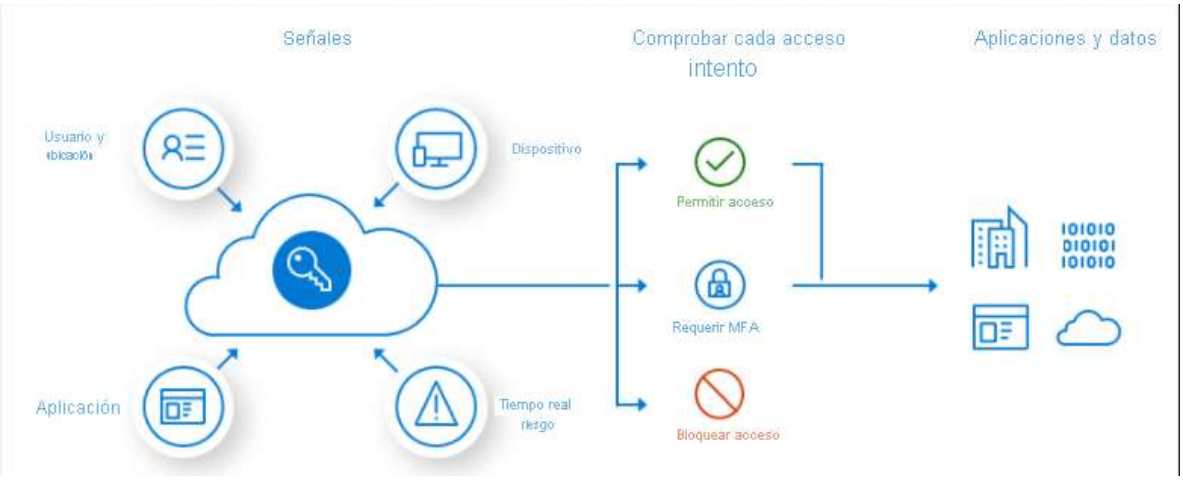
Descripción del acceso condicional en Azure AD

El acceso condicional es una característica de Azure AD que proporciona una capa de seguridad adicional antes de permitir que los usuarios autenticados tengan acceso a los datos o a otros recursos. El acceso condicional se implementa a través de las directivas que se crean y administran en Azure AD. Una directiva de acceso condicional analiza las señales que incluyen el usuario, la ubicación, el dispositivo, la aplicación y el riesgo para automatizar las decisiones de autorización de acceso a los recursos (aplicaciones y datos).



Es posible que una directiva de acceso condicional indique que *si* un usuario pertenece a un grupo determinado, se le pida que proporcione autenticación multifactor para iniciar sesión en una aplicación.

Vea el vídeo para descubrir cómo funcionan las directivas de acceso condicional.

Señales de acceso condicional

Entre algunas de las señales comunes que puede tener en cuenta el acceso condicional al tomar una decisión sobre una directiva se pueden incluir las siguientes:

- **Pertenencia a grupo o usuario**. Las directivas se pueden dirigir a todos los usuarios, grupos específicos de usuarios, roles de directorio o usuarios invitados externos, lo que proporciona a los administradores un control específico sobre el acceso.
- **Información de la ubicación con nombre**. La información de ubicación con nombre se puede crear con intervalos IP y usarse al tomar decisiones relacionadas con las directivas. Además, los administradores pueden optar por bloquear o permitir el tráfico desde el intervalo IP de todo un país o una región.
- **Dispositivo**. Se pueden usar los usuarios con dispositivos de plataformas específicas o marcados con un estado específico.
- **Aplicación**. Los usuarios que intentan acceder a aplicaciones específicas pueden desencadenar distintas directivas de acceso condicional.

