Exploración del modelo de confianza cero

Atrás quedaron los días en los que la seguridad se centraba en una defensa perimetral sólida para mantener alejados a los hackers malintencionados.

Cualquier cosa fuera del perímetro se trataba como una amenaza, mientras que dentro, se confiaba en los sistemas de la organización. La posición de seguridad actual es asumir que ha habido una vulneración y usar el modelo de confianza cero. Los profesionales de seguridad ya no se centran en la defensa perimetral. Las organizaciones modernas tienen que admitir el acceso a datos y servicios de forma uniforme desde dentro y fuera del firewall corporativo.

Este curso le servirá como hoja de ruta al crear y mover aplicaciones y datos a Microsoft Azure. Comprender los servicios de seguridad que Azure ofrece es fundamental para implementar servicios con seguridad mejorada.

¿Qué significa Confianza cero?

El modelo de análisis Confianza cero indica que nunca debe asumirse la confianza, sino que debe validarse continuamente. Cuando los usuarios, los dispositivos y los datos residían en el firewall de la organización, se daba por sentado que eran de confianza. Esta confianza dada por sentado permitía un movimiento lateral sencillo después de que un hacker malintencionado pusiera en peligro un dispositivo de punto de conexión.

En lugar de suponer que todo lo que hay detrás del firewall corporativo es seguro, el **modelo de Confianza cero asume que puede existir una vulneración y comprueba cada solicitud como si se originara en una red abierta**. Con independencia de dónde se origine la solicitud o a qué recursos acceda, el modelo de Confianza cero nos enseña a **nunca confiar, siempre comprobar**. Todas las solicitudes de acceso se autentican, autorizan y cifran por completo antes de concederse el acceso. Se aplican los principios de microsegmentación y acceso con privilegios mínimos para minimizar el movimiento lateral. La inteligencia y el análisis enriquecidos se usan para detectar anomalías y responder a estas en tiempo real. Ahora que la mayoría de los usuarios accede a las aplicaciones y a los datos desde Internet, la mayor parte de los componentes de las transacciones (es decir, los usuarios, la red y los dispositivos) ya no están totalmente bajo el control de la organización.

El modelo de Confianza cero se basa en notificaciones de confianza de usuario y de dispositivo comprobables para conceder acceso a los recursos de la organización. Ya no se da por hecha la confianza en función de la ubicación dentro del perímetro de una organización.

En la ilustración siguiente se muestran los componentes básicos del modelo de Confianza cero.

Observe los componentes de determinación de la confianza:

- **Proveedor de identidades**. Establece la identidad de un usuario y la información relacionada.
- **Directorio del dispositivo**. Valida un dispositivo y la integridad de este.

- **Servicio de evaluación de directivas**. Determina si el usuario y el dispositivo cumplen las directivas de seguridad.
- **Proxy de acceso**. Determina a qué recursos de la organización se puede acceder.

Implementación de un modelo de seguridad de Confianza cero

La migración a un modelo de seguridad de Confianza cero ofrece la mejora simultánea de la seguridad con respecto a los enfoques convencionales basados en la red y de las posibilidades de acceso de los usuarios donde lo necesiten. Un modelo de Confianza cero requiere **señales** para informar sobre las decisiones, **directivas** para tomar decisiones de acceso y **capacidades de cumplimiento** para implementar esas decisiones de manera eficaz.

Señal: para tomar una decisión fundamentada.	**Decisión**: basada en la directiva de la organización.	**Cumplimiento**: de la directiva entre los recursos.
El modelo de Confianza cero tiene en cuenta numerosos orígenes de señal (desde sistemas de identidad hasta herramientas de administración de dispositivos y de seguridad de dispositivos) para obtener conclusiones con un contexto completo que ayude a tomar decisiones fundamentadas.	La solicitud de acceso y la señal se analizan para ofrecer una decisión basada en directivas de acceso bien ajustadas, lo que proporciona un control de acceso detallado y centrado en la organización.	A continuación, se aplican las decisiones en todo el patrimonio digital, como el acceso de solo lectura a la aplicación SaaS o la corrección de contraseñas en peligro con un autoservicio de restablecimiento de contraseña.

