**Introducción**

Este módulo está diseñado para proporcionar a los administradores los conocimientos y habilidades necesarios para gestionar eficazmente la autorización utilizando Microsoft Entra ID, garantizando que los usuarios tengan el acceso adecuado a los recursos y datos.

**Escenario**

Imagine que es un especialista en administración de identidades y acceso responsable de controlar y supervisar el acceso a los recursos y datos de su organización. Su organización se basa en Microsoft Entra ID para la administración de identidades y acceso, y debe configurar directivas de autorización, roles y permisos para asegurarse de que los usuarios tienen el nivel de acceso adecuado al mismo tiempo que mantiene la seguridad.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Configure los permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos individuales para controlar el acceso en varios niveles.
* Asigne roles integrados en Microsoft Entra ID y Azure para conceder a los usuarios permisos predefinidos para tareas específicas.
* Cree y asigne roles personalizados, incluidos los roles de Azure y los roles de Microsoft Entra ID, para adaptar el control de acceso a los requisitos de la organización.
* Implemente y administre Administración de permisos de Microsoft Entra para refinar el control de acceso para los usuarios de Microsoft Entra ID.
* Configure Microsoft Entra Privileged Identity Management (PIM) para administrar y supervisar el acceso con privilegios.
* Configure la administración de roles y las revisiones de acceso en Microsoft Entra ID para garantizar el cumplimiento continuo y la seguridad.
* Implemente directivas de acceso condicional para aplicar condiciones de acceso basadas en el comportamiento del usuario y factores contextuales.

**Objetivos**

El módulo tiene como objetivo equipar a los participantes con los conocimientos y aptitudes necesarios para administrar la autorización de forma eficaz dentro de Microsoft Entra ID y Azure. Los participantes aprenderán a configurar roles y permisos, asignar privilegios, crear roles personalizados e implementar directivas de control de acceso, garantizando en última instancia que los usuarios tengan el nivel correcto de acceso al mismo tiempo que mantienen la seguridad y el cumplimiento.

**Configuración de permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos**

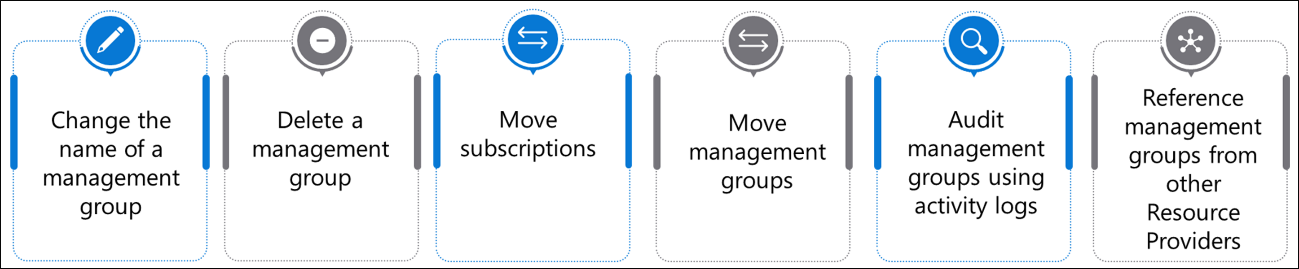
Es posible organizar las suscripciones en contenedores llamados **grupos de administración** y aplicarles las condiciones de gobernanza. Los grupos de administración proporcionan capacidad de administración de nivel empresarial a gran escala con independencia del tipo de suscripciones que tenga.

**Requisitos previos**

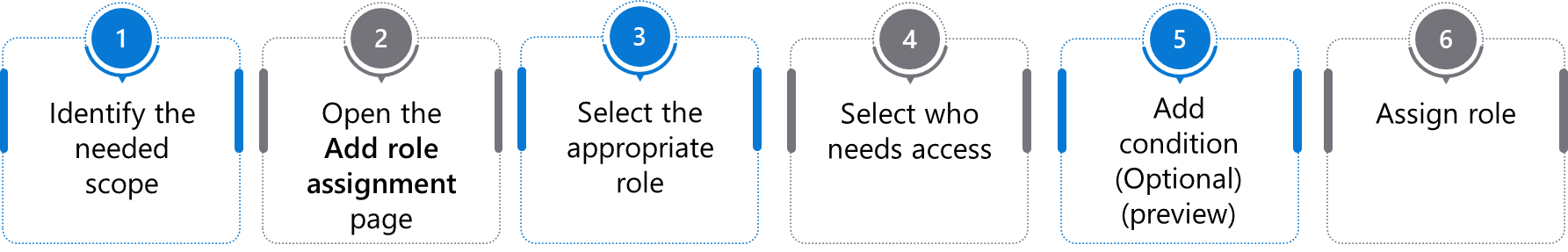
Para asignar roles de Azure, es necesario tener:

* Microsoft.Authorization/roleAssignments/write permissions, como la administrador de acceso de usuario o propietario.

**Para configurar los permisos de rol de Azure, tiene las siguientes opciones:**



**Para asignar roles de Azure, siga los siguientes pasos de alto nivel:**



**Asignación de roles integrados en Microsoft Entra ID**

La capacidad de administrar recursos se concede mediante la asignación de roles que proporcionan los permisos necesarios. Los roles se pueden asignar a usuarios o grupos individuales. Para alinearse con los principios rectores de Confianza cero, use directivas Just-In-Time y Just-Enough-Access al asignar roles.

**Asignación de roles**

Hay dos pasos principales para el proceso de asignación de roles. En primer lugar, debe seleccionar el rol que se va a asignar. A continuación, debe ajustar la configuración y la duración del rol.

