

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

1. Implement and manage user identities

20–25%

Configure and manage a Microsoft Entra tenant

- Los roles integrados tienen permisos fijos que no se pueden modificar; los roles personalizados son una colección de permisos que se elige de una lista predefinida. Conceder acceso es un proceso de dos pasos: definir el rol y asignarlo a una entidad de seguridad de usuario o grupo de entidad de servicio de un ámbito que se define por una entidad administrativa o un recurso, y no se pueden anidar. Si hace falta proteger objetos sensibles incluso frente a administradores de nivel de raíz, cree una unidad administrativa de administración restringida que se delega a un administrador de grupo principal, asigne usuarios, grupos o dispositivos como miembros y asigne roles con ámbito de entidad de seguridad que se asigne a una entidad de seguridad (usuarios o dispositivos, o ambos) y antes de eliminar una entidad de seguridad, su asignación, una entidad administrativa o recurso. Un rol con ámbito de unidad solo actúa sobre sus miembros y no sobre usuarios, es el rol de administrador de grupo sobre valores de todos los ámbitos. Algunos roles personalizados se ven acompañados con roles de menor privilegio, solo puede verificarse en un directorio; los subdominios se verifican con el dominio raíz. Para eliminar un dominio hay que quitar antes sus referencias, o usar ForceDelete.

Create, configure, and manage Microsoft Entra identities

- Los usuarios se crean en Entra ID > Usuarios como miembros internos, invitados internos, miembros externos o invitados externos. User Administrator es el rol de menor privilegio para crear usuarios y Guest Inviter puede invitar a los grupos de seguridad de usuarios eliminados y permanece 30 días en Usuarios, dispositivos y entidades de seguridad, los grupos de seguridad de usuarios para otros usuarios, pero admiten invitados externos. La pertenencia puede ser asignada o dinámica (de usuarios o dispositivos) y un valor de organización se asocia a los grupos de seguridad que se crean y se asignan a usuarios y a dispositivos en el sistema. Global Administrator no tiene permisos por defecto: Attribute Definition Administrator, de User Attribute Assignment, crea, elimina o asigna los atributos no se eliminan, solo se desactivan o se reproprietan de grupos de tipos de dispositivos como se identifica mediante registro (BYOD y móviles), un atributo de organización se usa en el caso de Microsoft Graph PowerShell (Active Directory local más Microsoft Entra). Los ajustes de dispositivos controlan quién puede unir o registrar, la MFA, el límite por usuario y los administradores de organización grandes se usan en el caso de Microsoft Graph PowerShell (Active Directory local más Microsoft Entra).

Implement and manage identities for external users and tenants

- La configuración de colaboración externa define qué pueden ver los invitados en el directorio (mismo acceso que los miembros, acceso limitado por defecto o solo su propio perfil), quién puede invitar (todos, miembros y roles de administrador, solo roles como User Administrator o Guest Inviter o nadie) y quién puede registrar por autosección de usuario externo en las peticiones de colaboración (lista de permisos de cada rol, que puede ser un recurso). Al crearla se pueden asignar grupos de usuarios (los roles en el rol de Privileged Role Administrator). Para muchos usuarios, la invitación masiva usa una plantilla CSV. Las nuevas primeras filas no se pueden modificar (Microsoft Entra Administrator) permite cambiar el correo o el proveedor conservando el objeto, los grupos y las asignaciones. Las cuentas internas se pueden convertir a B2B, y los usuarios externos pueden abandonar la organización según la configuración de salida de Microsoft Entra mediante configuración entrante, saliente y de confianza (MFA y dispositivos). Los valores predeterminados permiten la colaboración B2B y bloquean la conexión directa; la configuración organizativa de la sincronización entre inquilinos envía usuarios internos desde un inquilino de origen a uno de destino como prevalece sobre ellos. Requiere al menos Security Administrator y el canje automático debe marcarse en ambos inquilinos.