- **Detección de riesgo de inicio de sesión en tiempo real**. La integración de señales con Azure AD Identity Protection permite que las directivas de acceso condicional identifiquen el comportamiento de riesgo de inicio de sesión, la probabilidad de que un inicio de sesión determinado o una solicitud de autenticación, no estén autorizados por el propietario de la identidad. Luego, las directivas pueden obligar a los usuarios a realizar cambios de contraseña o a usar la autenticación multifactor para reducir su nivel de riesgo, o a bloquear su acceso hasta que algún administrador lleve a cabo una acción manual.
- **Acciones o aplicaciones en la nube**. Las aplicaciones o acciones en la nube pueden incluir o excluir las aplicaciones en la nube o acciones del usuario que estarán sujetas a la directiva.
- **Riesgo de usuario**. En el caso de los clientes con acceso a Identity Protection, el riesgo del usuario se puede evaluar como parte de una directiva de acceso condicional. Un riesgo de usuario representa la probabilidad de que una identidad o cuenta determinada esté en peligro. El riesgo de los usuarios se puede configurar para una probabilidad alta, media o baja.

Al crear una directiva de acceso condicional, los administradores pueden determinar qué señales usar a través de asignaciones. La parte de asignaciones de la directiva controla el quién, el qué y el dónde de una directiva de acceso condicional. A todas las asignaciones se les asigna la operación lógica AND. Si tiene más de una asignación configurada, se deben satisfacer todas las asignaciones para desencadenar una directiva.

Controles de acceso

Cuando se ha aplicado la directiva de acceso condicional, se toma una decisión informada sobre si se debe conceder acceso, bloquear el acceso o requerir una comprobación adicional. La decisión se conoce como la parte de controles de acceso de la directiva de acceso condicional y define cómo se aplica una directiva. Las decisiones comunes son las siguientes:

- Bloquear acceso
- Conceder acceso
- Requerir que se cumplan una o más condiciones antes de conceder acceso:
    - Exigir la autenticación multifactor.
    - Requerir que el dispositivo esté marcado como compatible.
    - Requerir un dispositivo unido a Azure AD híbrido.
    - Requerir aplicación cliente aprobada.
    - Requerir la directiva de protección de aplicaciones.
    - Requerir cambio de contraseña.
- Controlar el acceso del usuario en función de controles de sesión para habilitar experiencias limitadas en aplicaciones en la nube determinadas. Por ejemplo, Control de

aplicaciones de acceso condicional usa las señales de aplicaciones de Microsoft Defender for Cloud para bloquear las funciones de descargar, cortar, copiar e imprimir documentos confidenciales, o bien para exigir el etiquetado de archivos confidenciales. Otros controles de sesión incluyen la frecuencia de inicio de sesión y las restricciones aplicadas a la aplicación que, en el caso de las aplicaciones seleccionadas, usan la información del dispositivo para proporcionar a los usuarios una experiencia limitada o completa, según el estado del dispositivo.

Las directivas de acceso condicional se pueden destinar a miembros de grupos o invitados específicos. Por ejemplo, puede crear una directiva para impedir que todas las cuentas de invitado tengan acceso a recursos confidenciales. El acceso condicional es una característica de las ediciones de Azure AD de pago.

Guía interactiva

En esta guía interactiva, creará una directiva de acceso condicional para un grupo de usuarios.

Descripción de las ventajas de los roles de Azure AD y el control de acceso basado en roles

Los roles de Azure AD controlan los permisos para administrar los recursos de Azure AD. Por ejemplo, permitir la creación de cuentas de usuario o ver la información de facturación. Azure AD admite roles integrados y personalizados.

La administración del acceso mediante roles se conoce como **control de acceso basado en roles (RBAC)**. Los roles integrados y personalizados de Azure AD son una forma de RBAC en que los roles de Azure AD controlan el acceso a los recursos de Azure AD. Esto se denomina RBAC de Azure AD.

Roles integrados

En Azure AD hay muchos roles integrados, que son los que tienen un conjunto fijo de permisos de rol. Algunos de los roles integrados más comunes son los siguientes:

- *Administrador global*: los usuarios con este rol tienen acceso a todas las características administrativas de Azure Active Directory. El usuario que se suscribe al inquilino de Azure Active Directory se convierte en administrador global de manera automática.
- *Administrador de usuarios*: los usuarios con este rol pueden crear y administrar todos los aspectos de los usuarios y grupos. Además, este rol incluye la capacidad de administrar incidencias de soporte técnico y supervisar el estado del servicio.
- *Administrador de facturación*: los usuarios que tienen este rol realizan compras, administra suscripciones e incidencias de soporte técnico y supervisan el estado del servicio.

