

Microsoft Certified: Azure Database Administrator Associate

Resumen de los pesos oficiales y habilidades clave del temario de DP-300, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Plan and implement data platform resources

15–20%

Plan and deploy Azure SQL solutions

- Azure SQL Database es PaaS para aplicaciones nativas de la nube, con grupos elásticos para SaaS multiinquilino; Azure SQL Managed Instance ofrece casi toda la compatibilidad de SQL Server (SQL Server Agent, CLR, Service Broker, Database Mail) para migrar con pocos cambios; SQL Server en Azure VMs da control total del sistema operativo y del motor, necesario para características como la ETL y las plantillas ARM (az deployment group create o New-AzResourceGroupDeployment) y con comandos como az sql db create. El modo incremental es el predeterminado y reaplica todas las propiedades; la operación what-if muestra los cambios previstos sin desplegar, y @secure() evita que las contraseñas queden en el historial.
- SQL Server habilitado por Azure Arc lleva la administración de Azure a instancias de centros de datos, ubicaciones perimetrales y otras nubes: inventario consultable con Azure Resource Graph, evaluación de procedimientos recomendados y de migración, Microsoft Defender for Cloud, autenticación con Microsoft Entra ID, pago por uso y Extended Security Updates. Se conecta con tráfico HTTPS saliente.
- SQL Database en Microsoft Fabric es una base de datos transaccional basada en el motor de Azure SQL Database que refleja automáticamente sus datos en OneLake y ofrece un punto de conexión de análisis SQL de solo lectura. Solo admite Microsoft Entra ID y no admite CDC, TDE con claves del cliente ni Always Encrypted; encaja en aplicaciones como A, ODS, ETL inversa y aplicaciones transaccional.
- El particionamiento divide horizontalmente una tabla o índice; la función de partición define los límites (RANGE LEFT o RIGHT) y el esquema asigna particiones a grupos de archivos. Facilita el mantenimiento por partición, el cambio de particiones y la eliminación de particiones en consultas. En Azure SQL Database todo va en PRIMARY y un índice clúster único debe incluir la columna de partición.

Configure resources for scale and performance

- Una base de datos única se escala con T-SQL, el portal, Set-AzSqlDatabase o az sql db update; sigue en línea, pero al final se interrumpen las conexiones, así que la aplicación necesita lógica de reintento. Business Critical, Premium y Hyperscale permiten el escalado horizontal de lectura con ApplicationIntent=ReadOnly, y los grupos elásticos comparan recursos entre bases de datos con precios impredecibles.
- En SQL Server en Azure Virtual Machines, los discos de datos usan caché de host Read Only y los de registro, None; tempdb va en la unidad SSD local D: y los discos de datos se formatean con unidades de asignación de 64 KB. El número de columnas de un grupo de almacenamiento se fija al crearlo, así que añadir discos solo amplía capacidad. En series M, Write Accelerator mejora la latencia de escritura del registro.
- Una función de partición define los límites y si cada valor límite pertenece a la izquierda (RANGE LEFT, predeterminado) o a la derecha (RANGE RIGHT); un esquema de partición asigna las particiones a grupos de archivos. SPLIT RANGE y MERGE RANGE añaden o eliminan límites, SWITCH mueve una partición entera entre tablas y, en Azure SQL Database, todas las particiones quedan en PRIMARY.
- La compresión de filas y de páginas reduce el tamaño de tablas e índices de almacén de filas a cambio de más CPU; se configura por tabla, índice o partición, y los índices no clúster no heredan la compresión de la tabla. sp_estimate_data_compression_savings calcula el ahorro con una muestra en tempdb. Los índices de almacén de columnas admiten además compresión de archivo, más lenta de consultar.