1. Inicie sesión en el **centro de administración de Microsoft Entra** como **Administrador de roles con privilegios**.
2. Vaya a **Identidad**, **Usuarios**, **Todos los usuarios**.
3. Busque y seleccione el **usuario** que obtiene la asignación de roles.
4. Seleccione **Roles asignados** en el menú lateral y, a continuación, seleccione **Agregar asignaciones**.
5. Seleccione un rol para asignar de la lista desplegable y seleccione el botón **Siguiente**.

**Ajuste la configuración del rol**

Puede asignar roles como **aptos** o **activos**. Los roles aptos se asignan a un usuario, pero el usuario debe elevarlos a Just-In-Time a través de Privileged Identity Management (PIM).

1. En la sección Configuración de la página **Agregar asignaciones**, seleccione una opción de **Tipo de asignación**.
2. Deje seleccionada la opción **Elegible permanentemente** en caso de que el rol deba estar siempre disponible para que el usuario lo eleve. Si desactiva esta opción, puede especificar un intervalo de fechas para la elegibilidad del rol.
3. Seleccione el botón **Asignar**.

Los roles asignados aparecen en la sección asociada al usuario, por lo que los roles aptos y activos se muestran por separado.

**Actualizar roles**

Puede cambiar la configuración de una asignación de roles, por ejemplo, para cambiar un rol de activo a apto.

1. Vaya a **Identidad**, **Usuarios**, **Todos los usuarios**.
2. Busque y seleccione el usuario que obtiene la actualización de roles.
3. Vaya a la página **Roles asignados** y seleccione el vínculo **Actualizar** para el rol que debe cambiarse.
4. Cambie la configuración según sea necesario y seleccione el botón **Guardar**.

**Quitar roles**

Puede quitar asignaciones de roles de la página **Roles administrativos** de un usuario seleccionado.

1. Vaya a **Identidad**, **Usuarios**, **Todos los usuarios**.
2. Busque y seleccione el usuario que quita la asignación de roles.
3. Vaya a la página **Roles asignados** y seleccione el vínculo **Quitar** para el rol que debe quitarse. Confirme el cambio en el mensaje emergente.

**Asignar roles integrados en Azure**

El control de acceso basado en rol (RBAC) de Azure es el sistema de autorización que puede utilizar para administrar el acceso a los recursos de Azure. Para conceder acceso, debe asignar roles a usuarios, grupos, entidades de servicio o identidades administradas en un ámbito determinado.

**Requisitos previos**

**Para asignar roles de Azure, es necesario tener**:

* Microsoft.Authorization/roleAssignments/write permissions, como **Administrador de acceso de usuario** o **Propietario**.

**Paso 1: Identificación del ámbito necesario**

1. Inicie sesión en **Azure Portal**.
2. En el cuadro Buscar de la parte superior, busque el ámbito al que quiere conceder acceso. Por ejemplo, busque **Grupos de administración**, **Suscripciones**, **Grupos de recursos** o un recurso específico.
3. Haga clic en el recurso específico de ese ámbito.

**A continuación, se muestra un grupo de recursos de ejemplo**.

**Paso 2: Abra la página Asignación de roles añadidos**

Control de acceso (IAM) es la página que se usa normalmente para asignar roles y conceder acceso a los recursos de Azure. También se conoce como administración de identidad y acceso (IAM) y aparece en varias ubicaciones de Azure Portal.

1. Haga clic en **Control de acceso (IAM).**
2. Haga clic en la pestaña **Asignaciones de roles** para ver todas las asignaciones de roles en este ámbito.
3. Haga clic en **Agregar**, **Agregar** asignación de roles.

**Nota**

Si no tiene permisos para asignar roles, la opción Agregar asignación de roles se deshabilitará.

**Paso 3: seleccionar el rol apropiado**

1. En la pestaña **Rol**, seleccione un rol que quiera usar.

Puede buscar un rol por nombre o por descripción. También puede filtrar los roles por tipo y categoría.

1. Si desea asignar un rol de administrador con privilegios, seleccione la pestaña **Roles de administrador con privilegios** para seleccionar el rol.

Los roles de administrador con privilegios son roles que conceden acceso de administrador con privilegios, como la capacidad de administrar recursos de Azure o asignar roles a otros usuarios. Debería evitar asignar roles de administrador con privilegios cuando se puedan asignar roles de función de trabajo en su lugar. Si fuera necesario asignar roles de administrador con privilegios, use un ámbito estrecho, como el grupo de recursos o el recurso.

1. En la columna **Detalles** haga clic en **Ver** para obtener más información sobre un rol.
2. Haga clic en **Next**.

**Paso 4: elegir quién necesita acceso**

1. En la pestaña **Miembros**, seleccione **Usuario**, **Grupo** o **Entidad de servicio** asignar el rol seleccionado a uno o varios usuarios, grupos o entidades de servicio (aplicaciones) de Microsoft Entra ID.
2. Haga clic en **Seleccionar miembros**.
3. Busque y seleccione los usuarios, grupos o entidades de servicio.

**Nota**

Puede escribir en el cuadro **Seleccionar** para buscar en el directorio por nombre para mostrar o dirección de correo electrónico.

1. Haga clic en Seleccionar para agregar los usuarios, grupos o entidades de servicio a la lista Miembros.
2. Para asignar el rol seleccionado a una o varias identidades administradas, seleccione **Identidad administrada**.
3. Haga clic en **Seleccionar miembros**.
4. En el panel **Selección de identidades administradas**, seleccione si el tipo es una identidad administrada asignada por el usuario o una identidad administrada asignada por el sistema.
5. Busque y seleccione las identidades administradas.

Para las identidades administradas asignadas por el sistema, puede seleccionar identidades administradas por instancia de servicio de Azure.

1. Haga clic en **Seleccionar** para agregar las identidades administradas a la lista Miembros.
2. En el cuadro de texto **Descripción**, escriba una descripción opcional para esta asignación de roles.

Más adelante puede mostrar esta descripción en la lista de asignaciones de roles.