Todos los roles integrados son agrupaciones preconfiguradas de permisos que se diseñaron para tareas específicas. El conjunto fijo de permisos incluidos en los roles integrados no se puede modificar.

Roles personalizados

Si bien hay muchos roles de administrador integrados en Azure AD, los roles personalizados proporcionan flexibilidad a la hora de conceder acceso. Una definición de roles personalizada es una colección de permisos que se seleccionan en una lista preestablecida. La lista de permisos entre los que se puede elegir son los mismos que usan los roles integrados. La diferencia es que puede elegir qué permisos quiere incluir en un rol personalizado.

La concesión de permisos mediante roles de Azure AD personalizados es un proceso de dos pasos. El primero implica la creación de una definición de rol personalizado, que consta de una colección de permisos que se agregan desde una lista preestablecida. Una vez que se crea la definición de rol personalizado, el segundo paso consiste en asignar ese rol a usuarios o grupos mediante la creación de una asignación de roles.

Una asignación de roles concede al usuario los permisos de una definición de roles según un ámbito específico. Un ámbito define el conjunto de recursos de Azure AD a los que tiene acceso el miembro del rol. Un rol personalizado se puede asignar en el ámbito de toda la organización, lo que significa que el miembro del rol tiene los permisos de rol sobre todos los recursos. También se puede asignar un rol personalizado en un ámbito de objeto. Un ejemplo del ámbito de objeto sería una aplicación única. Se puede asignar el mismo rol a un usuario en todas las aplicaciones de la organización y, luego, a otro usuario que solo tenga un ámbito de la aplicación de informes de gastos de Contoso.

Los roles personalizados requieren una licencia Azure AD Premium P1 o P2.

Solo se debe conceder el acceso que los usuarios necesitan

Es un procedimiento recomendado, y más seguro, para conceder a los usuarios el privilegio mínimo que necesitan para realizar su trabajo. Esto significa que si alguien administra principalmente usuarios, debe asignarle el rol de administrador de usuarios y no el de

administrador global. Mediante la asignación de privilegios mínimos, se limitan los daños que podrían ocurrir con una cuenta en peligro.

Categorías de roles de Azure AD

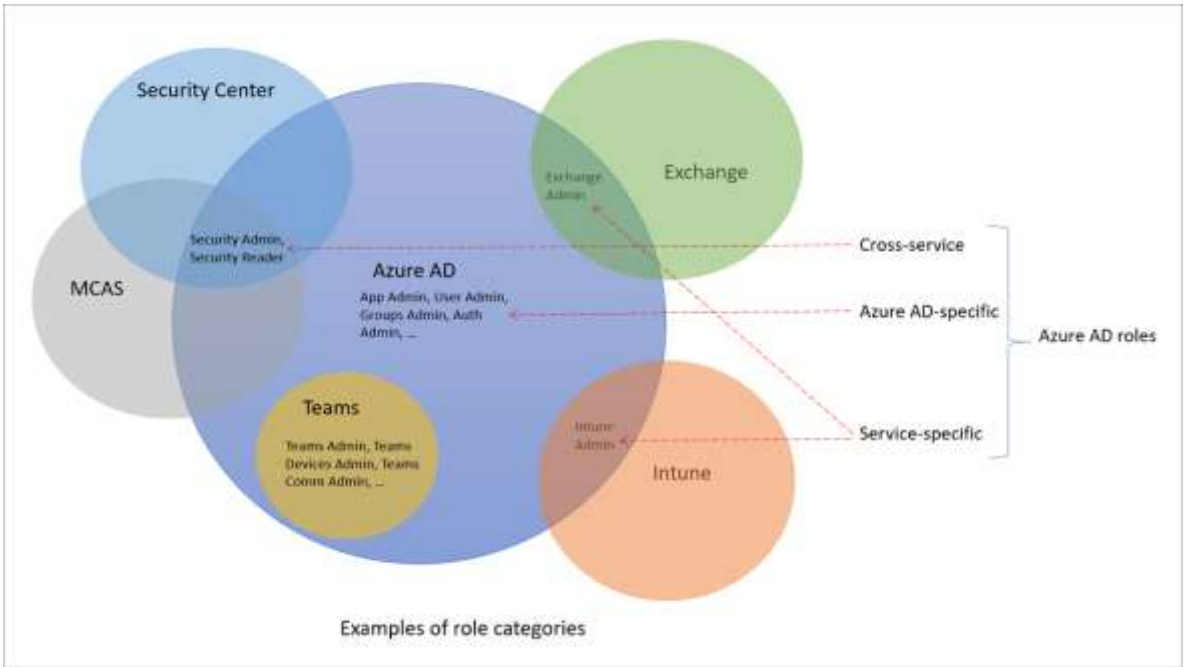
Como se ha definido antes, Azure Active Directory (Azure AD) es el servicio de administración de acceso y de identidades basado en la nube de Microsoft. Azure AD es un servicio disponible, si se suscribe a cualquier oferta empresarial de Microsoft Online, como Microsoft 365 y Azure.