Plan and implement a migration strategy

- Antes de migrar se evalúan el número y tamaño de las bases de datos, el tiempo de inactividad aceptable y las características usadas. SQL Server habilitado por Azure Arc genera automáticamente una evaluación de preparación con recomendaciones de destino y tamaño. Una VM de Azure encaja si se necesita acceso al sistema operativo y el motor, Azure SQL Database no admite trabajos de SQL Server Agent (se usan trabajos elásticos), tiempo de inactividad. Hacia Azure SQL Managed Instance, el vínculo de Managed Instance es la opción en línea con menor inactividad y permite leer el destino, y Log Replay Service en modo continuo también minimiza la inactividad.
- En una migración en línea, el origen sigue activo y replica los cambios hasta la transición; una sin conexión exige hacer una copia de seguridad. Hacia Azure SQL Database o DMS se replica con transaccional; se hace en línea con Log Replay Service en modo continuo se carga la última copia del registro y se ejecuta Complete-AzSqlInstanceDatabaseLogReplay; con el vínculo de Managed Instance se detiene la carga, se comprueba el retraso y se realiza una continuación planificada. Hacia Azure SQL Database se usa replicación transaccional.
- Una migración sin conexión detiene la aplicación durante la copia. Hacia Azure SQL Managed Instance se restaura de forma nativa un .bak desde Azure Blob Storage con una credencial SAS, o se usa Log Replay Service en modo de finalización automática, el único método que restaura copias diferenciales. Hacia Azure SQL Database, un BACPAC importado con sqlpackage es más rápido si se escala el destino y se desactivan las estadísticas automáticas.
- Hacia SQL Server en Azure VMs se puede usar copia de seguridad y restauración de bases de datos y asociadas desde una URL, trasvase de registros o convertir la máquina en VHD para llevar toda la instancia. Azure Database Migration Service necesita un runtime de integración autohospedado si las copias están en un recurso compartido local. SQL Server habilitado por Azure Arc migra a Managed Instance desde el portal.

2. Implement a secure environment

20–25%

Configure database authentication and authorization

- La autenticación de Microsoft Entra se activa al asignar un administrador de Microsoft Entra al servidor lógico o a la instancia administrada; es una sola identidad (usuario, grupo o aplicación) y es la primera que puede crear otras entidades de Entra. No se integra con Azure RBAC, y SQL Managed Instance necesita el rol Directory Readers en su identidad.
- En SQL Server 2022 o posterior en máquinas virtuales de Azure, la autenticación de Microsoft Entra se habilita mediante la extensión SQL IaaS Agent con una identidad administrada que pueda consultar Microsoft Graph; una vez habilitada no se puede deshabilitar. SQL Managed Instance no admite inicios de sesión FROM WINDOWS, pero ofrece autenticación de Windows para entidades de Microsoft Entra mediante Kerberos.
- Las entidades de seguridad de nivel de servidor son los inicios de sesión (SQL, Windows o Microsoft Entra) y los roles de servidor; las de nivel de base de datos son usuarios, roles de base de datos y roles de aplicación. Azure SQL Database ofrece roles fijos de servidor con prefijo ##MS_ que se gestionan desde master, y sus permisos llegan a cada base de datos si el inicio de sesión tiene usuario en ella o pertenece a ##MS_DatabaseConnector##.
- Para una entidad de Microsoft Entra puedes crear un usuario con CREATE USER ... FROM EXTERNAL PROVIDER o un usuario basado en un inicio de sesión con CREATE USER ... FROM LOGIN; ambos no están vinculados aunque compartan nombre. Los usuarios de Entra deben crearlos identidades de Entra, y si el nombre para mostrar de una entidad de servicio no es único se usa WITH OBJECT_ID con un alias.
- En SQL Server Management Studio, la página Permissions o Securables permite conceder o denegar permisos en la pestaña Explicit y ver en la pestaña Effective el resultado combinado con los roles, donde una denegación prevalece. La casilla With Grant es de solo lectura, así que WITH GRANT OPTION se aplica con T-SQL; los permisos por columna se fijan desde Column Permissions.

Implement security for data at rest and data in transit

- El cifrado de datos transparente (TDE) cifra en reposo datos, registros y copias de seguridad a nivel de página mediante una clave de cifrado de base de datos protegida por el protector de TDE. En Azure SQL Database está activo por defecto con clave administrada por el servicio y admite clave del cliente en Azure Key Vault; en SQL Server hay que crear clave maestra, certificada y clave de cifrado, y respaldar el certificado.
- Always Encrypted cifra columnas en el controlador del cliente con claves de cifrado de columna protegidas por una clave maestra de columna guardada fuera de la base de datos. El cifrado determinista admite búsquedas por igualdad, agrupación e índices; el aleatorio es más seguro, y para LIKE, rangos u ordenación se usan enclaves seguros. El cifrado por columna con clave simétrica se hace en T-SQL con EncryptByKey.
- En Azure SQL Database, las reglas de firewall IP de servidor se guardan en master y dan acceso a todas las bases de datos; las de base de datos se guardan en cada base de datos, solo se gestionan con T-SQL y requieren una primera regla de servidor. El firewall comprueba primero las reglas de la base de datos pedida y después las del servidor; la regla 0.0.0.0 admite todos los servicios de Azure.
- Always Encrypted cifra columnas en el controlador del cliente con claves de cifrado de columna protegidas por una clave maestra guardada fuera de la base de datos (por ejemplo, en Azure Key Vault), así que el motor nunca ve claves ni texto sin cifrar. El cifrado determinista admite búsquedas por igualdad, GROUP BY e índices; el aleatorio, sin enclave, no. Los valores se envían siempre como parámetros.
- Always Encrypted con enclaves seguros procesa datos cifrados dentro de una región de memoria protegida del motor, lo que permite cifrar en contexto con ALTER TABLE y consultas con LIKE, rangos y ordenación sobre columnas con cifrado aleatorio y claves habilitadas para enclaves (ENCLAVE_COMPUTATIONS). Las réplicas y secundarias geográficas también deben admitir enclaves.