1. Haga clic en **Next**.

**Paso 5: (Opcional) agregar condición**

Si seleccionó un rol que admite condiciones, aparecerá una pestaña **Condiciones** y tendrá la opción de agregar una condición a la asignación de roles. Una condición es una comprobación adicional que puede agregar opcionalmente a la asignación de roles para proporcionar un control de acceso más preciso.

La pestaña **Condiciones** tendrá un aspecto diferente en función del rol seleccionado.

Si seleccionó uno de los siguientes roles con privilegios, siga los pasos descritos en esta sección.

* Propietario
* Administrador de Access Control basado en roles **(versión preliminar)**
* Administrador de acceso de usuario

1. En la pestaña **Condiciones**, en **Tipo de delegación**, seleccione la opción **Restringido (recomendado)**.
2. Haga clic en **Agregar condición** para agregar una condición que restrinja los roles y entidades de seguridad a los que este usuario puede asignar roles.

**Paso 6: Asignar un rol**

1. En la pestaña **Revisión y asignación**, revise la configuración de la asignación de roles.
2. Haga clic en **Revisión y asignación** para asignar el rol.

Transcurridos unos instantes, se asigna el rol a la entidad de seguridad en el ámbito seleccionado.

1. Si no ve la descripción de la asignación de roles, haga clic en **Editar columnas** para agregar la columna **Descripción**.

**Quitar roles**

Puede quitar asignaciones de roles de la página **Roles administrativos** de un usuario seleccionado.

1. Vaya a **Identidad**, **Usuarios**, **Todos los usuarios**.
2. Busque y seleccione el usuario que quita la asignación de roles.
3. Vaya a la página **Roles asignados** y seleccione el vínculo **Quitar** para el rol que debe quitarse. Confirme el cambio en el mensaje emergente.

**Creación y asignación de un rol personalizado en Microsoft Entra ID**

Es posible crear roles personalizados desde la pestaña Roles y administradores de la página de información general de Azure AD. El rol se puede asignar en el ámbito de nivel de directorio o en un ámbito de recurso del registro de aplicación únicamente.

Los roles personalizados se pueden crear en la página Roles y administradores del centro de administración de Microsoft Entra.

**Creación de un rol en el centro de administración de Microsoft Entra**

**Creación de un rol personalizado para conceder acceso para administrar los registros de aplicaciones**

1. Inicie sesión en el **Centro de administración de Microsoft Entra** al menos como **Administrador de roles con privilegios**.
2. Vaya a **Identidad**, **Roles y administradores** y **Roles y administradores**.
3. Seleccione **Nuevo rol personalizado**.
4. En la pestaña **Aspectos básicos**, proporcione un nombre y una descripción para el rol y, luego, haga clic en **Siguiente**.
5. En la pestaña Permisos, seleccione los permisos necesarios para administrar las propiedades básicas y las propiedades de credenciales de los registros de aplicaciones.
6. En primer lugar, escriba "credenciales" en la barra de búsqueda y seleccione el microsoft.directory/applications/credentials/update permission.
7. A continuación, escriba "**básico**" en la barra de búsqueda, seleccione el microsoft.directory/applications/basic/update permission y, luego, haga clic en **Siguiente**.
8. En la pestaña **Revisar** + **crear**, revise los permisos y seleccione Crear.
9. El rol personalizado se mostrará en la lista de los roles disponibles para asignar.

**Asignación de un rol personalizado con ámbito de un recurso**

Al igual que los roles integrados, los roles personalizados se asignan de forma predeterminada en el ámbito predeterminado de toda la organización para conceder permisos de acceso a todos los registros de aplicaciones de la organización. Además, los roles personalizados y algunos roles integrados pertinentes (según el tipo de recurso de Microsoft Entra) también se pueden asignar en el ámbito de un único recurso de Microsoft Entra. Esto le permite entregar al usuario el permiso para actualizar las credenciales y las propiedades básicas de una aplicación única sin la necesidad de crear un segundo rol personalizado.

1. Inicie sesión en el **centro de administración de Microsoft Entra** al menos como **Desarrollador de aplicaciones**.
2. Vaya a **Identidad**, **Aplicaciones**, **Registros de aplicaciones**.
3. Seleccione el registro de aplicaciones al que se concede acceso para administrar. Es posible que tenga que seleccionar **Todas las aplicaciones** para ver la lista completa de los registros de aplicaciones de la organización de Microsoft Entra.
4. En el registro de aplicaciones, seleccione **Roles y administradores**. Si todavía no crea uno, puede encontrar instrucciones sobre cómo hacerlo en el procedimiento anterior.
5. Seleccione el rol para abrir la página **Asignaciones**.
6. Seleccione **Agregar asignación** para agregar un usuario. Al usuario se le concederán permisos únicamente sobre el registro de aplicaciones seleccionado.

**Implementación y administración de la Administración de permisos de Microsoft Entra**

Una vez que haya habilitado la Administración de permisos, puede conectarla a las plataformas Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP).

**Requisitos previos**

Para habilitar la Administración de permisos en una organización:

* Debe tener un inquilino de Microsoft Entra. Si todavía no la tiene, cree una cuenta gratuita.
* Debe poder optar por una asignación activa al rol Administrador de la administración de permisos como usuario en ese inquilino o bien tener ya asignado el rol.

**Habilitación de la administración de permisos en el inquilino de Microsoft Entra**

En el explorador, haga lo siguiente:

1. Vaya al centro de administración de Microsoft Entra e inicie sesión en Microsoft Entra ID. como Administrador global.
2. Si es necesario, active el rol Administrador de permisos en el inquilino de Microsoft Entra.
3. En Azure Portal, seleccione Administración de permisos de Microsoft Entra y, a continuación, seleccione el enlace para adquirir una licencia o iniciar una prueba.

**Activación de una prueba gratuita o una licencia de pago**

Hay dos formas de activar una prueba o una licencia de producto completa.