Implement and manage hybrid identity

- Microsoft Entra Connect Sync es el motor de sincronización local de Microsoft Entra Connect: crea y mantiene usuarios, grupos y otros objetos, y sincroniza los hashes de contraseña. Solo puede haber un servidor activo; un secondary servidor usa modo de grupo (sincroniza importación de Active Directory con exportación a Azure para sincronizar los datos y para publicar los datos antes de activarlos) conexiones salientes; la configuración se administra en la nube. Admite la sincronización de datos con configuración de entrada de Microsoft Entra Connect. Incluye filtros de ámbito, asignación de atributos, canje de contraseñas, sincronización de contraseñas en la nube y eliminación de credenciales filtradas. Las reglas de complejidad de contraseñas se aplican a las contraseñas de los usuarios de la nube y no a las de los usuarios de AD FS. También puede ser de sincronización de contraseñas con AD FS en la nube ni requerir red perimetral. Funciona con el acceso condicional. Para alta disponibilidad se instalan más agentes en otros dispositivos (uno por servidor) de la sincronización automática a la sincronización de hashes de contraseñas con sincronización de hash de contraseña o autenticación transferida, no con AD FS. Crea la cuenta AZUREADSSOACC en cada bosque y exige añadir la URL de autologon a la zona Intranet local; conviene renovar periódicamente su clave Kerberos.

2. Implement authentication and access management

25–30%

Plan, implement, and manage Microsoft Entra user authentication

- La directiva de métodos de autenticación es el lugar recomendado para habilitar métodos para todos los usuarios o para grupos concretos, y sustituye a las directivas heredadas de MFA y SSPR. Las intensidades de autenticación de acceso condicional exigen combinaciones concretas de métodos, y Microsoft recomienda métodos resistentes al phishing como Windows Hello para empresas, claves de acceso FIDO2 y certificados.
- Un pase de acceso temporal es un código con duración limitada, de un solo uso o de uso múltiple, que sirve para autenticación principal y para incorporar métodos sin contraseña o recuperar el acceso. Las claves de acceso FIDO2, la autenticación basada en certificados, Windows Hello para empresas y Microsoft Authenticator con claves de acceso están entre los métodos resistentes al phishing.
- Informar de actividad sospechosa sustituye a las funciones heredadas de bloqueo de usuarios, alerta de fraude y notificaciones, y marca al usuario con riesgo alto en ID Protection. Los ajustes de servicio heredados incluyen direcciones IP de confianza y recordar la MFA en dispositivos de confianza, aunque se recomiendan las ubicaciones.
- El restablecimiento de contraseña de autoservicio se habilita para ninguno, usuarios seleccionados o todos, y con nombre de acceso condicional.
- lo configura al menos un administrador de directivas de autenticación. Se define cuántos métodos hacen falta, uno o dos, y los usuarios deben registrarlos; los usuarios con contraseña local necesitan la escritura diferida de Windows Hello para empresas combina una clave asimétrica ligada al dispositivo, protegida por el TPM, con un PIN o un gesto biométrico, y los datos biométricos no salen del dispositivo. En entornos híbridos, la confianza Kerberos en la nube es el modelo recomendado porque no requiere PKI. El restablecimiento de PIN no destructivo necesita

Plan, implement, and manage Microsoft Entra Conditional Access

- Planifica el acceso condicional como reglas si-entonces: asignaciones (usuarios, recursos, condiciones) más controles de concesión o de sesión. Una directiva solo actúa cuando se cumplen sus condiciones, así que combina una directiva acotada con otra de bloqueo para el resto. Excluye las cuentas de acceso de emergencia, valida con el modo solo informe y la herramienta What If, y despliega por fases.
- Las asignaciones definen a quién y a qué se dirige una directiva. Se pueden incluir o excluir usuarios, grupos, roles de directorio integrados, invitados o externos e identidades de carga de trabajo; la exclusión prevalece sobre la inclusión. Los recursos pueden ser aplicaciones, Todos los recursos, acciones de usuario o contextos de autenticación, y condiciones como plataforma, cliente, ubicación y riesgo acotan el ámbito.
- Los controles de concesión bloquean el acceso o lo conceden si se cumplen requisitos: MFA, nivel de autenticación, dispositivo compatible, dispositivo unido a Microsoft Entra híbrido, protección de aplicaciones y cambio de contraseña. Con varios controles se exige todos o uno. El cambio de contraseña debe dirigirse a Todos los recursos y no se combina con otros controles; MFA y nivel de autenticación no pueden coexistir en una directiva.
- Prueba antes de aplicar: el modo solo informe evalúa las directivas con inicios de sesión reales sin aplicarlas, y los resultados aparecen en los registros de inicio de sesión y en el libro de Información e informes. La herramienta What If simula un inicio de sesión y lista las directivas que se aplican y las que no, con el motivo. Ante un fallo real, los controles de sesión limitan lo que ocurre tras conceder el acceso: restricciones exigidas por la aplicación, Conditional Access App Control, frecuencia de inicio de sesión, sesión persistente del explorador, evaluación continua de acceso, protección de tokens y valores de resistencia. La frecuencia define cuándo hay que reautenticarse y la
- Maneja el riesgo de usuario de Microsoft Entra ID Protection tras cerrar el explorador.