Implement compliance controls for sensitive data

- Data Discovery & Classification detecta columnas con datos confidenciales, recomienda clasificaciones y guarda etiquetas y tipos de información como metadatos de columna, que la auditoría registra en data_sensitivity_information. Se gestiona en el portal, con T-SQL (ADD SENSITIVITY CLASSIFICATION, sys.sensitivity_classifications).
- PowerShell o la API REST: cada columna tiene una sola clasificación.
- En Azure SQL Database, la auditoría de servidor cubre todas las bases de datos actuales y futuras y puede coexistir con auditorías de base de datos; escribe en Azure Storage, Log Analytics o Event Hubs. En SQL Server y SQL Managed Instance se usa SQL Server Audit: una auditoría de servidor con su destino (archivo, TO URL o EXTERNAL_MONITOR) y especificaciones de servidor o de base de datos.
- El seguimiento de cambios es síncrono y ligero: registra qué filas cambiaron (solo la clave principal) y se consulta con CHANGETABLE y las funciones de versión, ideal para sincronizar. La captura de datos modificados lee el registro de transacciones de forma asíncrona y guarda los valores en tablas de cambios para ETL; en Azure SQL Database la ejecuta un programador en lugar del Agente de SQL Server.
- El enmascaramiento dinámico de datos oculta valores en los resultados sin cambiar los datos almacenados, con funciones como default(), email(), random(), partial() y datetime(). Los administradores y db_owner ven los datos reales; al resto se le concede UNMASK a nivel de base de datos, esquema, tabla o columna. No impide deducir valores con consultas ad hoc ni actualizar la columna.
- El libro de contabilidad aporta detección criptográfica de manipulaciones: las tablas actualizables guardan versiones anteriores en una tabla de historial y las de solo anexión solo admiten inserciones. Los resúmenes se guardan en almacenamiento inmutable o Azure Confidential Ledger y se verifican con sp_verify_database_ledger_from_digest_storage. Una tabla de libro de contabilidad no puede revertirse.

3. Monitor, configure, and optimize database resources

20–25%

Monitor resource activity and performance

- Una línea base es un conjunto de métricas recogidas a lo largo del tiempo que define el rendimiento normal; sin ella no se distingue un problema real de la actividad habitual. En SQL Server en máquinas virtuales se combinan contadores del Monitor de rendimiento (o InfluxDB, Collectd y Grafana en Linux) con estadísticas de espera, y Azure Monitor añade alertas con umbrales dinámicos.
- El monitor de recursos de Azure SQL Database y Azure SQL Managed Instance usa sys.dm_db_resource_stats para datos recientes y detallados y sys.resource_stats (en master) el historial; Managed Instance usa sys.server_resource_stats. Database watcher centraliza la supervisión de los conjuntos de máquinas virtuales para los contadores de SQL Server y percentage miden el consumo respecto al límite de la carga de trabajo de usuario, y DTU percentage coincide con el valor más alto de CPU, E/S de datos y E/S del registro. sys.dm_db_resource_stats ofrece datos de 15 segundos.
- Las reglas de alerta de sys.resource_stats en master devuelven datos de 5 minutos para análisis histórico, notifican mediante grupos de acciones y pueden abarcar una base de datos, un grupo elástico o todo un grupo de recursos o suscripción. Las configuraciones de diagnóstico transmiten métricas y registros a Log Analytics, Event Hubs o Azure Storage y se configuran por separado para grupos elásticos de Azure SQL Database y Azure SQL Managed Instance que recopila datos de más de 70 vistas del sistema en un almacén de Azure Data Explorer o Real-Time Analytics de Microsoft Fabric, con paneles de patrimonio y de recurso en el portal. Se autentica preferentemente con Microsoft Entra mediante su identidad administrada y debe iniciarse tras configurarlo.

