**Introducción**

El acceso a los recursos de Azure se controla mediante cuentas de usuario e identidades definidas en Microsoft Entra ID. Microsoft Entra ID admite cuentas de grupo para ayudarle a organizar las cuentas de usuario y facilitar la administración.

En este módulo, su empresa quiere aprovechar las características de la cuenta de usuario y grupo en Microsoft Entra ID. Debe comprender los conceptos de cuentas de usuario y cuentas de grupo. Busca información sobre cómo crear, configurar y administrar estas cuentas. La organización necesita compatibilidad con la configuración masiva de opciones, la organización de cuentas de grupo y la administración de cuentas en varios directorios.

En este módulo, obtendrá información sobre las cuentas de usuario y las cuentas de grupo. Obtendrá información sobre un acceso directo de administrador para la creación masiva de cuentas de usuario. Obtenga información sobre cómo controlar el acceso de administrador a través de unidades administrativas. También simula la creación de usuarios y grupos en Azure Portal.

El objetivo de este módulo es crear y administrar correctamente cuentas de usuario y grupo.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Cree y configure cuentas de usuario, incluidas las propiedades de la cuenta y las actualizaciones masivas.
* Cree y configure cuentas de grupo, incluida la asignación de miembros del grupo.
* Use unidades administrativas para controlar el acceso de administrador.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/credentials/certifications/exams/az-104/).

**Requisitos previos**

* Comprenda los conceptos básicos de las soluciones de identidad centralizadas. Este conocimiento incluye identidades, cuentas y métodos de autenticación.
* Familiaridad con la administración de cuentas de usuario y grupo, incluido el principio de privilegios mínimos.

**Crear las cuentas de usuario**

Cada usuario que desee acceso a los recursos de Azure precisa una cuenta de usuario de Azure. Una cuenta de usuario contiene toda la información necesaria para autenticar al usuario durante el proceso de inicio de sesión. Microsoft Entra ID admite tres tipos de cuentas de usuario. Los tipos indican dónde se define el usuario (en la nube o en el entorno local) y si el usuario es interno o externo a la organización de Microsoft Entra.

**Aspectos que se deben conocer sobre las cuentas de usuario**

En la tabla siguiente se describen las cuentas de usuario admitidas en Microsoft Entra ID. A medida que revise estas opciones, tenga en cuenta qué tipos de cuentas de usuario se adaptan a su organización.

| **Cuenta de usuario** | **Descripción** |
| --- | --- |
| **Identidad en la nube** | Las cuentas de usuario con una *identidad en la nube* solo se definen en Microsoft Entra ID. Este tipo de cuenta de usuario incluye cuentas de administrador y usuarios que se administran como parte de la organización. Una identidad en la nube puede ser para las cuentas de usuario definidas en la organización de Microsoft Entra y también para las cuentas de usuario definidas en una instancia externa de Microsoft Entra. Cuando se quita una identidad en la nube del directorio principal, se elimina la cuenta de usuario. |
| **Identidades sincronizadas con Directory** | Las cuentas de usuario que tienen una *identidad sincronizada con Directory* se definen en una instancia local de Active Directory. Se realiza una actividad de sincronización a través de Microsoft Entra Connect para incorporar estos usuarios a Azure. El origen de estas cuentas es Windows Server Active Directory. |
| **Usuario invitado** | Las cuentas de *usuario invitado* se definen fuera de Azure. Algunos ejemplos son las cuentas de usuario de otros proveedores de nube y cuentas de Microsoft, como una cuenta de Xbox Live. El origen de las cuentas de usuario invitado es Usuario invitado. Las cuentas de usuario invitado son útiles cuando los proveedores externos o los contratistas necesitan acceso a sus recursos de Azure. |

**Aspectos que se deben tener en cuenta al elegir cuentas de usuario**

* **Tenga en cuenta dónde se definen los usuarios**. Determine dónde se definen los usuarios. ¿Se definen todos los usuarios dentro de la organización de Microsoft Entra o algunos de ellos se definen en instancias externas de Microsoft Entra? ¿Tiene usuarios externos a su organización? Es habitual que las empresas admitan dos o más tipos de cuenta en su infraestructura.
* **Considere la posibilidad de admitir colaboradores externos**. Permita que los colaboradores externos accedan a los recursos de Azure de su organización al admitir el tipo de cuenta de **usuario invitado**. Cuando el colaborador externo ya no requiera acceso, puede eliminar la cuenta de usuario y sus privilegios de acceso.
* **Considere usar una combinación de cuentas de usuario**. Implemente los tipos de cuenta de usuario que permiten a su organización satisfacer sus necesidades empresariales. Admita cuentas de usuario de identidad sincronizada con Directory para los usuarios definidos en Windows Server Active Directory. Admita identidades en la nube para los usuarios definidos en la estructura interna de Microsoft Entra o para usuarios definidos en una instancia externa de Microsoft Entra.