* La primera manera es ir al Centro de administración de Microsoft 365.  
  1. Inicie sesión como **administrador global** de su arrendatario.
  2. Vaya a Configuración y regístrese para obtener una versión de prueba de Administración de permisos de Entra.
  3. Para el autoservicio, vaya al Portal de Microsoft 365 para registrarse para obtener una prueba gratuita de 45 días o para comprar licencias.
* La segunda modalidad es mediante las licencias por volumen o los contratos Enterprise.
  1. Si su organización se ajusta a la modalidad de las licencias por volumen o contrato Enterprise, póngase en contacto con su representante de Microsoft.

La Administración de permisos se inicia con el panel **Recopiladores de datos**.

**Configuración de la recopilación de datos**

Use el panel Recopiladores de datos en la Administración de permisos para configurar los valores de la recopilación de datos para el sistema de autorización.

1. Si no se muestra el panel Recopiladores de datos al iniciarse Administración de permisos:

* En la página principal de Administración de permisos, seleccione Configuración (el icono de engranaje) y después la subpestaña Recopiladores de datos.

1. Seleccione el sistema de autorización que quiera: AWS (AWS), Azure (Azure) o GCP (GCP).
2. Para información sobre cómo incorporar una cuenta de AWS, una suscripción a Azure o un proyecto de GCP en la Administración de permisos, seleccione uno de los artículos siguientes y siga las instrucciones:

* Incorporación de una cuenta de AWS
* Incorporación de una suscripción de Azure
* Incorporación de un proyecto de GCP

**Configuración de Microsoft Entra Privileged Identity Management**

Privileged Identity Management proporciona activación de rol basada en tiempo y en aprobación para mitigar los riesgos de tener unos permisos de acceso excesivos, innecesarios o mal utilizados en los recursos que le interesan. Estas son algunas de las características clave de Privileged Identity Management:

* Conceda privilegios de acceso Just-In-Time a Microsoft Entra ID y a los recursos de Azure
* Asignar acceso limitado a los recursos con fechas de inicio y fin.
* Requiera aprobación para activar los roles con privilegios
* Aplique la autenticación multifactor para activar cualquier rol
* Use la justificación para comprender por qué se activan los usuarios
* Obtener notificaciones cuando se activan los roles con privilegios.
* Llevar a cabo revisiones de acceso para asegurarse de que los usuarios siguen necesitando roles.
* Descargue el historial de auditoría para la auditoría interna o externa
* Impide la eliminación de las últimas asignaciones de roles de administrador global y administrador de roles con privilegios activas

Una vez que se haya configurado Privileged Identity Management, verá las opciones Tareas, Administrar, y Actividad en el menú de navegación izquierdo. Como administrador, puede elegir entre distintas opciones, como administrar roles de Microsoft Entra, administrar roles de recursos de Azure o PIM para grupos. Cuando elija lo que desea administrar, verá el conjunto de opciones adecuado para esa opción.

En el caso de los roles de Microsoft Entra en Privileged Identity Management, los usuarios que tengan el rol Administrador de roles con privilegios o el rol Administrador global son los únicos que pueden administrar las asignaciones de otros administradores. Los administradores globales, administradores de seguridad, lectores globales y lectores de seguridad pueden ver también las asignaciones de roles de Microsoft Entra en Privileged Identity Management.

En el caso de los roles de los recursos de Azure en Privileged Identity Management, los únicos que pueden administrar asignaciones para los demás administradores son los administradores de suscripciones, los propietarios de los recursos o los administradores de acceso de usuario de los recursos. De forma predeterminada, los usuarios que son administradores de roles con privilegios, administradores de seguridad o lectores de seguridad no tienen acceso para ver asignaciones a roles de recursos de Azure en Privileged Identity Management.

**Terminología**

Para conocer mejor Privileged Identity Management y su documentación, debe revisar los términos siguientes.

| **Término** | **Definición** |
| --- | --- |
| action | Una actividad que una entidad de seguridad puede realizar en un tipo de objeto. A veces se conoce como una operación. |
| permiso | Definición que especifica la actividad que una entidad de seguridad puede realizar en un tipo de objeto. Un permiso incluye una o varias acciones. |
| permiso con privilegios | En Microsoft Entra ID, permisos que se pueden usar para delegar la administración de recursos de directorio en otros usuarios, modificar credenciales y directivas de autenticación o autorización, o acceder a datos restringidos. |
| rol con privilegios | Un rol integrado o personalizado que tiene uno o varios permisos con privilegios. |
| asignación de roles con privilegios | Asignación de roles que usa un rol con privilegios. |
| elevación de privilegios | Cuando una entidad de seguridad obtiene más permisos de los que su rol asignado proporcionó inicialmente suplantando otro rol. |
| acción protegida | Permisos con acceso condicional aplicado para mayor seguridad. |

**Introducción a la asignación de roles**

Las asignaciones de roles de PIM proporcionan una manera segura de conceder acceso a los recursos de su organización. En esta sección se describe el proceso de asignación. Incluye asignar roles a miembros, activar asignaciones, aprobar o denegar solicitudes, ampliar y renovar asignaciones.

PIM le mantiene informado mediante el envío de notificaciones de correo electrónico, a usted y a otros participantes. Estos mensajes de correo electrónico también podrían incluir vínculos a tareas pertinentes, tales como la activación, aprobación o negación de una solicitud.

En la captura de pantalla siguiente se muestra un mensaje de correo electrónico enviado por PIM. El correo electrónico informa a Patti de que Alex actualizó una asignación de roles para Emily.