Los servicios de Microsoft 365 disponibles incluyen Azure AD, Exchange, SharePoint, Microsoft Defender, Teams, Intune y muchos más.

Con el tiempo, algunos servicios de Microsoft 365, como Exchange y Intune, han desarrollado sus propios sistemas de control de acceso basado en roles, al igual que el servicio Azure AD tiene roles de Azure AD para controlar el acceso a los recursos de Azure AD (RBAC de Azure AD). Otros servicios como Teams y SharePoint no tienen sistemas de control de acceso basados en roles independientes; usan roles de Azure AD para su acceso administrativo.

Para que sea práctico administrar las identidades en los servicios de Microsoft 365, Azure AD ha agregado roles integrados de servicios específicos, y cada uno concede acceso administrativo a un servicio de Microsoft 365. Esto significa que los roles integrados de Azure AD difieren en dónde se pueden usar. Hay tres categorías principales.

- Roles específicos de Azure AD: estos roles conceden permisos para administrar recursos solo en Azure AD. Por ejemplo, Administrador de usuarios, Administrador de aplicaciones, Administrador de grupos, todos conceden permisos para administrar recursos que residen en Azure AD.
- Roles específicos del servicio: para los servicios de Microsoft 365 principales, Azure AD incluye roles específicos del servicio integrados que conceden permisos para administrar las características de ese servicio. Por ejemplo, Azure AD incluye roles integrados para Administrador de Exchange, Administrador de Intune, Administrador de SharePoint y Administrador de Teams que pueden administrar características de sus servicios respectivos.
- Roles multiservicio: hay algunos roles de Azure AD que abarcan varios servicios. Por ejemplo, Azure AD tiene roles relacionados con la seguridad, como Administrador de seguridad, que conceden acceso a varios servicios de seguridad dentro de Microsoft 365. Del mismo modo, en el rol Administrador de cumplimiento puede administrar la configuración relacionada con el cumplimiento en el Centro de cumplimiento de Microsoft 365, Exchange, etc.

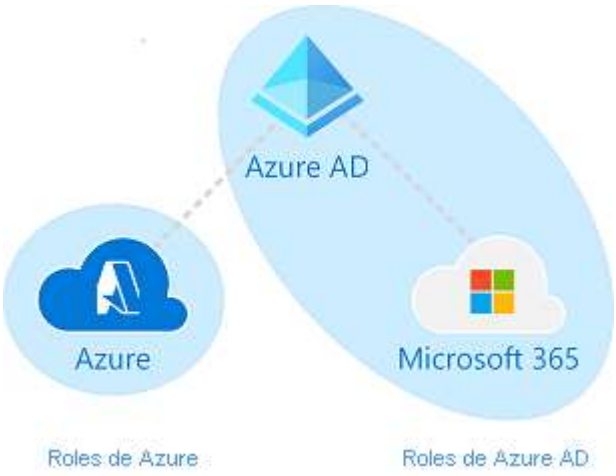


Diferencias entre los roles de RBAC de Azure y Azure AD

Como se ha descrito antes, los roles integrados y personalizados de Azure AD son una forma de RBAC por la que los roles de Azure AD controlan el acceso a los recursos de Azure AD. Esto se denomina RBAC de Azure AD. De la misma manera que los roles de Azure AD pueden controlar el acceso a los recursos de Azure AD, los roles de Azure también pueden controlar el acceso a los recursos de Azure. Esto se denomina RBAC de Azure. Aunque el concepto de RBAC se aplica tanto a RBAC de Azure AD como a RBAC de Azure, controlan aspectos diferentes.