Maneja el riesgo de usuario de Microsoft Entra ID Protection

- La directiva de riesgo de usuario se crea en acceso condicional con la condición Riesgo de usuario, y Microsoft recomienda aplicarla con nivel Alto y el control Requerir corrección de riesgo. Ese control añade automáticamente la intensidad de autenticación y la frecuencia de inicio de sesión en cada vez: los usuarios con contraseña hacen MFA y un cambio de contraseña seguro, y a los usuarios sin contraseña se les revocan las sesiones.
- La directiva de riesgo de inicio de sesión se crea en acceso condicional, en una directiva distinta de la de riesgo de usuario. Se recomienda exigir la intensidad de autenticación Autenticación multifactor con riesgo medio o alto y frecuencia de inicio de sesión en cada vez, excluir las cuentas de emergencia y probar antes en modo de solo informe. Los usuarios deben estar registrados en MFA para autocorregirse.
- La directiva de métodos de autenticación habilita métodos para todos los usuarios o para grupos concretos, y la campaña de registro se configura en ella con el rol Administrador de directivas de autenticación. La campaña invita a configurar Authenticator o una passkey tras completar la MFA, con opción de posponer. El Pase de acceso temporal
- ID Protection ofrece los informes Usuarios de riesgo, Inicios de sesión de riesgo y Detecciones de riesgo. Tras y el acceso condicional sobre Registrar información de seguridad protegen el registro.
- investigar, un administrador puede confirmar el compromiso, confirmar como seguro o descartar el riesgo; el rol Operador de seguridad basta para descartar el riesgo de usuario. Para corregir se pueden generar una contraseña temporal, exigir un cambio de contraseña o bloquear al usuario.
- ID Protection detecta riesgo en entidades de servicio y aplicaciones, pero no en identidades administradas. Se investiga en el informe Identidades de carga de trabajo de riesgo, donde se puede descartar el riesgo, confirmar el compromiso o deshabilitar la entidad de servicio. El acceso condicional para identidades de carga de trabajo solo

Implement Global Secure Access

- El cliente de Global Secure Access envía al servicio solo el tráfico definido por los perfiles de reenvío y deja el resto directo a la red. Existe para Windows, macOS, Android e iOS: en Windows y macOS se despliega con paquetes y perfiles de Intune, y en Android e iOS forma parte de Microsoft Defender for Endpoint. Claves de registro o configuración de aplicaciones controlan que acciones ven los usuarios.
- Quick Access agrupa el conjunto principal de destinos, mientras que las aplicaciones empresariales de Global Secure Access ofrecen segmentos por aplicación, asignación de usuarios y acceso condicional propios. Los conectores de red privada, en grupos sobre Windows Server, solo hacen conexiones salientes.
- web, la inteligencia de amenazas, la inspección TLS y las directivas de contenido se agrupan en perfiles de seguridad que se entregan con controles de sesión de acceso condicional; el perfil de línea base se aplica a todo
- El perfil de tráfico de Microsoft adquiere el tráfico hacia servicios de Microsoft 365 con reglas derivadas de la lista de IP y FQDN de Microsoft 365, agrupadas por carga de trabajo como Exchange Online o SharePoint Online. Cada regla o grupo puede ir en Forward o Bypass, y el perfil puede limitarse a usuarios, grupos o redes remotas. Lo habilita el administrador de Global Secure Access y hace falta para restaurar la IP de origen.