El usuario es el denominador común de estos componentes. Como se ha explicado anteriormente, esa es la razón por la que la identidad de un usuario y cómo se administra esa identidad ahora se denomina **plano de control**. Si no se puede determinar quién es el usuario, no se puede establecer una relación de confianza para otras transacciones.

Principios rectores de Confianza cero

- **Comprobación de forma explícita**. Autentique y autorice siempre las aplicaciones en función de todos los puntos de datos disponibles, como la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de los datos y las anomalías.
- **Uso de acceso con privilegios mínimos**. Limite el acceso de los usuarios con **Just-in-Time** y **Just-Enough Access (JIT/JEA)**, las directivas de adaptación basadas en riesgos y la protección de datos para proteger los datos y la productividad.
- **Asunción de infracciones de seguridad**. Minimice el radio de impacto de las vulneraciones y evite el desplazamiento lateral mediante la segmentación del acceso por red, usuario, dispositivos y reconocimiento de aplicaciones. Compruebe que todas las sesiones están

cifradas de un extremo a otro. Utilice el análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

Arquitectura de Confianza cero de Microsoft

A continuación, se muestra una arquitectura de referencia simplificada para nuestro enfoque de implementación de Confianza cero. Los componentes principales de este proceso son Intune para la administración de dispositivos y la configuración de directivas de seguridad de dispositivos, el acceso condicional de Azure AD para la validación del estado del dispositivo y Azure AD para el inventario de usuarios y dispositivos.

El sistema funciona con Intune, lo que permite insertar los requisitos de configuración de dispositivos en los dispositivos administrados. A continuación, el dispositivo genera un informe de mantenimiento, que se almacena en Azure AD. Cuando el usuario del dispositivo solicita acceso a un recurso, el estado de mantenimiento del dispositivo se comprueba como parte del intercambio de autenticación con Azure AD.

Importante

El Instituto Nacional de Estándares y Tecnología tiene una publicación sobre la arquitectura de Confianza cero, NIST 800-207.

Revisión de la evolución de la administración de identidades

Microsoft Identity Manager o MIM ayuda a las organizaciones a administrar los usuarios, las credenciales, las directivas y el acceso dentro de sus organizaciones y entornos híbridos. Con MIM, las organizaciones pueden simplificar la administración del ciclo de vida de la identidad con flujos de trabajo automatizados, reglas de negocio y una integración sencilla con plataformas heterogéneas en todo el centro de datos. MIM permite que las instancias de Active Directory Domain Services tengan los usuarios y los derechos de acceso adecuados para las aplicaciones locales. Después, Azure AD Connect puede hacer que esos usuarios y permisos estén disponibles en Azure AD para las aplicaciones de Microsoft 365 y hospedadas en la nube.

Una instancia local de Active Directory Domain Services, Azure Active Directory (Azure AD) o una combinación híbrida de ambos ofrecen servicios para la autenticación de usuarios y dispositivos, la administración de identidades y roles y el aprovisionamiento.

La identidad se ha convertido en el factor común entre diversos servicios, como Microsoft 365 y Xbox Live, donde el usuario es el centro de los servicios. La identidad es ahora el límite de seguridad, el nuevo firewall, el plano de control... como prefiera llamarlo. Su identidad digital es la combinación de quién es y qué se le permite hacer. Es decir:

Credenciales y privilegios = identidad digital

El primer paso es ayudar a proteger las cuentas con privilegios.

Estas identidades tienen más derechos de usuario de lo normal y, en caso de peligro, permiten que un hacker malintencionado acceda a recursos corporativos confidenciales. Ayudar a proteger estas identidades con privilegios es un paso fundamental a la hora de establecer garantías de seguridad para los recursos empresariales en una organización moderna. Los ciberdelincuentes tienen como fin estas cuentas y otros servicios con privilegios en su cadena de ataque para lograr sus objetivos.

Evolución de las identidades

La administración de identidades ha evolucionado del enfoque tradicional hasta llegar al óptimo, pasando por el avanzado.