- RBAC de Azure AD: los roles de Azure AD controlan el acceso a recursos de Azure AD como usuarios, grupos y aplicaciones.
- RBAC de Azure: los roles de Azure controlan el acceso a recursos de Azure como máquinas virtuales o almacenamiento mediante la administración de recursos de Azure.

Hay diferentes almacenes de datos donde se almacenan las definiciones de roles y las asignaciones de roles. Del mismo modo, hay diferente puntos de decisión de directivas donde se producen comprobaciones de acceso.



Los roles de Azure AD controlan los permisos para administrar los recursos de Azure AD. Por ejemplo, permitir la creación de cuentas de usuario o ver la información de facturación. Azure AD admite roles integrados y personalizados.

La administración del acceso mediante roles se conoce como **control de acceso basado en roles (RBAC)**. Los roles integrados y personalizados de Azure AD son una forma de RBAC en que los roles de Azure AD controlan el acceso a los recursos de Azure AD. Esto se denomina RBAC de Azure AD.

Roles integrados

En Azure AD hay muchos roles integrados, que son los que tienen un conjunto fijo de permisos de rol. Algunos de los roles integrados más comunes son los siguientes:

- *Administrador global*: los usuarios con este rol tienen acceso a todas las características administrativas de Azure Active Directory. El usuario que se suscribe al inquilino de Azure Active Directory se convierte en administrador global de manera automática.
- *Administrador de usuarios*: los usuarios con este rol pueden crear y administrar todos los aspectos de los usuarios y grupos. Además, este rol incluye la capacidad de administrar incidencias de soporte técnico y supervisar el estado del servicio.
- *Administrador de facturación*: los usuarios que tienen este rol realizan compras, administra suscripciones e incidencias de soporte técnico y supervisan el estado del servicio.

Todos los roles integrados son agrupaciones preconfiguradas de permisos que se diseñaron para tareas específicas. El conjunto fijo de permisos incluidos en los roles integrados no se puede modificar.

Roles personalizados

Si bien hay muchos roles de administrador integrados en Azure AD, los roles personalizados proporcionan flexibilidad a la hora de conceder acceso. Una definición de roles personalizada es una colección de permisos que se seleccionan en una lista preestablecida. La lista de permisos entre los que se puede elegir son los mismos que usan los roles integrados. La diferencia es que puede elegir qué permisos quiere incluir en un rol personalizado.

La concesión de permisos mediante roles de Azure AD personalizados es un proceso de dos pasos. El primero implica la creación de una definición de rol personalizado, que consta de una colección de permisos que se agregan desde una lista preestablecida. Una vez que se crea la definición de rol personalizado, el segundo paso consiste en asignar ese rol a usuarios o grupos mediante la creación de una asignación de roles.

Una asignación de roles concede al usuario los permisos de una definición de roles según un ámbito específico. Un ámbito define el conjunto de recursos de Azure AD a los que tiene acceso el miembro del rol. Un rol personalizado se puede asignar en el ámbito de toda la organización, lo que significa que el miembro del rol tiene los permisos de rol sobre todos los recursos. También se puede asignar un rol personalizado en un ámbito de objeto. Un ejemplo del ámbito de objeto sería una aplicación única. Se puede asignar el mismo rol a un usuario en todas las aplicaciones de la organización y, luego, a otro usuario que solo tenga un ámbito de la aplicación de informes de gastos de Contoso.

Los roles personalizados requieren una licencia Azure AD Premium P1 o P2.

Solo se debe conceder el acceso que los usuarios necesitan

Es un procedimiento recomendado, y más seguro, para conceder a los usuarios el privilegio mínimo que necesitan para realizar su trabajo. Esto significa que si alguien administra principalmente usuarios, debe asignarle el rol de administrador de usuarios y no el de administrador global. Mediante la asignación de privilegios mínimos, se limitan los daños que podrían ocurrir con una cuenta en peligro.