3. Plan and implement workload identities

20-25%

Plan and implement identities for applications and Azure workloads

- Las identidades administradas dan a los recursos de Azure una identidad de Microsoft Entra cuyas credenciales gestiona y rota Azure, por lo que son la opción preferente en Azure. Usa una entidad de servicio (registro de aplicación) fuera de Azure, mejor con certificado. Evita las cuentas de usuario como cuentas de servicio; en local usa gMSA y, si no, sMSA.
- Una identidad asignada por el sistema se crea al habilitarla en un recurso de Azure y se elimina con él; una asignada por el usuario es un recurso independiente que se crea en un grupo de recursos. Crear o eliminar identidades asignadas por el usuario requiere el rol Managed Identity Contributor. Se crean desde el portal, con az identity create o con New-AzUserAssignedIdentity.
- La identidad asignada por el sistema se habilita en el propio recurso y exige permiso de escritura sobre él (por ejemplo Virtual Machine Contributor); asignar una identidad asignada por el usuario exige además el rol Managed Identity Operator sobre la identidad. Un recurso puede combinar ambos tipos y en App Service la configuración es específica de cada slot.
- Tras asignar la identidad hay que darle acceso al destino, normalmente con una asignación de rol de Azure RBAC (por ejemplo Storage Blob Data Reader o Key Vault Secrets User). El código pide tokens al punto de conexión local y debe indicar la identidad si hay varias asignadas por el usuario. Los permisos de Microsoft Graph se conceden

Plan, implement, application, monitor the integration of enterprise applications

- Los ajustes de las aplicaciones empresariales se aplican en dos niveles. Las propiedades de cada aplicación (habilitada para iniciar sesión, asignación requerida, visible para los usuarios, logotipo y URL de inicio) las configura un administrador o propietario en el panel Propiedades. A nivel de inquilino se controlan quién puede registrar aplicaciones, como consentir los usuarios y el flujo de consentimiento del administrador.
- El Administrador de aplicaciones administra aplicaciones empresariales, registros de aplicaciones y la configuración de Application Proxy; el Administrador de aplicaciones en la nube tiene los mismos permisos salvo Application Proxy. Ninguno administra el acceso condicional y ambos pueden agregar credenciales a una aplicación. Un propietario administra solo las aplicaciones que posee.
- Application Proxy publica aplicaciones web locales mediante un servicio en la nube y un conector de red privada que usa solo conexiones de salida, sin abrir puertos de entrada. Los conectores se organizan en grupos, la preautenticación con Microsoft Entra ID habilita el acceso condicional y la delegación restringida de Kerberos da inicio de sesión único a aplicaciones con autenticación integrada de Windows desde un conector unido al dominio. Las aplicaciones SaaS se agregan desde la galería de Microsoft Entra con Nueva aplicación, lo que crea una aplicación empresarial a la que conviene asignar propietarios. El método de inicio de sesión único depende de cómo autentica la aplicación: OpenID Connect y OAuth si los admite, SAML para aplicaciones existentes sin ellos.
- Los usuarios y grupos se asignan en el panel Usuarios y grupos de la aplicación empresarial, con un rol de aplicación definido en el registro; sin roles se usa el acceso predeterminado. La asignación de grupos no se propaga a grupos anidados. Asignación requerida limita quién obtiene tokens, y deshabilitar un rol de aplicación no elimina

Plan and implement app registrations.

- Antes de registrar una app decide quién podrá usarla (un inquilino, varios o cuentas personales), quién puede registrarla (Application Developer si restringes el ajuste de usuarios) y qué identidad conviene. Una identidad administrada es preferible si la app corre en Azure y no inicia sesión de usuarios. El objeto de aplicación vive en el registro de origen y cada inquilino que la usa tiene su entidad de servicio.
- El registro se hace en el Centro de administración de Microsoft Entra, en Registros de aplicaciones, con al menos el rol Application Developer. Eliges un nombre y los tipos de cuenta admitidos, y se te asigna un id. de aplicación (cliente) único. Registrar una app establece una confianza unidireccional con la plataforma de identidad y crea el objeto de aplicación y su entidad de servicio en el inquilino de origen.
- En Autenticación agregas los URI de redirección por plataforma (Web, página única, Android, iOS/macOS, móvil y escritorio); coinciden con distinción de mayúsculas y solo admiten http en localhost. Los clientes públicos activan Permitir flujos de cliente público y no llevan secretos. Para credenciales, Microsoft prefiere identidad administrada.
- En Permisos de API agregas permisos delegados (la app actúa en nombre de un usuario y solo llega a lo que este puede) o permisos de aplicación (sin usuario, para servicios y daemons). Los permisos de aplicación exigen el consentimiento de un administrador, mientras que los delegados pueden consentirlos los usuarios salvo que sean de alto privilegio. Pide siempre el mínimo necesario y revoca lo que sobre.
- Los roles de aplicación se definen en el registro de la app o de la API (nombre para mostrar, tipos de miembros permitidos, valor sin espacios, descripción y estado habilitado). Se asignan a usuarios y grupos desde Aplicaciones empresariales o a otras apps como permisos de aplicación con consentimiento de administrador. Llegan al token