Enfoques de identidad tradicionales

- Proveedores de identidades locales.
- No hay ningún inicio de sesión único presente entre las aplicaciones en el entorno local y en la nube.

- La visibilidad del riesgo de las identidades es muy limitada.

Enfoques de identidad avanzados

- La identidad en la nube se federa con los sistemas de identidad en la nube.
- Las directivas de acceso condicional regulan el acceso y proporcionan acciones correctivas.
- Los análisis mejoran la visibilidad del riesgo de identidad.

Enfoques de identidad óptimos

- La autenticación sin contraseña está habilitada.
- El usuario, la ubicación, los dispositivos y el comportamiento se analizan en tiempo real.
- Protección continua frente al riesgo de identidad.

Pasos para un mundo sin contraseña

- **Exigir MFA**: se ajusta al estándar Fast Identity Online (FIDO) 2.0, por lo que puede requerir un PIN y datos biométricos para la autenticación en lugar de una contraseña. Windows Hello es un buen ejemplo, pero elija el método MFA que mejor funcione para su organización.
- **Reducir flujos de trabajo de autenticación heredados**: coloque las aplicaciones que requieran contraseñas en un portal de acceso de usuario independiente y migre los usuarios a flujos de autenticación modernos siempre que pueda. En Microsoft, solo el 10 por ciento de los usuarios escriben una contraseña en un día determinado.
- **Quitar contraseñas**: cree coherencia entre Active Directory Domain Services y Azure Active Directory (Azure AD) para permitir que los administradores puedan eliminar contraseñas del directorio de identidad.

Importante

Se recomienda **Azure AD Privileged Identity Management** como servicio de ayuda a la protección de cuentas con privilegios.

Implementación de Azure AD Privileged Identity Management

Con los servicios de Azure AD Privileged Identity Management (PIM), puede administrar, controlar y supervisar el acceso a recursos importantes en su organización. Esto incluye el acceso a los recursos de Azure AD, Azure y otros servicios en línea de Microsoft, como Microsoft 365 o Microsoft Intune. Este control no elimina la necesidad de que los usuarios lleven a cabo operaciones con privilegios en Azure AD, Azure, Microsoft 365 y aplicaciones de software como servicio (SaaS).

Las organizaciones pueden conceder a los usuarios privilegios de acceso "Just-In-Time" (JIT) a los recursos de Azure y a Azure AD. Es necesario supervisar lo que hacen esos usuarios con sus privilegios de administrador. PIM ayuda a mitigar el riesgo de derechos de acceso excesivos, innecesarios o mal usados.

Características clave de PIM

- Concesión de acceso con privilegios **Just-In-Time** a los recursos de Azure y Azure AD. Los administradores de TI pueden elegir un período de activación entre 0,5 y la duración máxima de un rol (máximo de 24 horas). Solo recibirán el privilegio durante ese período de tiempo. Una vez transcurrido el período de activación, los administradores tendrán que volver a realizar el proceso para activar.
- Asignación de acceso con **límite de tiempo** a los recursos mediante el uso de fechas de inicio y fin. PIM permite establecer una hora de finalización para el rol. Esto es especialmente útil en un escenario de invitado. Si la organización tiene invitados que trabajan durante un tiempo específico, el privilegio del rol expirará de forma automática.
- Requisito de **aprobación** para activar los roles con privilegios. Puede designar uno o varios aprobadores. Estos recibirán un correo electrónico cuando se realice una solicitud. Se requiere la aprobación para activar el privilegio.
- Aplicación de **Azure Multi-Factor Authentication** (MFA) para activar cualquier rol. Si la organización ya ha habilitado MFA, PIM no pedirá al usuario que vuelva a iniciar sesión.
- Uso de la **justificación** para comprender por qué se activan los usuarios. Esto beneficia tanto a los auditores internos como externos para entender por qué se activó el rol. También puede requerir un número de vale de servicio de cualquier producto de servicio que use.
- Obtención de **notificaciones** cuando se asigna un privilegio a un usuario y cuando el privilegio se activa.
- Realización de **revisiones de acceso** para saber qué usuarios tienen roles con privilegios en la organización y si aún los necesitan.
- Descarga del **historial de auditoría** para una auditoría interna o externa. De esta forma, se realiza un seguimiento de todos los eventos de PIM.