Categorías de roles de Azure AD

Como se ha definido antes, Azure Active Directory (Azure AD) es el servicio de administración de acceso y de identidades basado en la nube de Microsoft. Azure AD es un servicio disponible, si se suscribe a cualquier oferta empresarial de Microsoft Online, como Microsoft 365 y Azure.

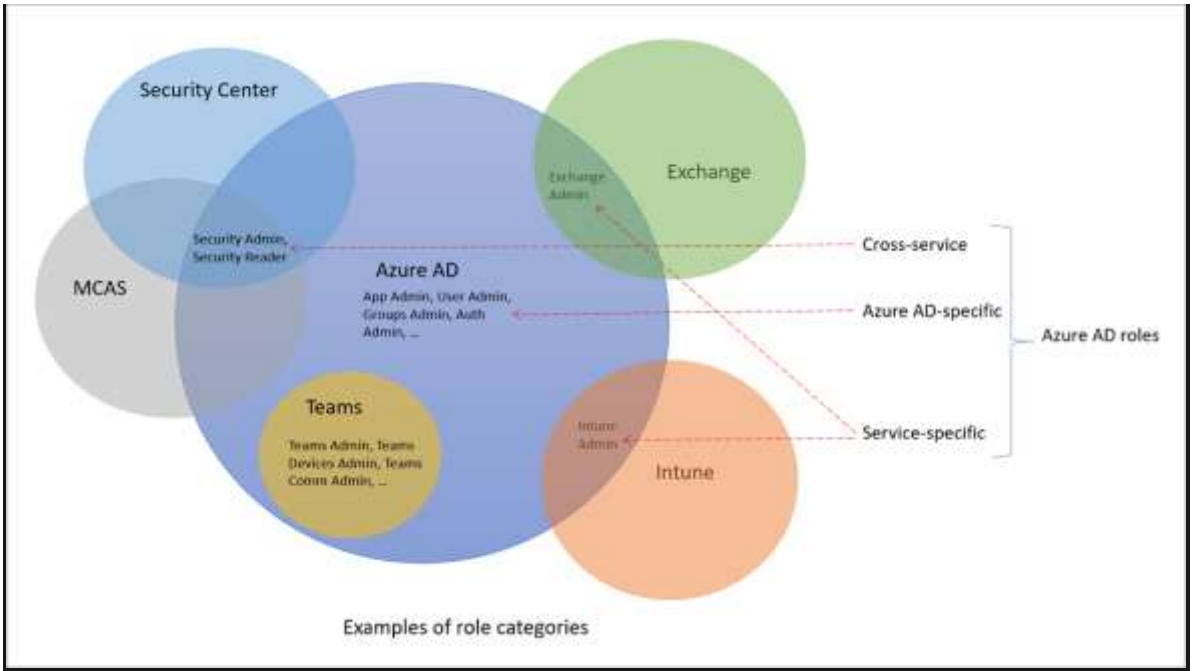
Los servicios de Microsoft 365 disponibles incluyen Azure AD, Exchange, SharePoint, Microsoft Defender, Teams, Intune y muchos más.

Con el tiempo, algunos servicios de Microsoft 365, como Exchange y Intune, han desarrollado sus propios sistemas de control de acceso basado en roles, al igual que el servicio Azure AD tiene roles de Azure AD para controlar el acceso a los recursos de Azure AD (RBAC de Azure AD). Otros servicios como Teams y SharePoint no tienen sistemas de control de acceso basados en roles independientes; usan roles de Azure AD para su acceso administrativo.

Para que sea práctico administrar las identidades en los servicios de Microsoft 365, Azure AD ha agregado roles integrados de servicios específicos, y cada uno concede acceso administrativo a un servicio de Microsoft 365. Esto significa que los roles integrados de Azure AD difieren en dónde se pueden usar. Hay tres categorías principales.