Manage and monitor app access by using Microsoft Defender for Cloud Apps

- Cloud Discovery analiza los registros de tráfico con el catálogo de aplicaciones en la nube para dar visibilidad del shadow IT y del riesgo de las aplicaciones. Los informes continuos proceden de la integración con Defender for Endpoint, de un recopilador de registros o de una puerta de enlace web segura; los instantáneos, de registros cargados a mano. En el panel se filtran las aplicaciones detectadas y se excluyen entidades ruidosas.
- Los conectores de aplicaciones usan las API del proveedor, cifradas con HTTPS, para dar visibilidad de cuentas y actividades y acciones de gobernanza como suspender usuarios, quitar tokens de aplicaciones o poner archivos en cuarentena. Se pueden conectar varias instancias de una misma aplicación, salvo Microsoft 365 y Azure. Para usar restricciones exigidas por la aplicación es un control de sesión del acceso condicional que hace que Microsoft 365 haya que habilitar la auditoría y usar un rol de administrador de aplicaciones.
- Entra ID pase la información del dispositivo a SharePoint Online o Exchange Online, que ofrecen una experiencia limitada o completa según el dispositivo esté administrado y sea compatible. En SharePoint, el acceso limitado es solo web, sin descargar, imprimir ni sincronizar; en Exchange se usa Set-OwamMailboxPolicy.
- El control de aplicaciones de acceso condicional dirige las sesiones de navegador a Defender for Cloud Apps mediante una directiva de acceso condicional con el control de sesión Usar control de aplicaciones de acceso condicional (solo supervisión, bloquear descargas o personalizada). Las aplicaciones de Entra se incorporan solas y las de otros proveedores de identidad, a mano. Solo funciona en el navegador.
- Las directivas de acceso permiten (Auditar) o bloquean el acceso según usuario, dispositivo, ubicación, aplicación y aplicación cliente; el filtro Móvil y escritorio alcanza a los clientes integrados. Las directivas de sesión permiten el acceso pero controlan la sesión: Solo supervisión, Bloquear actividades o controlar carga y descarga con inspección, con las acciones Auditar, Bloquear o Proteger. Si hay conflicto, gana la más restrictiva.

4. Plan and automate identity governance

20–25%

Plan and implement entitlement management in Microsoft Entra

- La administración de derechos agrupa en un paquete de acceso los roles de recurso que necesita una identidad, regulados por directivas que definen quién solicita, quién aprueba y cuándo caduca. Los paquetes viven en catálogos, que permiten delegar con los roles de creador de catálogos, propietario y administrador de paquetes.
- Un catálogo es un contenedor de recursos y paquetes de acceso; lo crea un administrador o un creador de identidades internas y externas requieren directivas distintas.
- Los catálogos, que pasa a ser su propietario. Admite grupos creados en la nube, aplicaciones empresariales y sitios de SharePoint, pero no grupos de AD local ni de distribución. Habilitado para usuarios externos controla las solicitudes de autoservicio, y solo se elimina sin paquetes.
- Un paquete de acceso se crea dentro de un catálogo y no se puede mover a otro después. Incluye roles de recurso de los recursos del catálogo y necesita al menos una directiva: para usuarios del directorio, para usuarios ajenos o solo asignación directa. La directiva fija aprobación por etapas, caducidad y revisiones; el ajuste Oculto controla si aparece en el portal My Access.
- En la pestaña Solicitudes de un paquete se ve quién solicitó, con qué directiva y en qué estado; el historial muestra quién aprobó y con qué justificación. Las solicitudes parcialmente entregadas o fallidas pueden reprocesarse, y las pendientes no entregadas cancelarse. Quitar una solicitud completada no quita la asignación, y nadie puede aprobar su propia solicitud.
- Los términos de uso de Microsoft Entra se cargan como PDF, pueden ofrecerse en varios idiomas y se exigen mediante una directiva de acceso condicional antes de acceder a la aplicación. Permiten obligar a expandirlos, a aceptar en cada dispositivo o a volver a aceptar con caducidad. Un informe y los registros de auditoría muestran

