio, los universales cuentas y grupos de cualquier dominio del bosque, y los locales de dominio también cuentas de dominios o bosques de confianza, pero solo conceden permisos en su dominio. Se crean con New-ADGroup y se gestionan con Add-ADGroupMember.
- El ámbito del grupo puede cambiar: Set-ADGroup -GroupScope. Global a universal solo si no es miembro de otro global, y de universal a global solo si no contiene ningún universal. Un grupo universal admite cuentas y grupos de cualquier dominio del mismo bosque, y un grupo local de dominio admite además cuentas de otros bosques, pero solo concede permisos en su dominio. Las membresías de ámbito local no se replican fuera del dominio.
- Una MSA es de ámbito local, una gMSA puede usarse en varios servidores y una dMSA de Windows Server 2025 liga la autenticación a la identidad del equipo y puede reemplazar a una cuenta tradicional, cuya contraseña queda bloqueada. Las cuentas virtuales usan la cuenta de equipo para acceder a la red.
- Una MSA es para un único servidor, una gMSA para un grupo de servidores con una contraseña que calcula el controlador de dominio (requiere una clave raíz de KDS) y una dMSA de Windows Server 2025 liga la autenticación a la identidad del equipo y puede reemplazar a una cuenta tradicional, cuya contraseña queda bloqueada. Las cuentas virtuales usan la cuenta de equipo para acceder a la red.

Manage Windows Server by using domain-based Group Policies

- Los GPO se procesan en orden local, sitio, dominio y UO (de la primaria a la secundaria), y el contenedor más cercano gana los conflictos. Exigido es una propiedad del vínculo que prevalece sobre Bloquear herencia; el filtrado de seguridad y los filtros WMI deciden a quién se aplica el GPO completo, y el bucle invertido (Combinar o Reemplazar) aplica la configuración del usuario según el equipo.
- Las preferencias de directiva de grupo despliegan configuraciones que el usuario puede cambiar, pero se vuelven a aplicar en cada actualización salvo con Aplicar una vez y no volver a aplicar; si chocan con una opción de directiva, prevalece la directiva. El destino de nivel de elemento filtra cada elemento por grupo, sitio, equipo portátil, consulta WMI y otros criterios combinables con AND u OR.

2. Manage Windows Server instances and workloads in a hybrid environment 10–15%

Configure remote management for Windows Server instances in a hybrid environment

- Windows Admin Center tiene dos experiencias que se instalan en sistemas distintos: el modo de administración y el modo de virtualización. En Azure Portal se instala como extensión en una VM de Azure o en un servidor habilitado para Arc (sin puertos de entrada, mediante un proxy inverso) y gestiona solo esa máquina; el acceso lo da el rol Windows Admin Center Administrator Login. Para varias VM se usa una puerta de enlace en una VM de Azure.
- El problema del segundo salto aparece porque las credenciales de la sesión remota no pasan al tercer servidor; la delegación restringida de Kerberos basada en recursos se configura en el servidor del recurso, no guarda credenciales y cruza dominios, mientras que CredSSP las almacena en caché. JEA combina archivos de capacidad de rol (.psrc) y de configuración de sesión (.pssc) que se registran con Register-PSSessionConfiguration.
- En Windows Server 2025 OpenSSH viene instalado pero hay que habilitar el servicio sshd. La configuración está en %programdata%\ssh\sshd_config y requiere reiniciar el servicio; los administradores usan administrators_authorized_keys para las claves. Los servidores habilitados para Arc admiten SSH sin IP pública ni puertos abiertos registrando Microsoft.HybridConnectivity y usando az ssh arc.
- Para RDP a VM de Azure sin IP pública se usa Azure Bastion, que se implementa en la red virtual y conecta sobre TLS. El acceso just-in-time de Defender for Cloud mantiene cerrados los puertos de administración y los abre solo para solicitudes aprobadas durante un tiempo. En servidores habilitados para Arc, az ssh arc --rdp abre RDP a través de SSH, y la autenticación a nivel de red protege la sesión.

Manage Windows Server instances and workloads by using Azure services in a hybrid environment

- Azure Arc representa en Azure servidores que están fuera de Azure tras instalar el agente Azure Connected Machine, que no se puede instalar en VM de Azure. A escala se incorpora con azcmagent connect y una entidad de servicio con el rol Azure Connected Machine Onboarding, tras registrar los proveedores de recursos necesarios. El agente envía latidos: sin ellos el estado pasa a Desconectado y una máquina expirada debe volver a conectarse.
- Azure Machine Configuration audita o configura opciones del sistema operativo como código, asignadas con Azure Policy o manualmente. Los servidores habilitados para Arc ya incluyen su agente, mientras que las VM de Azure necesitan la extensión y una identidad administrada asignada por el sistema. Cada asignación usa un modo de cumplimiento: Audit, Apply and Monitor o Apply and Autocorrect, que corrige el desfase.
- Los servidores habilitados para Arc admiten las mismas extensiones de VM que Azure, como el Azure Monitor Agent, el agente de dependencias para VM insights o Custom Script, y se gestionan desde Azure. Con azcmagent puedes fijar localmente listas de permitidos o bloqueados, el modo de supervisión o deshabilitar el administrador de extensiones; nadie puede invalidar esas listas desde Azure, y no quitan las extensiones ya instaladas.
- Azure Update Manager gestiona las actualizaciones de VM de Azure y servidores habilitados para Arc sin depender de Log Analytics ni Azure Automation. La evaluación periódica o a petición detecta lo pendiente, y las programaciones recurrentes se guardan como configuraciones de mantenimiento, a las que se asocian máquinas estáticamente o con ámbitos dinámicos. Las VM de Azure necesitan la orquestación Customer Managed Schedules.
- Azure Automation admite runbooks de PowerShell, flujo de trabajo de PowerShell, Python y gráficos; los gráficos y los textuales no se convierten entre sí. Un runbook nuevo o importado es un borrador y hay que publicarlo para ejecutarlo; se inicia desde el portal, PowerShell, webhooks o programaciones. Para llegar a recursos locales se ejecuta en un grupo de Hybrid Runbook Worker, no en un worker concreto.

3. Manage VMs

10–15%

Manage Hyper-V and guest VM

- El Modo de sesión mejorada de VMConnect usa RDP para conectarse a máquinas virtuales Windows, lo que permite ventanas redimensionables y compartir portapapeles, impresoras, audio, unidades y dispositivos USB. Requiere Escritorio remoto habilitado en el invitado y que el host permita el modo mejorado (Set-VMHost -EnableEnhanced-SessionMode). Por defecto solo se comparten portapapeles, impresoras y reproducción de audio.
- PowerShell Direct ejecuta PowerShell en una máquina virtual Windows desde su host de Hyper-V sin depender de la red ni de la administración remota, con Enter-PSSession, Invoke-Command o New-PSSession y el parámetro -VMName. La máquina virtual debe ejecutarse localmente y estar encendida, hay que ser administrador de Hyper-V y dar credenciales del invitado. Copy-Item -ToSession copia archivos al invitado.
- La virtualización anidada permite ejecutar Hyper-V dentro de una máquina virtual exponiendo las extensiones de virtualización del procesador con Set-VMProcessor -ExposeVirtualizationExtensions $true, con la máquina apagada. Para la red se usa la suplantación de MAC en el primer nivel o NAT con un conmutador interno. Mientras Hyper-V corre en la máquina virtual, su memoria no varía aunque haya memoria dinámica.
- Con memoria dinámica, la memoria de inicio es la que usa la máquina virtual al arrancar (y al instalar o actualizar el sistema), la mínima permite recuperar memoria tras el arranque y no puede superar a la de inicio, y la máxima es el techo. El búfer añade un porcentaje sobre la demanda y el peso decide el reparto cuando falta memoria. En ejecución se puede subir la máxima y bajar la mínima.
- Los servicios de integración de Hyper-V (Heartbeat, apagado del invitado, sincronización de hora, intercambio de datos KVP, VSS, Guest Service Interface y PowerShell Direct) comunican el invitado con el host. Cada servicio debe estar habilitado en el host y en el invitado; se controlan con Enable-VMIntegrationService y Disable-VMIntegrationService. En invitados Windows todos están activos por defecto salvo Guest Service Interface.

Manage Windows Server VMs in Azure

- Una máquina virtual de Azure tiene un disco del sistema operativo, discos de datos administrados para aplicaciones y datos, y normalmente un disco temporal (la unidad D en Windows) cuyos datos pueden perderse al detenerla. Los discos de datos se amplían sin tiempo de inactividad, el del sistema requiere desasignar, ningún disco se puede reducir y después hay que extender el volumen en Windows.
- Para escalar verticalmente se cambia el tamaño de la máquina virtual, lo que la reinicia si está en ejecución; si el tamaño no está en el clúster actual, hay que desasignarla, o desasignar todo su conjunto de disponibilidad. Para escalar horizontalmente se usan conjuntos de escalado con escalado automático; la orquestación flexible es la recomendada y el modo no se puede cambiar tras crearlos.
- Un conjunto de disponibilidad reparte las máquinas virtuales entre dominios de error y de actualización, pero sigue expuesto a fallos de un centro de datos y no protege frente a errores del sistema operativo. Las zonas de disponibilidad son ubicaciones físicamente separadas de una región y ofrecen más resiliencia. Una máquina virtual solo se agrega a un conjunto al crearla.
- El acceso just-in-time de Defender for Servers Plan 2 agrega reglas de denegación para los puertos de administración en el NSG o en Azure Firewall y los abre solo para la IP y el tiempo aprobados; requiere un NSG o un firewall. Azure Bastion ofrece RDP y SSH sobre TLS en el puerto 443 hacia máquinas virtuales que solo tienen direcciones IP privadas.
- Las reglas de un grupo de seguridad de red se evalúan por prioridad, del número más bajo al más alto, y se detienen en la primera coincidencia; los NSG tienen estado y los cambios solo afectan a conexiones nuevas. Cada interfaz de red tiene una configuración IP principal y puede tener secundarias; la IP pública nunca se configura dentro de Windows.

4. Implement and manage an on-premises and hybrid networking infrastructure 10–15%

Implement on-premises and hybrid name resolution

- Las zonas integradas en Active Directory solo existen en controladores de dominio con el rol DNS, admiten actualizaciones dinámicas seguras y permiten que cada controlador procese cambios. Su ámbito de replicación puede ser el bosque, el dominio, el heredado o una partición personalizada; las zonas secundarias no se pueden almacenar en AD DS.
- Una zona principal tiene la copia en la que se escribe; la secundaria es una copia de solo lectura que se obtiene por transferencia de zona (AXFR completa o IXFR incremental), y la de código auxiliar solo guarda los servidores autoritativos. Los registros (A, AAAA, CNAME, MX, PTR, SRV, TXT) se crean con el módulo DnsServer; para cambiar el nombre o el tipo hay que eliminar y volver a crear.
- Los reenviadores de nivel de servidor reciben las consultas que el servidor no resuelve con sus zonas ni su caché; los reenviadores condicionales envían un espacio de nombres concreto a servidores designados y se evalúan antes. UseRootHint decide si se recurre a las sugerencias de raíz, y un reenviador condicional integrado en AD DS solo se crea en un controlador de escritura.
- Azure DNS Private Resolver resuelve entre redes virtuales y la red local sin servidores DNS propios. El punto de conexión de entrada recibe las consultas locales, que llegan con un reenviador condicional hacia su IP; el de salida reenvía de Azure a la red local según conjuntos de reglas vinculados a las redes virtuales, donde gana el sufijo más largo.
- Las directivas DNS usan subredes de cliente, ámbitos de zona y ámbitos de recursión para responder según la ubicación, la hora, la interfaz o el FQDN: tráfico por ubicación, DNS de cerebro dividido, filtrado y bloqueo. Hay directivas de resolución de consultas, de recursión y de transferencia de zona; se guardan en cada servidor y no se replican con AD DS.

Manage IP addressing in on-premises and hybrid scenarios

- Para implementar DHCP se instala el rol, se autoriza el servidor en AD DS (un servidor no autorizado no concede direcciones) y se crea un ámbito. La conmutación por error de DHCP comparte ámbitos IPv4 y concesiones entre dos servidores, en modo de equilibrio de carga o de espera activa, y los cambios del ámbito se replican a mano.
- En Azure, la red virtual entrega IP y DNS por DHCP: tras cambiar sus servidores DNS hay que renovar la concesión (ipconfig /renew) para que se apliquen. Las redes conectadas no pueden superponerse. En local, si falla otra subred, revisa el agente de retransmisión, la autorización, las direcciones libres y las IP estáticas no excluidas.
- Un ámbito DHCP es el intervalo de direcciones de una subred con su máscara, duración de concesión, opciones y reservas; cada subred admite un solo ámbito con un intervalo continuo, y los intervalos de exclusión protegen las direcciones estáticas. Hay ámbitos simples, de multidifusión (MADCAP) y superámbitos; las opciones de servidor se aplican a todos los clientes.
- Una reserva DHCP asigna siempre la misma dirección de un ámbito a un cliente identificado por su MAC (id. de cliente) y se crea con Add-DhcpServerv4Reservation, también a partir de una concesión existente. En un ámbito con conmutación por error de DHCP replica ámbitos IPv4 y concesiones entre dos servidores. El modo de equilibrio de carga reparte los clientes entre ambos; el modo de espera activa deja un servidor en reserva que solo concede si el activo cae. Los cambios en el ámbito se replican a mano (Invoke-DhcpServerv4FailoverReplication) y los clientes deben llegar a ambos servidores, por ejemplo con dos agentes de retransmisión.
- La conmutación por error de DHCP replica ámbitos IPv4 y concesiones entre dos servidores. El modo de equilibrio de carga reparte los clientes entre ambos; el modo de espera activa deja un servidor en reserva que solo concede si el activo cae. Los cambios en el ámbito se replican a mano con Invoke-DhcpServerv4FailoverReplication. En Azure no se reservan IP privadas para máquinas virtuales futuras.

5. Manage storage and file services 15–20%

Configure and manage Azure Files

- Los recursos compartidos clásicos se crean en una cuenta de almacenamiento cuyo tipo y SKU fijan el nivel de medios (SSD o HDD), el modelo de facturación y la redundancia; SSD solo admite LRS y ZRS. Un recurso no puede cambiar de nivel de medios: hay que crear otro y copiar. La protección se basa en la eliminación temporal, las instantáneas de solo lectura y Azure Backup.
- El acceso a Azure Files con identidad tiene dos capas: los roles de Azure RBAC a nivel de recurso compartido (o un permiso predeterminado para todas las identidades autenticadas) y las ACL de Windows en carpetas y archivos; prevalece lo más restrictivo. Las cuentas no sincronizadas con Microsoft Entra ID usan el permiso predeterminado, y las ACL se editan con icacls o el Explorador si el origen es AD DS.
- Azure File Sync convierte Windows Server en una caché de un recurso compartido de Azure. Se implementa un servicio de sincronización de almacenamiento, se instala el agente, se registra el servidor (solo en un servicio) y se crea un grupo de sincronización con un punto de conexión de nube y puntos de conexión de servidor en volúmenes NTFS. Los niveles de nube usan directivas de espacio libre y de fecha.
- Azure File Sync envía métricas a Azure Monitor (por ejemplo Server online status, Files not syncing o Sync session result) que sirven para reglas de alertas con grupos de acciones. El servicio de sincronización muestra el estado de servidores y puntos de conexión, el registro Telemetry (Microsoft-FileSyncAgent) y los contadores AFS del Monitor de rendimiento muestran la sincronización y los niveles de nube.
- Para migrar DFS-R a Azure File Sync se crea un grupo de sincronización, se empieza por el servidor con el conjunto completo de datos (sin niveles de nube), se deja sincronizar todo, se deshabilita DFS-R y se crean los puntos de conexión de los demás servidores. Si ambas tecnologías conviven, los niveles de nube deben estar desactivados en los volúmenes replicados por DFS-R.

Configure and manage Windows Server file shares

- Los permisos de recurso compartido SMB se gestionan con el módulo SmbShare: New-SmbShare con FullAccess, ChangeAccess, ReadAccess o NoAccess, y después Grant, Block, Revoke y Unblock-SmbShareAccess. La enumeración basada en el acceso (FolderEnumerationMode AccessBased) oculta lo que el usuario no puede abrir y está desactivada por defecto; en DFS solo oculta carpetas, no bloquea el acceso.
- FSRM es un servicio de rol de Windows Server para volúmenes NTFS que ofrece cuotas (estrictas o flexibles, con plantillas y aplicación automática a subcarpetas), filtrado de archivos (activo o pasivo, con excepciones), clasificación de archivos, tareas de administración de archivos como la expiración e informes de almacenamiento. Se gestiona con su consola o con PowerShell.
- Espacios de nombres DFS agrupa carpetas compartidas de varios servidores bajo una ruta lógica. Un espacio independiente guarda la información en el registro y gana disponibilidad con un clúster; uno basado en dominio la guarda en AD DS y usa varios servidores de espacio de nombres, y el modo Windows Server 2008 admite enumeración basada en el acceso. Replication DFS sincroniza carpetas con RDC.
- SMB over QUIC sustituye el transporte TCP 445 por un túnel TLS 1.3 sobre UDP 443 para acceder a servidores de archivos perimetrales desde Internet sin VPN. Requiere un certificado de autenticación de servidor con nombres DNS en el SAN, asignado con New-SmbServerCertificateMapping. Los clientes usan TCP primero, el RDC Proxy permite Kerberos y, al renovar el certificado, hay que reasignarlo.

Configure Windows Server storage

- La firma SMB protege la integridad y el cifrado SMB protege los datos en tránsito, por recurso (Set-SmbShare -EncryptData), por servidor (Set-SmbServerConfiguration) o al asignar unidades (-RequirePrivacy). Windows Server 2025 exige la firma saliente. Con la configuración predeterminada solo los clientes SMB 3.x acceden a recursos cifrados, y SMB 1.0 debe quitarse porque permite degradar la conexión.
- Un disco nuevo se inicializa (GPT o MBR por defecto) antes de crear volúmenes. GPT admite más de cuatro particiones y discos más grandes que MBR, y cambiar el estilo exige un disco sin particiones (Clear-Disk e Initialize-Disk). Un volumen NTFS o ReFS se extiende contiguo del mismo disco con Resize-Partition; solo los volúmenes NTFS o sin formato se pueden reducir.
- Storage Spaces agrupa discos físicos en blanco en un grupo de almacenamiento y crea discos virtuales con resistencia simple, de reflejo (doble o triple) o de paridad, y aprovisionamiento fino o fijo. Los HBA deben estar en modo no RAID. El reflejo es la opción general, la paridad encaja en cargas secuenciales y lo simple, en datos temporales. Sobre los discos virtuales se crean volúmenes NTFS o ReFS.
- Storage Spaces Direct agrupa las unidades internas de un clúster de conmutación por error en un grupo definido por software con caché en las unidades más rápidas y volúmenes ReFS en Volúmenes compartidos de clúster. Se valida con Test-Cluster, se habilita con Enable-ClusterStorageSpacesDirect y se crean volúmenes con New-Volume. Puede ser hiperconvergente o convergente, con un servidor de archivos de escalabilidad horizontal.
- Storage Replica replica volúmenes por bloques sobre SMB 3 en modo síncrono (sin pérdida de datos, red de baja latencia) o asíncrono (largas distancias). Admite clúster extendido con conmutación automática y clúster a clúster o servidor a servidor con conmutación manual. Exige discos GPT, volúmenes de datos de igual tamaño y un volumen de registro dedicado, no sustituye a las copias de seguridad.
- La deduplicación de datos usa un modelo de postprocesamiento: escribe los datos sin optimizar y el trabajo de optimización los fragmenta y guarda cada fragmento único en el almacén de fragmentos. Se habilita por volumen con un tipo de uso: Default (servidores de archivos), Hyper-V (VDI) o Backup (copias virtualizadas). DDPEval.exe estima el ahorro y el trabajo Unoptimization la deshace.

6. Secure Windows Server infrastructure

10–15%

Secure Windows Server operating system

- La protección contra vulnerabilidades aplica mitigaciones como DEP, ASLR obligatorio o CFG a todo el sistema y otras, como ACG o bloquear imágenes remotas, solo por aplicación; la configuración de programa prevalece sobre la del sistema. Se configura en Seguridad de Windows o con Set-ProcessMitigation, se exporta a XML y se distribuye con la directiva de grupo de configuración común, que invalida los cambios locales.
- App Control for Business solo deja ejecutar el código que permite su directiva, incluidos scripts e instaladores MSI. En formato de varias directivas, dos directivas base se combinan por intersección y una base con sus complementarias por unión. El modo de auditoría registra en CodeIntegrity Operational lo que se bloquearía. La directiva de grupo solo implementa el formato de una directiva, CiTool agrega archivos .cip.
- Credential Guard usa la seguridad basada en virtualización para aislar los hashes NTLM, los TGT de Kerberos y las credenciales de dominio frente a ataques pass-the-hash y pass-the-ticket. En Windows Server 2025 se habilita por defecto, sin UEFI lock, en servidores miembro que cumplen los requisitos, pero no en controladores de dominio. Bloquea DES y la delegación no restringida de Kerberos, y en VM exige generación 2.
- Microsoft Defender SmartScreen protege frente a sitios de phishing o malware y archivos descargados de Internet mediante comprobaciones de reputación; no cubre archivos de recursos compartidos internos. Por defecto permite omitir las advertencias, así que se recomienda habilitar con directiva de grupo Configure Windows Defender SmartScreen con Warn and prevent bypass y las opciones de Microsoft Edge que impiden omitirlas.
- Las líneas base de seguridad de Microsoft se publican como copias de seguridad de GPO en el Security Compliance Toolkit: Import-GPO las carga en GPO de tu dominio y LGPO.exe administra la directiva local de los servidores sin dominio. Policy Analyzer compara conjuntos de GPO y detecta conflictos. Los GPO de dominio invalidan la directiva local, y el filtrado de seguridad o WMI decide si se aplica el GPO completo.

Secure AD DS

- El dominio tiene una directiva de contraseñas y de bloqueo predeterminada; para dar otra a ciertos usuarios se usan directivas de contraseñas específicas (PSO), aplicables solo a usuarios y grupos de seguridad globales, nunca a una UO. Si hay varios PSO, gana el aplicado directamente al usuario y, si no, el de menor valor de precedencia. Se gestionan con el Centro de administración de Active Directory o PowerShell.
- Microsoft Entra Password Protection aplica en AD DS local las listas global y personalizada de contraseñas prohibidas de Microsoft Entra ID. El servicio proxy, en un servidor miembro, reenvía las descargas de directivas; el agente de DC valida los cambios y debe estar en todos los DC grabables (los RODC no lo necesitan). Los DC no salen a Internet y la función complementa, no sustituye, la directiva de contraseñas de AD DS.
- Usuarios protegidos es un grupo de seguridad global que aplica protecciones no configurables contra el robo de credenciales: sin NTLM, solo Kerberos con AES, sin delegación (restringida o no), TGT no renovables más allá de su duración inicial y sin inicio de sesión sin conexión. No se deben agregar cuentas de servicio ni de equipo, y conviene probar antes de incluir cuentas muy privilegiadas.
- Los controladores de dominio se protegen de forma separada y más estricta: racks dedicados, TPM y BitLocker en todos los volúmenes (con almacenamiento local), DC virtuales en hosts propios y RODC en sucursales sin sala segura. Se recomienda Server Core, administración remota desde estaciones seguras, parches gestionados aparte, sin exploradores web y sin salida a Internet desde los DC.
- El acceso a los controladores de dominio se restringe con GPO vinculados a la UO Domain Controllers que combinan derechos de usuario y reglas del Firewall de Windows, por ejemplo RDP solo desde servidores de salto; una actualización de directiva corrige los cambios manuales. La administración se hace en remoto desde estaciones seguras y la cuenta Administrador integrada se limita al inicio de sesión local.

7. Monitor and troubleshoot Windows Server environments

15–20%

Monitor by using Windows Server tools and Azure services

- El Monitor de rendimiento es un complemento MMC integrado que muestra contadores en tiempo real, conjuntos de recopiladores de datos e informes, en local o en remoto. Cada contador sigue la forma objeto, instancia y contador. Para diagnosticar se miran latencia de disco, memoria disponible frente al conjunto de trabajo de los procesos y CPU, y un intervalo de muestreo largo evita gráficos resumidos en capturas de varios días.
- Un conjunto de recopiladores de datos guarda contadores de rendimiento, seguimientos o alertas durante un periodo. Se crea en el Monitor de rendimiento o con logman: create counter registra contadores (-c, -si, -o, -f bincirc, -s para un equipo remoto) y create alert revalúa umbrales con -th y puede iniciar otro conjunto con -rdcs. Los conjuntos se exportan e importan como XML.
- Windows Admin Center supervisa un servidor con Overview (CPU, memoria y red actuales), Events, Performance Monitor y System Insights. Su herramienta Azure Monitor conecta el servidor a un área de trabajo de Log Analytics y habilita contadores de rendimiento, las alertas por correo se crean en el Azure portal como reglas de alertas con un grupo de acciones. En VM insights, los servidores locales usan Performance y Maps.
- System Insights aporta análisis predictivo local a Windows Server con cuatro funcionalidades predeterminadas: previsión de capacidad de CPU, de red, de almacenamiento total y de consumo por volumen. Analiza datos diarios sin conexión a la nube y devuelve estados Ok, Warning, Critical, Error o None. Se gestiona con Windows Admin Center o PowerShell, admite programaciones y scripts de corrección, y publica los resultados en el registro de eventos.
- wevtutil consulta, exporta (epl), vacía con copia (cl /bu) y configura registros (sl). /rt:true conserva los eventos existentes al llenarse y /ab:true, que exige /rt:true, hace copia automática. wecutil administra suscripciones del recopilador de eventos de Windows: qc habilita ForwardedEvents e inicio retrasado del servicio, y ds no borra los eventos ya recibidos.

Troubleshoot Windows Server issues

- Ante un fallo de RDP, comprueba con qwinsta que el agente de escucha rdp-tcp está en Listen y, desde la misma red, ejecuta Test-NetConnection -Port 3389: si TcpTestSucceeded es False revisa puerto, DNS, reglas de firewall y NSG (obligatorio con IP pública estándar), si es True, revisa el equipo, por ejemplo que el PID de TermService sea el que escucha en el 3389.
- En el cliente, revisa ipconfig /all, haz ping al servidor DNS y prueba con nslookup, que no usa la caché del cliente; las respuestas negativas en caché se borran con ipconfig /flushdns. En el servidor, un tiempo de espera agotado apunta al servicio DNS detenido y Server failure a una zona en pausa; Clear-DnsServerCache vacía la caché que sirve a los clientes y dnscmd /zonerefresh fuerza la transferencia a una zona secundaria.
- Si una actualización falla por daños, ejecuta DISM /Online /Cleanup-Image /RestoreHealth (sin acceso a Windows Update, con /Source a una instalación de la misma versión y /LimitAccess), después sfc /scannow y de nuevo Windows Update; los resultados quedan en CBS.log. En Azure Update Manager, la evaluación periódica de servidores Arc exige registrar Microsoft.Compute en la suscripción.
- Los miembros del dominio sincronizan la hora con la jerarquía del dominio (NT5DS) y el emulador de PDC del dominio raíz del bosque se configura con un origen externo. w32tm /config /syncfromflags:domhier /update devuelve un cliente a la jerarquía, /query /source y /query /configuration muestran el origen y la configuración efectiva, y la directiva de grupo prevalece sobre el registro.
- Para un uso de CPU sostenido, identifica el proceso con el Administrador de tareas, el Monitor de recursos o Process Explorer y recopila un registro del Monitor de rendimiento, unos minutos de WPR y dos volcados con ProcDump. Un svchost compartido se separa con sc config servicio type= own y se revierte con type= share. Con Lsass.exe alto en un controlador de dominio, ejecuta el conjunto de recopiladores Active Directory Diagnostics.

Troubleshoot Active Directory

- La papelera de reciclaje de Active Directory no está habilitada de forma predeterminada, se habilita con Enable-ADOptionalFeature o el Centro de administración y es irreversible. Conserva todos los atributos, por lo que los usuarios recuperan sus grupos, pero solo para objetos eliminados después de habilitarla. Hay que restaurar el objeto primario antes que los hijos, Restore-ADObject sin -Target path usa lastKnownParent.
- Una restauración del estado del sistema en DSRM, por ejemplo con wbadmin start systemstaterecovery, es no autoritativa: el DC recibe después los cambios de sus asociados. Para recuperar objetos eliminados sin papelera, tras restaurar se ejecuta ntdsutil authoritative restore (restore object o restore subtree), se reinicia en modo normal y se replica con repadmin /syncall, la contraseña de DSRM se establece con ntdsutil set dsrm password.
- SYSVOL replicado por DFSR se restaura de forma autoritativa con wbadmin start systemstaterecovery -authsysvol o editando msDFSR-Options=1 en SYSVOL Subscription; tras marcar un DC autoritativo, preferiblemente el emulador de PDC, los demás se sincronizan de forma no autoritativa con msDFSR-Enabled y DFSRDIAG POLLAD. Para reparar un único DC basta con hacerlo no autoritativo; Administración de DFS no sirve para SYSVOL.
- Los errores de replicación de AD se diagnostican con el registro Directory Service y repadmin /showrepl: el error 5 indica un fallo de autenticación, el 8524 un error DNS y el Event ID 2042 que se superó la vida útil de los objetos de exclusión. Ante el 2042 se identifican los objetos persistentes con repadmin /removelingeringobjects en modo /advisory_mode, se eliminan y solo después se reanuda la replicación.
- DCDiag analiza el estado de los controladores de dominio; /e prueba toda la empresa, /test:DNS debe pedirse explícitamente y /fix solo corrige los SPN en la prueba MachineAccount. Advertising, KnowsOfRoleHolders, NetLogons y SysVolCheck comprueban la localización del DC, los roles FSMO, el acceso a los recursos compartidos y SYSVOL. Un DC que no volverá se retira limpiando sus metadatos con Ntdsutil.