- Roles específicos de Azure AD: estos roles conceden permisos para administrar recursos solo en Azure AD. Por ejemplo, Administrador de usuarios, Administrador de aplicaciones, Administrador de grupos, todos conceden permisos para administrar recursos que residen en Azure AD.
- Roles específicos del servicio: para los servicios de Microsoft 365 principales, Azure AD incluye roles específicos del servicio integrados que conceden permisos para administrar las características de ese servicio. Por ejemplo, Azure AD incluye roles integrados para Administrador de Exchange, Administrador de Intune, Administrador de SharePoint y Administrador de Teams que pueden administrar características de sus servicios respectivos.
- Roles multiservicio: hay algunos roles de Azure AD que abarcan varios servicios. Por ejemplo, Azure AD tiene roles relacionados con la seguridad, como Administrador de seguridad, que conceden acceso a varios servicios de seguridad dentro de Microsoft 365. Del mismo modo, en el rol Administrador de cumplimiento puede administrar la

configuración relacionada con el cumplimiento en el Centro de cumplimiento de Microsoft 365, Exchange, etc.

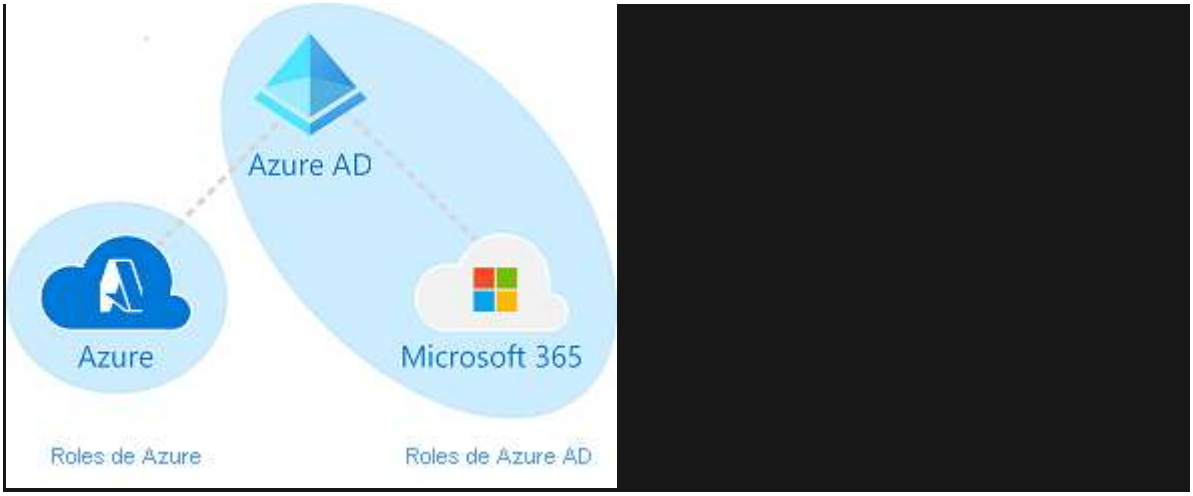


Diferencias entre los roles de RBAC de Azure y Azure AD

Como se ha descrito antes, los roles integrados y personalizados de Azure AD son una forma de RBAC por la que los roles de Azure AD controlan el acceso a los recursos de Azure AD. Esto se denomina RBAC de Azure AD. De la misma manera que los roles de Azure AD pueden controlar el acceso a los recursos de Azure AD, los roles de Azure también pueden controlar el acceso a los recursos de Azure. Esto se denomina RBAC de Azure. Aunque el concepto de RBAC se aplica tanto a RBAC de Azure AD como a RBAC de Azure, controlan aspectos diferentes.

- RBAC de Azure AD: los roles de Azure AD controlan el acceso a recursos de Azure AD como usuarios, grupos y aplicaciones.
- RBAC de Azure: los roles de Azure controlan el acceso a recursos de Azure como máquinas virtuales o almacenamiento mediante la administración de recursos de Azure.

Hay diferentes almacenes de datos donde se almacenan las definiciones de roles y las asignaciones de roles. Del mismo modo, hay diferente puntos de decisión de directivas donde se producen comprobaciones de acceso.


Azure AD
Azure
Microsoft 365
Roles de Azure
Roles de Azure AD