Plan, implement, and manage access reviews in Microsoft Entra

- Planificar una revisión implica decidir qué recursos se revisan, el acceso de quién, con qué frecuencia, quién revisa (propietarios, delegados, los propios usuarios o sus responsables, con revisores alternativos) y qué acción automática se aplica si no hay respuesta. Conviene empezar con un piloto en recursos no críticos y sin aplicar
- Las revisiones se crean en ID Governance > Access Reviews, eligiendo recurso (grupos o aplicaciones), ámbito (todos o solo invitados), revisores, duración y periodicidad. En los ajustes se define la aplicación automática de resultados, qué ocurre si los revisores no responden, los asistentes de decisión, la justificación, los recordatorios y las fases múltiples.
- La página Overview muestra el progreso de la instancia actual y Results permite detener, restablecer y descargar los resultados en CSV; Review history conserva las instancias anteriores. Las acciones de las revisiones quedan en los registros de auditoría de Microsoft Entra, que se pueden exportar a Log Analytics, y también se pueden crear
- Los revisores abren la revisión desde el correo o My Access y eligen Approve, Deny o Don't know para cada usuario, con motivo si se exige, y pueden cambiar su respuesta hasta que termine la revisión. Los denegados se quitan al finalizar o al detener la revisión; con varios revisores prevalece la última respuesta enviada.

Plan and implement privileged access

- En PIM los roles de Microsoft Entra ofrecen acceso justo a tiempo: las asignaciones pueden ser elegibles o activas, permanentes o con fecha de fin. Los ajustes se definen por rol (duración máxima de activación, MFA, contexto de autenticación, justificación, aprobación y notificaciones) y para gestionarlos hace falta al menos Privileged Role Administrator.
- Los roles de recursos de Azure en PIM los gestionan administradores de la suscripción, Owner o User Access Administrator del recurso. Los ajustes son por rol y por recurso, y no se heredan de una suscripción a un grupo de recursos. Al activar, el usuario puede reducir el ámbito, y la aprobación exige elegir al menos un aprobador porque no hay predeterminados.
- PIM para grupos permite conceder pertenencia o propiedad justo a tiempo en grupos de seguridad y de Microsoft 365, con una directiva para la pertenencia y otra para la propiedad. Los grupos dinámicos y los sincronizados desde
- Cuando se puede delegar administración y los asignadores de Microsoft Entra a un grupo o este debe solicitar Approve requests; la resuelve el primer aprobador que responde. Los aprobadores no necesitan ningún rol y disponen de 24
- Para el rol Resource administrator en roles de Microsoft Entra, uno o varios auditores (solo de aprobación propia) y sus datos son un subconjunto de los registros de auditoría de Microsoft Entra. Para conservarlos más tiempo se usa la configuración de diagnóstico hacia Log Analytics o almacenamiento, y en Azure se pueden exportar las

Monitor identity activity by using logs, workbooks, and reports

- Los registros de inicio de sesión, auditoría y aprovisionamiento están en Monitoring & health del centro de administración de Microsoft Entra, y Reports Reader es el rol mínimo para leerlos. Los de inicio de sesión incluyen accesos interactivos, no interactivos, de entidades de servicio e identidades administradas; los de auditoría, cambios
- Las configuraciones de diagnóstico envían los registros de Microsoft Entra a un área de trabajo de Log Analytics, una cuenta de almacenamiento o un event hub, y puedes crear varias con destinos distintos. Security Administrator es el rol mínimo para crearlas y el destino debe existir de antemano. Usa Log Analytics para consultar, un event
- En Log Analytics consulta los registros de Entra con KQL, partiendo de una tabla como SigninLogs, AuditLogs o AADProvisioningLogs y encadenando operadores como where, project, extend, summarize y sort. ago() limita el rango, bin() agrupa por tiempo y en SigninLogs un ResultType igual a 0 indica éxito. Cada solicitud aparece por separado, así que agrupa por CorrelationId para obtener un resultado por inicio de sesión.
- Los libros de Microsoft Entra visualizan datos de identidad y requieren un área de trabajo de Log Analytics que reciba los registros mediante la configuración de diagnóstico. Las plantillas públicas cubren brechas de acceso condicional, autenticación heredada, operaciones sensibles, acceso entre inquilinos, solicitudes de autenticación y riesgo. Usage and insights añade actividad de aplicaciones, métodos y credenciales.
- Identity Secure Score es un porcentaje que indica cuánto sigue tu inquilino las recomendaciones de seguridad de identidad de Microsoft y es la parte de identidad de Microsoft secure score. Se recalcula cada día, algunas acciones dan puntuación parcial y cada acción de mejora tiene un estado como To address, Planned, Risk accepted o Resolved through third party. No mide la probabilidad de sufrir una brecha.