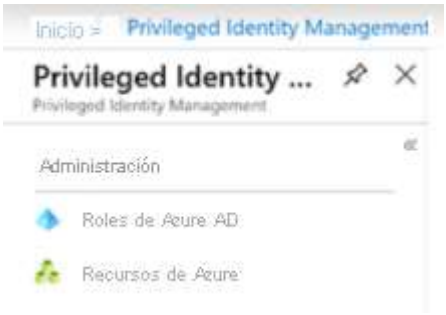
Formas de usar PIM

Azure AD PIM se usa para lo siguiente:

- Ver los usuarios que tienen asignados roles con privilegios para administrar los recursos de Azure, así como los usuarios que tienen asignados roles administrativos en Azure AD.
- Habilitar el acceso administrativo "Just-In-Time" a petición a servicios de Microsoft Online Services, como Microsoft 365 e Intune, y a recursos de Azure de las suscripciones, grupos de recursos y recursos individuales, como máquinas virtuales.
- Revisar un historial de activación del administrador, incluidos los cambios que los administradores han realizado en los recursos de Azure.
- Obtener alertas sobre los cambios en las asignaciones del administrador.
- Requerir la aprobación para activar los roles de administrador con privilegios de Azure AD.

- Revisar la pertenencia a roles administrativos y requerir a los usuarios que proporcionen una justificación para la pertenencia continuada.

Configuración del ámbito de Privileged Identity Management



- **Roles de Azure AD**. Todos estos roles están en Azure Active Directory (por ejemplo, Administrador global, Administrador de Exchange y Administrador de seguridad). Puede leer más sobre los roles y sus funcionalidades en Permisos de roles de administrador en Azure Active Directory.
- **Roles de recursos de Azure**. Estos roles están vinculados a un recurso, grupo de recursos, suscripción o grupo de administración de Azure. Privileged Identity Management ofrece acceso Just-In-Time a ambos roles integrados, como propietario, administrador de acceso de usuario y colaborador, así como roles personalizados.

Roles de Azure AD

Se pueden asignar usuarios a distintos roles administrativos en Azure AD. Estas asignaciones de roles controlan las tareas (como agregar o quitar usuarios o cambiar la configuración del servicio) que los usuarios pueden realizar en Azure AD, Microsoft 365 y en otras aplicaciones conectadas y de Microsoft Online Services.

Un administrador global puede actualizar los usuarios que están asignados **permanentemente** a roles de Azure AD, con cmdlets de PowerShell como Add-MsolRoleMember y Remove-MsolRoleMember o a través de Azure Portal.

Privileged Identity Management (PIM) de Azure AD administra las directivas de acceso con privilegios para los usuarios en Azure AD. PIM asigna a usuarios a uno o varios roles de Azure AD y puede asignar una persona para que esté permanentemente en el rol o sea apta para el rol. Cuando un usuario está asignado permanentemente a un rol o activa una asignación de roles elegibles, este puede administrar Azure Active Directory, Microsoft 365 y otras aplicaciones con los permisos asignados a sus roles.

No hay ninguna diferencia en el acceso proporcionado de forma permanente a una persona o una asignación de roles aptos. La única diferencia es que algunas personas no necesitan ese acceso todo el tiempo. Son aptas para el rol y, pueden activarlas y desactivarlas cada vez que lo necesiten.

Roles administrados en PIM

Privileged Identity Management (PIM) permite asignar usuarios a roles de administrador comunes, como los siguientes:

- **administrador global** (también conocido como "administrador de la compañía") tiene acceso a todas las características administrativas. Puede tener más de un administrador global en la organización. La persona que se suscribe para comprar Microsoft 365 se convierte automáticamente en administrador global.
- **administrador de roles con privilegios** administra PIM de Azure AD y actualiza las asignaciones de roles para otros usuarios.
- **Administrador de facturación** : hace compras, administra suscripciones, administra incidencias de soporte técnico y supervisa el estado del servicio.
- **Administrador de contraseñas**: restablece contraseñas, administra solicitudes del servicio y supervisa el estado de dicho servicio. Los administradores de contraseñas están limitados a restablecer las contraseñas de los usuarios.
- **Administrador de servicios** : administra las solicitudes de servicio y supervisa el estado del servicio.