**Assign**

El proceso de asignación comienza asignando roles a los miembros. Para conceder acceso a un recurso, el administrador asigna roles a usuarios, grupos, entidades de servicio o identidades administradas. La asignación incluye los datos siguientes:

* Los miembros o propietarios para asignar el rol.
* El ámbito de la asignación. El ámbito limita el rol asignado a un conjunto determinado de recursos.
* Tipo de asignación
  + Las asignaciones tipo Apto requieren que el miembro del rol realice una acción para usar el rol. Las acciones pueden incluir la activación o la solicitud de aprobación de los aprobadores designados.
  + Las asignaciones tipo Activo no requieren que el miembro realice ninguna acción para usar el rol. Los miembros asignados como activos tienen privilegios asignados al rol.
* Duración de la asignación, con fechas de inicio y finalización o permanentes. En el caso de las asignaciones aptas, los miembros pueden activar o solicitar aprobación durante las fechas de inicio y finalización. En el caso de las asignaciones activas, los miembros pueden usar el rol de asignación durante este período de tiempo.

En la captura de pantalla siguiente se muestra cómo el administrador asigna un rol a los miembros.

**Activar**

Si los usuarios han sido aptos para un rol, deben activar la asignación de roles antes de usar el rol. Para activar el rol, los usuarios seleccionan duración de activación específica dentro del máximo (configurado por los administradores) y el motivo de la solicitud de activación.

En la captura de pantalla siguiente se muestra cómo los miembros activan su rol en un tiempo limitado.

Si el rol requiere aprobación para activarse, aparece una notificación en la esquina superior del explorador del usuario que informa de que la solicitud está pendiente de aprobación. Si no se requiere una aprobación, el miembro puede empezar a usar el rol.

**Aprobar o denegar**

Los aprobadores delegados reciben notificaciones por correo electrónico cuando una solicitud de rol está pendiente de su aprobación. Los aprobadores pueden ver, aprobar o denegar estas solicitudes pendientes en PIM. Una vez aprobada la solicitud, el miembro puede empezar a usar el rol. Por ejemplo, si a un usuario o grupo se le asignó el rol de Contribución a un grupo de recursos, pueden administrar ese grupo de recursos determinado.

**Extensión y renovación de asignaciones**

Después de que los administradores configuren las asignaciones de miembros o propietarios con límite de tiempo, la primera pregunta que podría surgir es qué sucede si una asignación expira. En esta nueva versión, se proporcionan dos opciones para este escenario:

* **Extensión**: cuando una asignación de roles está a punto de expirar, el usuario puede usar Privileged Identity Management para solicitar una extensión
* **Renovación**: cuando una asignación de roles ya ha expirado, el usuario puede usar Privileged Identity Management para solicitar una renovación

Ambas acciones iniciadas por el usuario requieren una aprobación de un Administrador global o un Administrador de roles con privilegios. Los administradores no necesitan estar en el negocio de administrar las expiraciones de las asignaciones. Puede simplemente esperar a que lleguen las solicitudes de extensión o renovación para la aprobación o denegación.

**Configuración de la administración de roles y las revisiones de acceso con Microsoft Entra Identity Governance**

La necesidad de acceso a recursos de Azure y roles de Microsoft Entra con privilegios por parte de los empleados cambia con el tiempo. Para reducir el riesgo asociado con las asignaciones de roles obsoletas, debe revisar el acceso periódicamente. Puede usar Microsoft Entra Privileged Identity Management (PIM) para crear revisiones de acceso para obtener acceso con privilegios a los roles de recursos de Microsoft Entra. También puede configurar revisiones de acceso periódicas que se produzcan automáticamente.

**Requisitos previos**

Se necesitan licencias para usar Privileged Identity Management.

Para crear revisiones de acceso en los recursos de Azure, es preciso tener asignado los roles de Azure Propietario o Administrador de acceso de usuario para los recursos de Azure. Para crear revisiones de acceso para los roles de Microsoft Entra, debe tener asignado los roles de Administrador global o Administrador de roles con privilegios.

Las revisiones de acceso para entidades de servicio requieren un plan Premium de id. de carga de trabajo de Microsoft Entra además de las licencias de Microsoft Entra ID P2 o gobierno de Microsoft Entra ID.

* Licencias premium de identidades de carga de trabajo: puede ver y adquirir licencias en la hoja Identidades de carga de trabajo de la Azure Portal.

**Crear revisiones de acceso**

1. Inicie sesión en el centro de administración de Microsoft Entra como usuario asignado a uno de los roles de requisitos previos.
2. Vaya a Gobernanza de identidades > Privileged Identity Management.
3. Para los roles de Microsoft Entra, seleccione roles de Microsoft Entra. En Recursos de Azure, seleccione Recursos de Azure.
4. Para los roles de Microsoft Entra, seleccione roles de Microsoft Entra de nuevo en Administrar. En Recursos de Azure, seleccione la suscripción que desea administrar.
5. En Administrar, seleccione Revisiones de acceso y, luego, elija Nuevapara crear una nueva revisión de acceso.
6. Ponga un nombre a la revisión de acceso. Opcionalmente, asigne a la revisión una descripción. El nombre y la descripción se muestran a los revisores.
7. Establezca un valor para **Fecha de inicio**. De forma predeterminada, una revisión de acceso ocurre una vez, se inicia a la misma hora en que se crea y finaliza en un mes. Puede cambiar las fechas de inicio y de finalización para hacer que una revisión de acceso se inicie en el futuro, transcurridos tantos días como desee.
8. Para realizar que la revisión de acceso sea periódica, cambie la opción Frecuencia de Una vez a Semanal, Mensual, Trimestral, Anual o Semestral. Use el control deslizante o el cuadro de texto Duración para definir cuántos días se abrirá cada revisión de la serie periódica para que los revisores escriban datos. Por ejemplo, la duración máxima que puede establecer para una revisión mensual es 27 días, con el fin de evitar la superposición de revisiones.
9. Use el valor Fin para especificar cómo finalizar la serie de revisión de acceso periódica. La serie puede terminar de tres formas: se ejecuta continuamente para iniciar revisiones indefinidamente, hasta una fecha concreta, o hasta que se haya completado un número definido de veces. Cualquier administrador que pueda administrar revisiones puede detener la serie después de su creación cambiando la fecha en Configuración, de manera que termine en esa fecha.
10. En la sección Ámbito de los usuarios, seleccione el ámbito de la revisión. En Roles de Microsoft Entra, la primera opción de ámbito es Usuarios y grupos. En esta selección se incluirán los usuarios asignados directamente y los grupos a los que se pueden asignar roles. En Roles de recursos de Azure, el primer ámbito será Usuarios. Los grupos asignados a los roles de recursos de Azure se expanden para mostrar asignaciones de usuario transitivas en la revisión con esta selección. También puede seleccionar Entidades de servicio para examinar las cuentas de máquina con acceso directo al recurso de Azure o al rol de Microsoft Entra.
11. También puede crear revisiones de acceso solo para usuarios inactivos (versión preliminar). En la sección Ámbito de los usuarios, establezca Solo usuarios inactivos (en el nivel de inquilino) en true. Si el botón de alternancia se establece en true, el ámbito de la revisión se centrará solo en los usuarios inactivos. A continuación, especifique un valor para Días sin actividad de como máximo 730 días (dos años). Los usuarios inactivos durante el número de días especificado serán los únicos usuarios de la revisión.
12. En Pertenencia a rol de revisión, seleccione el recurso de Azure o los roles de Microsoft Entra con privilegios que desea revisar.
13. En el **tipo de asignación**, defina el ámbito de la revisión según la asignación de la entidad de seguridad al rol. Elija Eligible assignments only (Solo asignaciones aptas) para revisar las asignaciones aptas (independientemente del estado de activación al crear la revisión) o Solo asignaciones activas para revisar las asignaciones activas. Elija All active and eligible assignments (Todas las asignaciones activas y aptas) para revisar todas las asignaciones, independientemente del tipo.
14. En la sección **Revisores**, seleccione una o más personas para que revisen a todos los usuarios. También puede seleccionar que los miembros revisen su propio acceso.

* **Usuarios seleccionados**: use esta opción para designar un usuario específico para completar la revisión. Esta opción está disponible independientemente del ámbito de la revisión y los revisores seleccionados pueden revisar usuarios, grupos y entidades de servicio.
* **Miembros (por sí mismos)** : use esta opción para hacer que los usuarios revisen sus propias asignaciones de roles. Esta opción solo está disponible si el ámbito de la revisión es Usuarios y grupos o Usuarios. En Roles de Microsoft Entra, los grupos a los que se pueden asignar roles no formarán parte de la revisión cuando se selecciona esta opción.
* **Administrador**: use esta opción para que el administrador del usuario revise su asignación de roles. Esta opción solo está disponible si el ámbito de la revisión es Usuarios y grupos o Usuarios. Tras seleccionar Administrador, también tendrá la opción de especificar un revisor de reserva. Se pide a los revisores de reserva que revisen a un usuario cuando este no tiene ningún administrador especificado en el directorio. En Roles de Microsoft Entra, el revisor de reserva examinará los grupos a los que se pueden asignar roles si hay alguno seleccionado.

**Configuración de finalización**

1. Para especificar lo que sucede una vez finalizada una revisión, expanda la sección **Configuración de finalización**.
2. Si desea quitar automáticamente el acceso para los usuarios que se han denegado, establezca Aplicar automáticamente los resultados al recurso en Habilitar. Si desea aplicar manualmente los resultados cuando se complete la revisión, establezca el conmutador en Deshabilitar.
3. Use la lista Si el revisor no responde para especificar lo que ocurre con los usuarios a los que el revisor no ha revisado dentro del período de revisión. Este valor no afecta a los usuarios que los revisores revisaron.

* Sin cambios: dejar el acceso del usuario sin cambios
* Quitar acceso: quitar el acceso del usuario
* Aprobar acceso: aprobar el acceso del usuario
* Aceptar recomendaciones: aceptar la recomendación del sistema sobre la denegación o aprobación del acceso continuo del usuario

1. Use la lista Action to apply on denied guest users (Acción que se aplica a los usuarios invitados denegados) para especificar lo que les sucede a los usuarios invitados denegados. Este valor no se puede editar para las revisiones de los recursos de Azure y los roles de Microsoft Entra ID en este momento; los usuarios invitados, al igual que todos los usuarios, siempre perderán el acceso al recurso si se deniegan.
2. Puede enviar notificaciones a usuarios o grupos adicionales para recibir actualizaciones de finalización de las revisiones. Esta característica permite que partes interesadas que no sean el creador de la revisión reciban actualizaciones sobre el progreso de la revisión. Para usar esta característica, seleccione Seleccionar usuarios o grupos y agregue un usuario o grupo adicional cuando quiera recibir el estado de finalización.

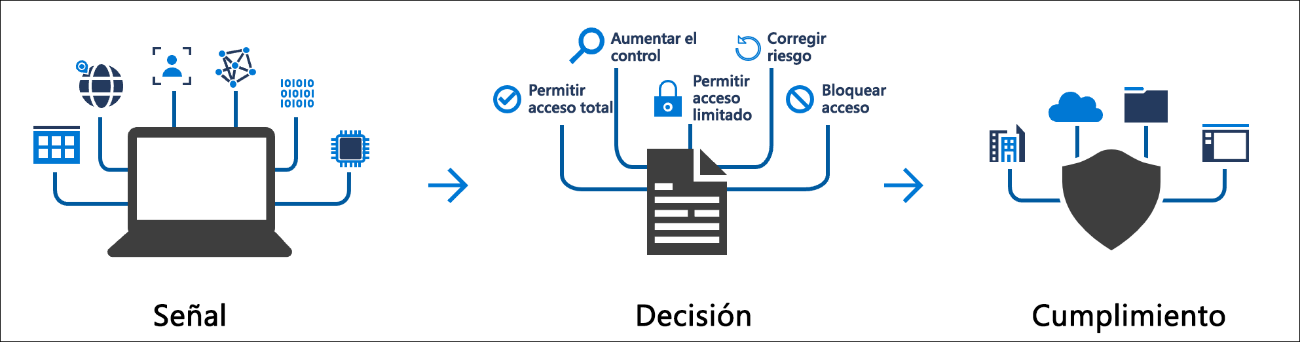
**Configuración avanzada**

1. Para especificar configuraciones adicionales, expanda la sección Configuración avanzada.
2. Establezca Mostrar recomendaciones en Habilitar para mostrar las recomendaciones del sistema de los revisores según la información del acceso del usuario. Las recomendaciones se basan en un período de intervalo de 30 días en el que se recomienda el acceso a los usuarios que han iniciado sesión en los últimos 30 días, mientras que a los usuarios que no lo han hecho se les recomienda la denegación de acceso. Estos inicios de sesión son independientes de si eran interactivos. El último inicio de sesión del usuario también se muestra junto con la recomendación.
3. Establezca Requerir motivo de la aprobación en Habilitar para requerir que el revisor proporcione un motivo para la aprobación.
4. Establezca Notificaciones de correo en Habilitar para que Microsoft Entra ID envíe notificaciones de correo electrónico a los revisores cuando se inicie una revisión de acceso y a los administradores cuando se complete.
5. Establezca Recordatorios en Habilitar para que Microsoft Entra ID envíe recordatorios de revisiones de acceso en curso a los revisores que no hayan completado su revisión.
6. El contenido del correo electrónico enviado a los revisores se genera automáticamente en función de los detalles de la revisión, como el nombre de la revisión, el nombre del recurso, la fecha de vencimiento, etc. Si necesita una forma de comunicar más información, como instrucciones adicionales o información de contacto, puede especificar estos detalles en el correo electrónico de contenido adicional para el revisor que se incluirá en la invitación y en los correos electrónicos de recordatorio enviados a los revisores asignados. La sección resaltada a continuación es donde se mostrará esta información.

**Implementar directivas de acceso condicional**

El perímetro de seguridad moderno se extiende más allá de la red de una organización, e incluye tanto la identidad del usuario como la del dispositivo. Las organizaciones ahora usan señales basadas en identidades como parte de sus decisiones de control de acceso.

El acceso condicional de Microsoft Entra reúne las señales para tomar decisiones y aplicar las directivas de la organización. El acceso condicional es el motor de directivas de Confianza cero de Microsoft que tiene en cuenta señales de varios orígenes al aplicar decisiones de directivas.



En su forma más simple, las directivas de acceso condicional son instrucciones if-then; si un usuario desea tener acceso a un recurso, deben completar una acción. **Ejemplo**: Un responsable de nóminas quiere acceder a la aplicación de nóminas y para ello es obligatorio realizar la autenticación multifactor.

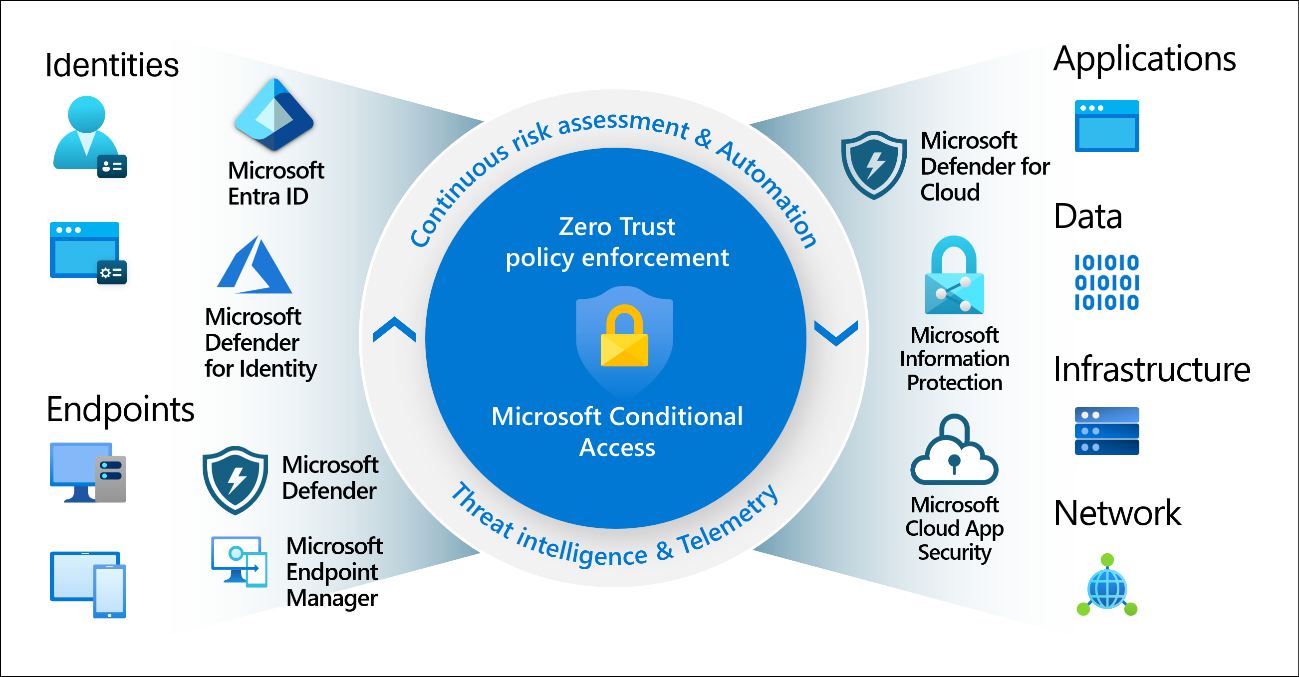
Los administradores se enfrentan a dos objetivos principales:

* Capacitar a los usuarios para ser productivos donde sea y cuando sea
* Proteger los recursos de la organización.