**Creación masiva de cuentas de usuario**

Microsoft Entra ID admite varias operaciones masivas, como la creación y eliminación masivas de cuentas de usuario. El enfoque más común para este tipo de operaciones es usar Azure Portal. Se puede usar Azure PowerShell para la carga masiva de cuentas de usuario.

**Aspectos que se deben conocer sobre las operaciones de cuentas masivas**

Vamos a examinar algunas características de las operaciones masivas Azure Portal. Este es un ejemplo que muestra la opción **Creación masiva de usuarios** para nuevas cuentas de usuario en Microsoft Entra ID:

* Solo los administradores globales o los administradores de usuarios tienen privilegios para crear y eliminar cuentas de usuario en Azure Portal.
* Para completar operaciones de creación o eliminación masivas, el administrador rellena una plantilla de valores separados por comas (CSV) de los datos de las cuentas de usuario.
* Las plantillas de operación masiva se pueden descargar desde el Centro de administración de Microsoft Entra.
* Se pueden descargar listas masivas de cuentas de usuario.

**Aspectos que se deben tener en cuenta al crear cuentas de usuario**

Estas son algunas consideraciones de diseño para crear y eliminar cuentas de usuario. Piense en qué convenciones y procesos de cuenta de usuario podrían ser necesarios para su organización.

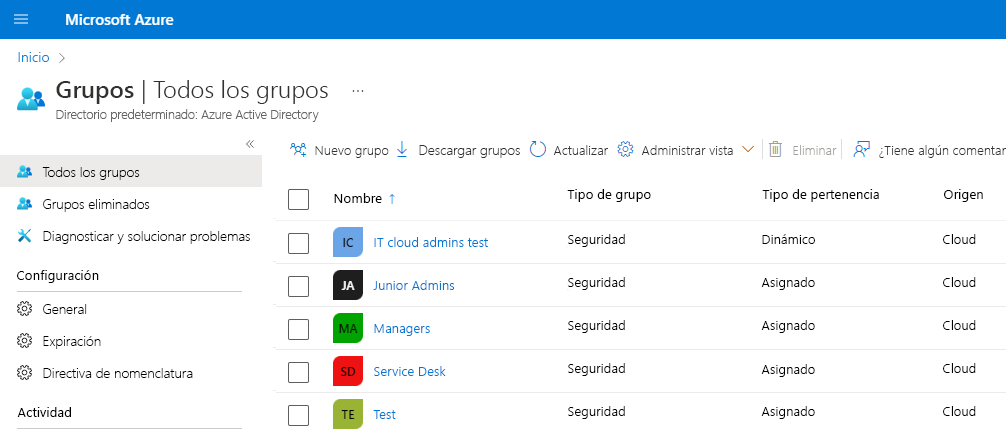
* **Considere el uso de convenciones de nomenclatura**. Establezca o implemente una convención de nomenclatura para las cuentas de usuario. Aplique convenciones a los nombres de cuenta de usuario, los nombres para mostrar y los alias de usuario para que haya coherencia en toda la organización. Las convenciones para nombres y alias pueden simplificar el proceso de creación masiva mediante la reducción de áreas de unicidad en el archivo CSV. Una convención para los nombres de usuario podría comenzar con el apellido del usuario seguido de un punto y terminar con el nombre del usuario, como en Sawyer-Miller.Aran@contoso.com.
* **Considere la posibilidad de usar contraseñas iniciales**. Implante una convención para la contraseña inicial de un usuario recién creado. Diseñe un sistema para notificar a los nuevos usuarios sobre sus contraseñas de forma segura. Puede generar una contraseña aleatoria y enviarla por correo electrónico al nuevo usuario o a su administrador.
* **Considere las estrategias para minimizar errores**. Vea y solucione los errores; para ello, descargue el archivo de resultados en la página **Resultados de la operación masiva** en Azure Portal. El archivo de resultados contiene el motivo de cada error. Un error puede ser una cuenta de usuario que ya se ha creado o una cuenta duplicada. Por lo general, es más fácil cargar y solucionar problemas de grupos de usuarios más pequeños.

**Creación de cuentas de grupo**

Microsoft Entra ID permite a su organización definir dos tipos diferentes de cuentas de grupo. Los **grupos de seguridad** se usan para administrar el acceso de miembros y equipos a los recursos compartidos de un grupo de usuarios. Puede crear un grupo de seguridad para una directiva de seguridad específica y aplicar los mismos permisos a todos los miembros del grupo. Los **grupos de Microsoft 365** proporcionan oportunidades de colaboración. Los miembros del grupo tienen acceso a un buzón, un calendario, archivos, un sitio de SharePoint y muchos más recursos compartidos.

**Aspectos que debe conocer sobre la creación de cuentas de grupo**

Revise las siguientes características de las cuentas de grupo en Microsoft Entra ID. En la captura de pantalla siguiente se muestra una lista de grupos en Azure Portal:



* Use grupos de seguridad para establecer permisos para todos los miembros del grupo al mismo tiempo, en lugar de agregar permisos para cada miembro individualmente.
* Agregue grupos de Microsoft 365 para habilitar el acceso de grupo para usuarios invitados fuera de la organización de Microsoft Entra.
* Un administrador de Microsoft Entra solo puede implementar grupos de seguridad.
* Los usuarios normales y los administradores de Microsoft Entra pueden usar grupos de Microsoft 365.

**Aspectos que se deben tener en cuenta al agregar miembros a grupos**

Al agregar miembros a un grupo, hay diferentes maneras de asignar derechos de acceso a miembros. A medida que lea estas opciones, tenga en cuenta qué grupos son necesarios para el funcionamiento de su organización y qué derechos de acceso se deben aplicar a los miembros del grupo.

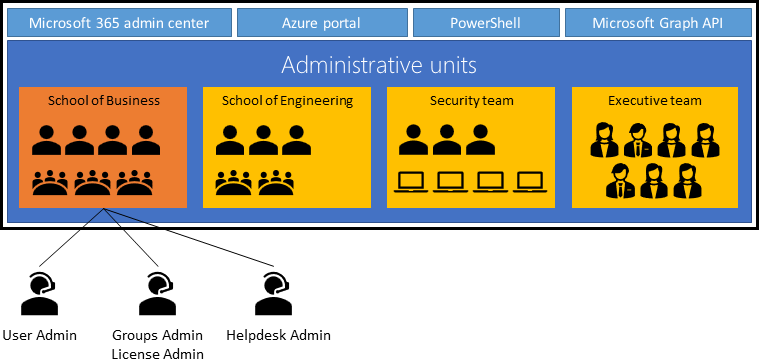
| **Derechos de acceso** | **Descripción** |
| --- | --- |
| **Asignado** | Agregue usuarios específicos como miembros de un grupo, donde cada usuario puede tener permisos únicos. |
| **Usuario dinámico** | Use reglas de pertenencia dinámicas para agregar y quitar miembros de un grupo automáticamente. Cuando los atributos de un miembro cambian, Azure revisa las reglas de grupos dinámicos del directorio. Si los atributos del miembro cumplen los requisitos de la regla, el miembro se agrega al grupo. Si los atributos del miembro ya no cumplen los requisitos de la regla, el miembro se elimina. |
| **Dispositivo dinámico** | (*Solo para grupos de seguridad*) Aplique reglas de grupos dinámicos para agregar y quitar automáticamente dispositivos en grupos de seguridad. Si los atributos de un dispositivo cambian, Azure revisa las reglas de grupos dinámicos del directorio. Si los atributos de un dispositivo cumplen los requisitos de la regla, el dispositivo se agrega al grupo de seguridad. Si los atributos del dispositivo ya no cumplen los requisitos de la regla, el dispositivo se elimina. |

**Crear unidades administrativas**

A medida que diseña la estrategia para la administración de identidades y la gobernanza en Azure, es fundamental planificar la administración completa de la infraestructura de Microsoft Entra. Puede ser útil restringir el ámbito administrativo mediante unidades administrativas para su organización. La división de roles y responsabilidades es especialmente útil para las organizaciones que tienen muchas divisiones independientes.

Pensemos en las tareas de administración de una universidad grande compuesta por varias escuelas diferentes, por ejemplo, de Negocios, Ingeniería y Medicina. La universidad cuenta con oficinas administrativas, edificios académicos, edificios sociales y dormitorios estudiantiles. Con fines de seguridad, cada oficina de negocios tiene su propia red interna para recursos como servidores, impresoras y máquinas de fax. Todos los edificios académicos están conectados a la red universitaria, para que tanto instructores como alumnos puedan acceder a sus cuentas. La red también está disponible para estudiantes y decanos en las habitaciones compartidas y los edificios sociales. En toda la universidad, los usuarios invitados necesitan acceso a Internet a través de la red universitaria.

La universidad tiene un equipo de administradores de TI que trabajan juntos para controlar el acceso a los recursos, administrar usuarios y establecer directivas para la escuela. Algunos administradores tienen privilegios mayores que otros en función del ámbito de sus responsabilidades. Se necesita una autoridad central para planificar, administrar y supervisar la estructura completa. En este escenario, puede asignar unidades administrativas para facilitar la administración de la organización.



**Aspectos que hay que tener en cuenta en las unidades administrativas**

Veamos cómo un rol de administrador central puede usar unidades administrativas para dar soporte al departamento de Ingeniería en nuestro escenario:

* Cree un rol que tenga permisos administrativos solo para los usuarios de Microsoft Entra en la unidad administrativa del departamento de Ingeniería.
* Cree una unidad administrativa para el departamento de Ingeniería.
* Rellene la unidad administrativa solo con los alumnos, el personal y los recursos del departamento de Ingeniería.
* Agregue el equipo de TI del departamento de Ingeniería al rol, junto con su ámbito.

**Aspectos que se deben tener en cuenta al trabajar con unidades administrativas**

Piense en cómo puede implementar unidades administrativas en su organización. A continuación, se indican algunas consideraciones:

* **Considere la posibilidad de usar herramientas de administración**. Revise las opciones para administrar las unidades administrativas. Puede usar Azure Portal, cmdlets y scripts de PowerShell o Microsoft Graph.
* **Considere los requisitos de rol de Azure Portal**. Planifique su estrategia para unidades administrativas según los privilegios de rol. En Azure Portal, solo los usuarios con el rol Administrador global o Administrador de roles con privilegios pueden administrar las unidades administrativas.
* **Considere el ámbito de las unidades administrativas**. Tenga en cuenta que el ámbito de una unidad administrativa solo se aplica a los permisos de *administración*. Los miembros y administradores de una unidad administrativa pueden ejercer sus permisos de *usuario* predeterminados para examinar otros usuarios, grupos o recursos fuera de su unidad administrativa.

**Prueba de conocimientos**

Su empresa ha decidido implementar las características de cuenta de usuario y grupo de Microsoft Entra ID en su estrategia de identidad y gobernanza. Debe explicar los tipos de cuentas, roles y asignaciones al equipo de planificación y guiarlos en su estrategia.

**Responda a las siguientes preguntas**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Qué tipo de cuenta de usuario permite a una organización externa acceder a los recursos?**

1. Una cuenta de usuario colaborador para cada miembro del equipo.
2. Una cuenta de administrador para cada miembro del equipo.
3. Una cuenta de usuario invitado para cada miembro del equipo externo.

**2. ¿Qué tipo de cuenta de grupo puede crear para que pueda aplicar los mismos permisos a todos los miembros del grupo?**

Grupo de seguridad

Grupo masivo de Microsoft Entra

Grupo de Microsoft 365

**3. ¿Qué rol de Microsoft Entra permite a un usuario administrar todos los grupos en los inquilinos de Teams y asignar también otros roles de administrador?**

1. Administrador global
2. Administrador de seguridad
3. Administrador de usuarios
4. C
5. A
6. A

Final del formulario

**Resumen y recursos**

Los administradores de Azure deben estar familiarizados con la configuración de cuentas de usuario y grupo en Microsoft Entra ID.

En este módulo, ha aprendido que todos los usuarios que desean acceder a los recursos de Azure necesitan una cuenta de usuario de Azure. Microsoft Entra ID admite el acceso a los recursos de la organización mediante la asignación de derechos de acceso a usuarios y grupos. Ha descubierto cómo se crean las cuentas de usuario y grupo en Microsoft Entra ID. Ha explorado cómo configurar y administrar cuentas de usuario y grupo, incluida la configuración masiva. Ha revisado cómo puede admitir su organización la organización de cuentas de grupo y administrar cuentas en varios directorios.

Las principales conclusiones de este módulo son las siguientes:

* Microsoft Entra ID admite tres tipos de cuentas de usuario: identidades en la nube, identidades sincronizadas por directorios e identidades de usuario invitado.
* Las identidades en la nube tienen información de perfil, como el puesto de trabajo y la ubicación de la oficina. Esta información puede adaptarse a las necesidades de su organización.
* Puede crear de forma masiva cuentas de usuario y grupo. El proceso usa un archivo de plantilla administrado a través del portal.
* Hay dos tipos de cuentas de grupo: Seguridad y Microsoft 365.
* Las unidades administrativas le ayudan a controlar el acceso de administrador a los recursos.