Nota

Si usa Microsoft 365, antes de asignar el rol de administrador de servicios a un usuario, asigne primero los permisos administrativos de usuario a un servicio, como Exchange Online.

- **administrador de control de usuarios** restablece las contraseñas, supervisa el estado del servicio y administra cuentas de usuario, grupos de usuarios y solicitudes de servicio. El administrador de usuarios no puede eliminar a un administrador global, crear otros roles de administrador o restablecer contraseñas de los administradores de facturación, globales y de servicios.
- **Administrador de Exchange**: tiene acceso administrativo a Exchange Online a través del centro de administración de Exchange (EAC) y puede realizar prácticamente cualquier tarea en Exchange Online.
- **Administrador de SharePoint**: tiene acceso administrativo a SharePoint Online a través del centro de administración de SharePoint Online y puede realizar prácticamente cualquier tarea en SharePoint Online.
- **Administrador de Skype Empresarial**: tiene acceso administrativo a Skype Empresarial a través del centro de administración de Skype Empresarial y puede realizar prácticamente cualquier tarea en Skype Empresarial Online.

Roles no administrados en PIM

Los roles de Exchange Online o SharePoint Online, excepto los mencionados anteriormente, no están representados en Azure AD y, por lo tanto, no son visibles en PIM. Las suscripciones de Azure y los grupos de recursos tampoco están representados en Azure AD.

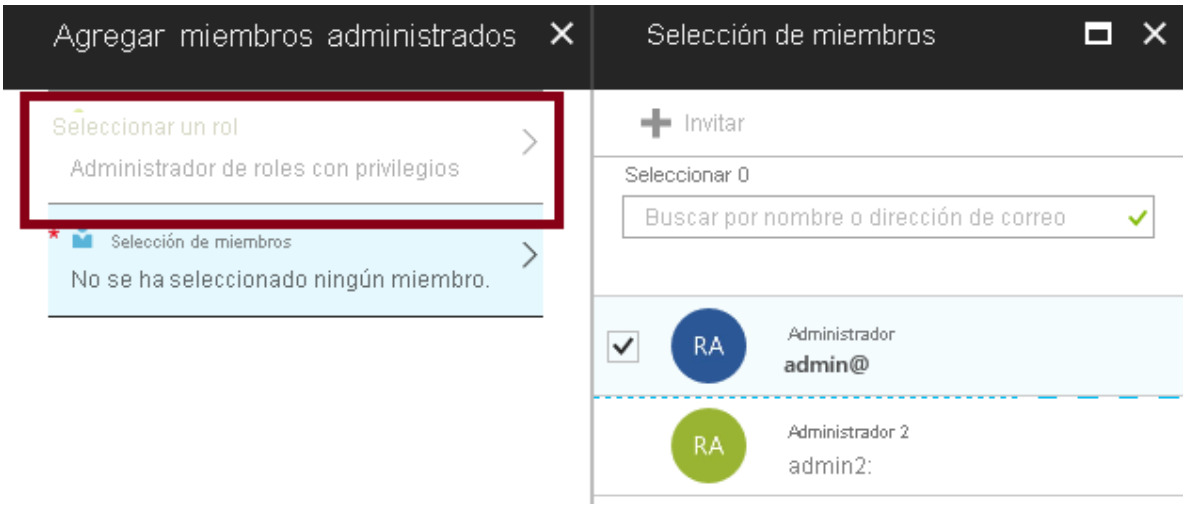
Recursos de Azure

La primera vez que se configura Privileged Identity Management para recursos de Azure, es preciso detectar y seleccionar los recursos que se van a proteger con Privileged Identity Management. No hay ningún límite en cuanto al número de recursos que se pueden administrar con Privileged Identity Management. