AZ-305 · CHEAT SHEET · CERTIFYDECK

Microsoft Certified: Azure Solutions Architect Expert

Dominios, pesos oficiales y habilidades clave del temario de AZ-305, para repasar antes del examen.

Nivel: Advanced (Expert) Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Design identity, governance, and monitoring solutions

25–30%

Design solutions for logging and monitoring

- Los logs de Azure Monitor se almacenan en áreas de trabajo de Log Analytics y se consultan con KQL. Empieza con un único área de trabajo y añade más solo por residencia de datos, propiedad, facturación o retención distinta. El registro de actividad se recopila solo; los logs de recursos requieren una configuración de diagnóstico, y los planes de tabla ajustan coste y retención.
- Las configuraciones de diagnóstico enrutan logs de recursos, métricas de plataforma y el registro de actividad a un área de trabajo, una cuenta de almacenamiento, Event Hubs o una solución de partner. Las reglas de exportación copian tablas del área de trabajo, las transformaciones filtran antes de almacenar y Azure Monitor pipeline procesa datos en sitios remotos o híbridos.
- Azure Monitor cubre cada capa: Application Insights para aplicaciones, VM insights y Azure Monitor Agent para máquinas (también híbridas con Azure Arc), Prometheus y Grafana administrados para Kubernetes y Connection monitor para la red. Las alertas de métricas, de logs, del registro de actividad y de Service Health cubren señales distintas, y los libros sirven para informes.

Design authentication and authorization solutions

- En entornos híbridos hay tres métodos: sincronización de hash de contraseñas (el más simple), autenticación pass-through (valida contra Active Directory local) y federación (necesaria para requisitos que Entra no cubre de forma nativa). Conviene activar la sincronización de hash como respaldo. Complementan los métodos sin contraseña resistentes al phishing, Conditional Access y las identidades administradas.
- Cloud Sync sincroniza Active Directory con Entra ID con agentes ligeros y admite bosques desconectados; Domain Services ofrece LDAP, Kerberos y unión a dominio administrados para aplicaciones heredadas. External ID cubre colaboración B2B y clientes en un inquilino externo, y ID Governance gestiona el ciclo de vida con derechos, revisiones y flujos de trabajo.
- Azure RBAC concede acceso mediante asignaciones de rol (entidad de seguridad, definición de rol y ámbito) que se heredan por la jerarquía de grupo de administración, suscripción, grupo de recursos y recurso, y cuyos permisos se suman. Las condiciones ABAC afinan el acceso y PIM aporta acceso justo a tiempo. En Key Vault se separan plano de control y de datos.
- Microsoft Entra application proxy publica aplicaciones web locales con un conector solo saliente, autenticación previa y Conditional Access, y usa delegación restringida de Kerberos para SSO integrado. Private Access canaliza recursos privados por FQDN o IP con Quick Access o aplicaciones por recurso. La confianza Kerberos en la nube da SSO a recursos de Active Directory.
- Azure Key Vault centraliza secretos, claves y certificados; usa un almacén por aplicación y entorno, identidades administradas y Azure RBAC con el mínimo privilegio. Activa soft-delete y protección contra purga. Para raíz de confianza propia y un solo inquilino elige Managed HSM; los certificados de CA asociadas se renuevan solos.

Design governance

- Usa una jerarquía de grupos de administración plana que agrupe suscripciones por necesidades de directivas, con suscripciones de plataforma separadas. Los grupos de recursos agrupan recursos con el mismo ciclo de vida. Las etiquetas no se heredan: impón o hereda etiquetas con Azure Policy (modify) y no las uses para datos sensibles.
- Azure Policy evalúa recursos y aplica efectos como audit, deny o deployIfNotExists; empieza con audit, usa iniciativas y tareas de corrección para lo existente, y exenciones con caducidad para excepciones. Defender for Cloud muestra el cumplimiento normativo por controles; Blueprints migra a deployment stacks y template specs.
- Microsoft Entra ID Governance cubre el ciclo de vida de identidades y accesos: la administración de derechos usa paquetes de acceso con aprobación y caducidad, las revisiones de acceso recertifican accesos, los flujos de ciclo de vida automatizan altas y bajas, y PIM da acceso privilegiado just-in-time con MFA y aprobación.

2. Design data storage solutions

20–25%

Design data storage solutions for relational data

- Azure SQL Database encaja en aplicaciones nuevas en la nube, SQL Managed Instance en migraciones con casi total compatibilidad de instancia (Agente SQL, servidores vinculados, CLR) y SQL Server en VM cuando hace falta acceso al sistema operativo. Para motores de código abierto están Azure Database for PostgreSQL y para MySQL.
- En el modelo vCore elige Uso general para cargas equilibradas, Crítico para la empresa para OLTP con baja latencia y réplica de lectura incluida, e Hiperescala para almacenamiento muy escalable. El cómputo sin servidor se ajusta a un uso intermitente; el aprovisionado, a uso constante. En PostgreSQL, Burstable no es para producción.
- Escala en vertical cambiando el tamaño de cómputo o usando grupos elásticos para bases de datos con picos que no coinciden. El escalado horizontal de lectura y las réplicas con nombre de Hiperescala descargan lecturas, y la replicación geográfica añade lectores en otras regiones. Si una base de datos no basta, particiona (sharding) con las herramientas de Elastic Database.
- Azure SQL ofrece capas de protección distintas: TDE cifra datos y copias en reposo (con clave del servicio o administrada por el cliente en Key Vault), Always Encrypted mantiene las claves fuera del motor, el enmascaramiento dinámico oculta valores en los resultados y ledger aporta evidencia de manipulación. Las copias a largo plazo y su redundancia cubren cumplimiento y residencia.

Design data storage solutions for semi-structured and unstructured data

- Para datos semiestructurados se elige según el modelo y el patrón de acceso: Cosmos DB for NoSQL para documentos JSON con esquema flexible y distribución global, Cosmos DB for Table o Table storage para clave/atributo, Redis para caché clave-valor y Data Explorer para telemetría y series temporales. La clave de partición y el nivel de coherencia condicionan escala y latencia.
- Para datos no estructurados, Blob Storage es el almacén de objetos para imágenes, documentos, copias y datos de análisis; Data Lake Storage añade espacio de nombres jerárquico, ACL POSIX y acceso compatible con Hadoop sobre Blob; Azure Files ofrece recursos compartidos SMB y NFS administrados para aplicaciones que esperan un sistema de archivos.
- Los niveles de acceso de Blob equilibran coste y rendimiento: el frecuente tiene el mayor coste de almacenamiento y el menor de acceso, esporádico y frío bajan el almacenamiento y suben el acceso con latencia de milisegundos, y archivo es el más barato pero sin conexión. La administración del ciclo de vida automatiza transiciones y borrados, y en Azure Files HDD o SSD se elige según la latencia.
- La redundancia (LRS, ZRS, GRS, GZRS y variantes de lectura) protege frente a fallos de hardware, zona o región, pero replica también borrados y sobrescrituras. Para ello se combinan bloqueos de Resource Manager, eliminación temporal de contenedores y blobs, control de versiones, restauración a un momento dado y directivas de inmutabilidad WORM.

Design data integration

- Azure Data Factory orquesta canalizaciones ETL y ELT con actividades de copia y transformación; el entorno de ejecución de integración se elige según la red: Azure para almacenes públicos, autohospedado para redes privadas y Azure-SSIS para trasladar paquetes SSIS. Event Hubs ingiere flujos de eventos con soporte de Kafka y Stream Analytics los procesa con SQL.
- Microsoft Fabric unifica ingeniería de datos, almacén, tiempo real y Power BI sobre OneLake como SaaS; dentro de Fabric, el almacén sirve BI con T-SQL, el lakehouse big data y ML con Spark, y Eventhouse series temporales con KQL. Azure Databricks ofrece un lakehouse abierto con Spark, Delta Lake y MLflow, y Stream Analytics procesa flujos sencillos con SQL.

3. Design business continuity solutions

15–20%

Design solutions for backup and disaster recovery

- Elige la solución según el RTO y el RPO de cada nivel de criticidad: copia y restauración para cargas administrativas, espera parcial o en frío para las operativas y activo-activo multirregión para las de misión crítica. Azure Site Recovery replica VM de Azure, VMware, Hyper-V y servidores físicos y orquesta la conmutación con planes de recuperación.
- Azure Backup protege la computación según la carga: la copia de VM toma instantáneas coherentes con la aplicación (VSS en Windows, scripts previos y posteriores en Linux), Disk Backup hace instantáneas incrementales sin agente de un disco, y la copia de AKS protege el estado del clúster y los volúmenes persistentes. App Service para apps codificadas o personalizadas, Cosmos DB ofrece modo periódico o continuo con restauración a un momento dado. Para bases de datos autoadministradas, la redundancia geográfica del almacén permite restaurar en otra región.
- Azure SQL Database hace copias automáticas completas, diferenciales y de registro de transacciones y conserva los backups según el plazo de retención configurado. Una eliminación temporal de contenedores y bloques, y control de versiones, protege frente a borrados accidentales. La replicación geográfica del almacén permite restaurar en otra región.

Design high availability

- Para alta disponibilidad de computación, reparte las instancias entre zonas de disponibilidad (los conjuntos de disponibilidad solo reparten por dominios de error dentro de un centro de datos) y usa un equilibrador que redirija el tráfico. Lo permiten los conjuntos de escalado con orquestación flexible, App Service con redundancia de zona de una zona sin perder datos confirmados. Entre regiones, los grupos de conmutación por error mueven conjuntos de bases de datos con puntos de conexión fijos y la replicación geográfica activa va por base. SQL Server en VM usa grupos de disponibilidad o instancias de clúster; PostgreSQL alta disponibilidad con zona redundante.
- En Azure SQL Database la disponibilidad local es la base y la redundancia de zona añade resiliencia ante la caída de una zona sin perder datos confirmados. Entre regiones, los grupos de conmutación por error mueven conjuntos de bases de datos con puntos de conexión fijos y la replicación geográfica activa va por base. SQL Server en VM usa grupos de disponibilidad o instancias de clúster; PostgreSQL alta disponibilidad con zona redundante.
- AKS con zonas repartes nodos y discos ZRS entre regiones. Front Door o Traffic Manager enrutador externo para multirregión.
- En Azure Storage, ZRS mantiene los datos legibles y escribibles si cae una zona y GZRS añade una región secundaria; solo las variantes RA-GRS y RA-GZRS permiten leer del secundario sin conmutación, y Azure Files no las admite. En Cosmos DB, la redundancia de zona se configura por región y varias regiones de escritura dan mayor resiliencia, sin consistencia fuerte y con resolución de conflictos.

4. Design infrastructure solutions

30–35%

Design compute solutions

- Elegir proceso empieza por el modelo de hospedaje: IaaS (máquinas virtuales) da el máximo control y exige administrar el SO; PaaS (App Service, Container Apps) y FaaS (Functions) delegan más. Evalúa cada componente por separado, ten en cuenta las habilidades del equipo, y recuerda que todas las plataformas son regionales y cubren tareas finitas.
- Para máquinas virtuales, elige el tamaño según la carga (propósito general, serie B con ráfagas, proceso, memoria, almacenamiento) y la disponibilidad con zonas de disponibilidad y conjuntos de escalado en modo flexible. Spot sirve para trabajo interrumpible, Dedicated Host para aislamiento y control del mantenimiento, y Site Recovery para recuperar ante una caída regional.
- Container Apps ofrece contenedores sin servidor con KEDA, Dapr, revisiones y escalado a cero, sin exponer la API de Kubernetes. AKS da el máximo control (API de Kubernetes, directivas de red, cargas dispares) a costa de más operación. Container Instances ejecuta contenedores sueltos sin orquestación, y los trabajos de Container Apps conectores). Container Apps (contenedores con escalado a cero) y Event Grid. Flex Consumption escala desde cero con red virtual, Durable Functions añade flujos con estado en código y las funciones HTTP tienen un tiempo máximo de respuesta fijo.
- Azure Batch administra un grupo de nodos de máquinas virtuales, instala la aplicación y programa trabajos sin software de programación propio; sirve para cargas paralelas independientes y para cargas acopladas con MPI. Spot y el escalado automático reducen el coste, y CycleCloud encaja cuando debes conservar un programador existente como Slurm.

Design an application architecture

- Un broker de mensajes desacopla productor y consumidor en el tiempo, nivela la carga y permite consumidores concurrentes. Usa Service Bus para comandos de alto valor (sesiones, deduplicación, mensajes fallidos, temas con filtros), Event Hubs para flujos de eventos con reproducción y Claim Check cuando la carga excede el broker.
- Una arquitectura controlada por eventos tiene productores, canales y consumidores desacoplados. Usa publicación-suscripción (Event Grid) para notificaciones discretas y streaming (Event Hubs) cuando se necesita orden por partición y reproducción. Elige entre topología de broker o de mediador y asume coherencia eventual, duplicados e idempotencia.
- API Management actúa como fachada de los backends: valida claves y tokens, aplica cuotas y límites de llamadas, transforma mensajes con políticas y puede cachear. La puerta de enlace autohospedada cubre APIs en entornos híbridos y los workspaces dan autonomía a equipos descentralizados. En mensajería, Service Bus transporta comandos, Event Grid eventos discretos, Event Hubs flujos de eventos y Logic Apps orquesta flujos con conectores.
- Una caché privada en memoria es rápida pero cada instancia guarda su propia copia; una caché compartida, como Azure Managed Redis, ofrece una vista común y puede crecer en clúster. Con cache-aside se actualiza primero el almacén y después se invalida la entrada, write-through da lectura inmediata tras escribir. La caché nunca debe ser el almacén principal y la aplicación necesita una alternativa si deja de estar disponible.
- Azure App Configuration centraliza ajustes jerárquicos y indicadores de característica, que las aplicaciones pueden refrescar sin redesplegar, y complementa a Key Vault: los secretos se quedan en Key Vault y App Configuration solo guarda la referencia. Las etiquetas crean variantes por entorno, las instantáneas son inmutables para desplegar con seguridad y volver a una configuración válida, y la replicación geográfica añade resiliencia.