Monitor and optimize query performance

- Query Store se configura con ALTER DATABASE SET QUERY_STORE: OPERATION_MODE, MAX_STORAGE_SIZE_MB, SIZE_BASED_CLEANUP_MODE, CLEANUP_POLICY, INTERVAL_LENGTH_MINUTES y QUERY_CAPTURE_MODE (ALL, AUTO, CUSTOM o NONE). Si supera su tamaño pasa a solo lectura, lo que se ve en sys.database_query_store_options. Está activado por defecto en Azure SQL Database y Managed Instance.
- Query Store conserva el historial de consultas, planes, estadísticas de tiempo de ejecución y esperas, lo que permite detectar regresiones de plan y forzar el plan anterior con sp_query_store_force_plan sin tocar la aplicación. En SSMS las vistas Regressed Queries, Top Resource Consuming Queries y Query Wait Statistics ayudan al análisis.
- El plan que se ejecuta de Query Store aplica cambios sin cambiar el código. Si aparece uno incompatible sobre el mismo recurso. Para resolverlo se localiza el origen de la cadena con blocking_session_id de sys.dm_exec_requests, se revisa su última instrucción con sys.dm_exec_input_buffer y se corrige la causa, como transacciones abiertas tras un tiempo.
- Las DMVs permiten el diagnóstico. El rendimiento de sys.dm_db_resource_stats y sys.dm_elastic_pool_resource_stats muestran el consumo reciente, sys.dm_exec_requests y sys.dm_os_waiting_tasks las esperas actuales, y sys.dm_exec_query_stats las estadísticas de los planes en caché. Los tipos de espera orientan el diagnóstico: PAGEIOLATCH indica E/S de datos, WRITELOG E/S del registro y RESOURCE_SEMAPHORE esperas de memoria.
- Las sugerencias de índices que faltan aparecen en los planes de ejecución y en DMV como sys.dm_db_missing_index_details, pero son estimaciones previas a la ejecución, se borran al reiniciar o conmutar y solo proponen índices no agrupados. Antes de crearlos hay que combinarlas con los índices existentes, poner las columnas de igualdad antes que las de desigualdad y validar el cambio con Query Store; los índices filtrados sirven para subconjuntos.

Configure database solutions for optimal performance

- Mide la fragmentación y la densidad de página de los índices rowstore con sys.dm_db_index_physical_stats antes de actuar. La reorganización consume menos recursos, siempre es en línea y solo desfragmenta el nivel hoja; la regeneración elimina la fragmentación en todos los niveles y actualiza las estadísticas del índice con un examen completo. En Azure SQL, use la regeneración o regeneración operativa si es necesario.
- Mantén activada la SQL, use la regeneración o regeneración operativa si es necesario. Añade actualizaciones manuales con UPDATE STATISTICS o sp_updatestats tras cargas masivas o en claves ascendentes. sys.dm_db_stats_properties muestra la última actualización y el contador de modificaciones. PERSIST_SAMPLE_PERCENT conserva el muestreo elegido, NORECOMPUTE desactiva la actualización automática y la asíncrona coincide con las estadísticas existentes.
- DBCC CHECKDB ejecuta comprobaciones de asignación, de tablas y del catálogo usando una instantánea interna de la base de datos. PHYSICAL_ONLY es una opción ligera para ejecuciones frecuentes en producción, con comprobaciones completas periódicas. Es preferible restaurar una copia de seguridad buena que usar REPAIR. Azure SQL Database gestiona la integridad y no permite reparaciones del cliente; Hyperscale usa DBCC CHECKTABLE en línea automática.
- El ajuste automático ofrece FORCE_LAST_GOOD_PLAN, CREATE_INDEX y DROP_INDEX en Azure SQL Database, pero solo FORCE_LAST_GOOD_PLAN en Azure SQL Managed Instance, que se configura con T-SQL. Conviene configurarlo en el servidor lógico y que las bases de datos lo hereden. Las acciones aplicadas automáticamente se ejecutan en paralelo.
- Mantén la validez de los planes de ejecución y fuerza el plan anterior con sp_query_store_force_plan para planes de ejecución en serie las consultas baratas, optimize for ad hoc workloads guarda solo un stub de plan para lotes de un solo uso y max y min server memory acotan el grupo de búferes. En máquinas virtuales de Azure, usa caché de solo lectura en datos, ninguna en el registro y tempdb en la SSD local.

15–20%

20–25%