Utilizar las directivas de acceso condicional para aplicar los controles de acceso correctos cuando sea necesario para mantener protegida la organización.

**Señales comunes**

El acceso condicional tiene en cuenta señales de varios orígenes al tomar decisiones de acceso.



**Importante**

Las directivas de acceso condicional se aplican una vez que se completa la autenticación en una fase. El acceso condicional no está pensado como una primera línea de defensa de una organización en escenarios como los ataques por denegación de servicio (DoS), pero puede usar señales de estos eventos para determinar el acceso.

**Señales comunes**

Estas señales incluyen:

* Pertenencia a un usuario o grupo
  + Las directivas pueden dirigirse a usuarios y grupos concretos, lo que proporciona a los administradores un mayor control sobre el acceso.
* Información de la ubicación de la IP
  + Las organizaciones pueden crear intervalos de direcciones IP de confianza que se pueden usar al tomar decisiones sobre directivas.
  + Los administradores pueden especificar que se bloquee o se permita el tráfico de intervalos de direcciones IP de países o regiones completos.
* Dispositivo
  + Los usuarios con dispositivos de plataformas concretas o marcados con un estado concreto se pueden usar al aplicar directivas de acceso condicional.
  + Use filtros para los dispositivos a fin de destinar directivas a dispositivos específicos, como estaciones de trabajo de acceso con privilegios.
* Aplicación
  + Los usuarios que intentan acceder a aplicaciones específicas pueden activar diferentes directivas de acceso condicional.
* Detección de riesgo calculado y en tiempo real
  + La integración de señales con Microsoft Entra ID Protection permite que las directivas de acceso condicional identifiquen y corrijan a los usuarios y comportamientos de inicio de sesión peligrosos.
* Microsoft Defender for Cloud Apps
  + Permite supervisar y controlar en tiempo real el acceso a las aplicaciones y las sesiones de los usuarios. Esta integración aumenta la visibilidad y el control sobre el acceso y las actividades realizadas en el entorno de la nube.

**Decisiones comunes**

* Bloquear acceso
  + Decisión más restrictiva
* Conceder acceso
  + La decisión menos restrictiva, puede requerir una o varias de las opciones siguientes:
    - Requiere autenticación multifactor
    - Requerir que el dispositivo esté marcado como compatible
    - Requerimiento de dispositivos híbridos unidos a Microsoft Entra ID
    - Requerir aplicación cliente aprobada

**Directivas aplicadas habitualmente**

Muchas organizaciones tienen problemas de acceso comunes que las directivas de Acceso condicional pueden solucionar si, por ejemplo:

* Requerir la autenticación multifactor a los usuarios con roles administrativos
* Requerir la autenticación multifactor para las tareas de administración de Azure
* Bloquear los inicios de sesión a los usuarios que intenten usar protocolos de autenticación heredados
* Se exigen ubicaciones de confianza para el registro de la autenticación multifactor de Microsoft Entra ID
* Bloquear o conceder el acceso desde ubicaciones concretas
* Bloquear de comportamientos de inicio de sesión peligrosos
* Requerir dispositivos administrados por la organización para aplicaciones concretas

**Prueba de conocimientos**

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

**Comprobación de conocimientos**

Principio del formulario

**1. Un administrador de roles con privilegios debe asignar un rol a un usuario. ¿Cuáles son los dos pasos principales del proceso de asignación de roles?**

1. Vaya a Identidad, Usuarios, Todos los usuarios y seleccione el usuario.
2. Seleccione el usuario y ajuste la configuración del rol.
3. Seleccione el rol para asignar y ajustar la configuración y la duración del rol.

**2. Una organización quiere revisar periódicamente el acceso a los recursos de Azure con privilegios y a los roles de Microsoft Entra ID. ¿Qué herramienta puede usar para crear revisiones de acceso para el acceso con privilegios?**

1. Microsoft Advanced Threat Analytics
2. Protección de Microsoft Entra ID
3. Microsoft Entra Privileged Identity Management PIM

**3. Un responsable del equipo debe conceder acceso a un grupo de recursos específico en Azure. ¿Cuál es el primer paso que deben realizar?**

1. Haga clic en la pestaña Control de acceso y seleccione el rol que se va a asignar.
2. Seleccione el usuario, el grupo o la entidad de servicio para asignar el rol seleccionado.
3. Identifique el ámbito necesario mediante la búsqueda del grupo de recursos en Azure Portal.

**4. Una empresa quiere habilitar la administración de permisos para su organización. ¿Cuál es el primer paso que deben realizar?**

1. Activación de una versión de prueba gratuita o una licencia de pago a través de Azure Portal
2. Póngase en contacto con su representante de Microsoft para contratos de licencias por volumen o Enterprise
3. Asegúrese de que tienen un inquilino de Microsoft Entra ID y son aptos para o tienen una asignación activa al rol Administrador de administración de permisos

**5. Un administrador de seguridad debe agregar una asignación de roles para un nuevo usuario. ¿Qué paso debe llevar a cabo para agregar una condición a la asignación de roles?**

1. Omita la pestaña Condiciones y vaya a la pestaña Revisar asignación.
2. Seleccione la opción Sin restricciones en Tipo de delegación en la pestaña Condiciones.
3. Seleccione la opción recomendada Restringida en Tipo de delegación en la pestaña Condiciones.
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo se trata la administración de la autorización en Microsoft Entra ID, centrándose en configurar permisos de rol, asignar roles, implementar la administración de permisos y Privileged Identity Management, administrar roles y revisiones de acceso, y aplicar directivas de acceso condicional para el control de acceso a recursos.