Design migrations

- El Cloud Adoption Framework ordena la adopción en siete fases: estrategia, plan, preparación (zona de aterrizaje), adopción, gobierno, seguridad y administración. Cada carga se trata con una estrategia (retirar, conservar, rehost, replatform, refactor, rearchitect, replace o rebuild) según su motivo de negocio. Las oleadas se ordenan por dependencias y riesgo, con ruta de datos, método con o sin inactividad y plan de reversión probado.
- Azure Migrate descubre servidores, bases de datos y aplicaciones web con un dispositivo (o con el recopilador en redes aisladas) y evalúa preparación, tamaño y coste. El análisis de dependencias sin agente agrupa los servidores que deben migrar juntos. Evalúa también rendimiento de referencia, seguridad e identidad, código, bases de datos, los hosts, servidores físicos y de otras nubes usan replicación con agente y dispositivo de replicación. Para bases de datos, SQL Managed Instance minimiza cambios y SQL Server en máquinas virtuales da acceso al sistema operativo. Las aplicaciones ASP.NET pueden ir a App Service, a contenedores o a Azure VMware Solution.
- En Azure Migrate, VMware se replica preferentemente sin agente con el dispositivo y Hyper-V con proveedores en el host; servidores físicos y de otras nubes usan replicación con agente y dispositivo de replicación. Para bases de datos, SQL Managed Instance minimiza cambios y SQL Server en máquinas virtuales da acceso al sistema operativo. Las aplicaciones ASP.NET pueden ir a App Service, a contenedores o a Azure VMware Solution.
- El destino se elige por el motor y el nivel de gestión. Azure SQL Managed Instance para migrar con pocos cambios, SQL Database para PaaS por base de datos y SQL Server en VM cuando necesitas el sistema operativo. El Managed Instance link da la migración en línea con menor parada y lectura en el destino, Log Replay Service y la restauración nativa son más simples. PostgreSQL ofrece migración en línea o sin conexión.
- La elección depende del ancho de banda, el volumen y el cambio de los datos. Azure Storage Mover migra recursos SMB y NFS en línea con una gestión central; AzCopy sirve para copias puntuales con scripts; Azure File Sync mantiene una caché híbrida a largo plazo; Azure Data Box importa sin conexión grandes volúmenes y se combina con Storage Mover para el delta final.

Design network solutions

- Para la salida a internet, Azure NAT Gateway es el método recomendado: asigna puertos SNAT de forma dinámica, solo permite tráfico de respuesta y da direcciones predecibles. Las IP públicas por instancia y las reglas de salida del equilibrador son alternativas explícitas; el acceso saliente predeterminado es implícito y no se recomienda. Private Link evita SNAT hacia PaaS y Bastion permite administrar VM sin IP pública.
- VPN Gateway cifra el tráfico con IPsec por internet y es la opción sencilla para tráfico ligero. ExpressRoute ofrece un circuito privado con más ancho de banda y latencia constante, pero requiere un proveedor y no cifra por defecto. Una VPN puede coexistir como ruta de respaldo, y Virtual WAN centraliza la conectividad y el tránsito entre sucursales y redes virtuales.
- Las redes aceleradas con SR-IOV pasan el tráfico directamente al hardware virtual del host y reducen latencia, jitter y CPU. Los grupos de selección de ubicación de proximidad colocan las VM cerca y se combinan con ellas, aunque no abarcan zonas. FastPath hace que ExpressRoute omita la puerta de enlace, el emparejamiento de redes virtuales conecta redes con baja latencia y Front Door acelera el contenido global.
- La seguridad de red se compone por capas: los NSG y los grupos de seguridad de aplicaciones filtran entre cargas sin listas de IP; Azure Firewall aplica reglas de red y de aplicación con FQDN e inteligencia de amenazas; WAF protege las aplicaciones web de inyección SQL y XSS; DDoS Protection mitiga ataques volumétricos de capas 3 y 4; Private Link restringe el acceso a PaaS a tu red.
- Los servicios se distinguen por ámbito y capa. Front Door es global y HTTP(S) con aceleración y conmutación rápida; Application Gateway es regional de capa 7 con rutas de URL, TLS y WAF; Load Balancer es de capa 4; Traffic Manager es global y basado en DNS con métodos como geográfico o ponderado. En el enrutamiento, las UDR y el prefijo más largo deciden el siguiente salto.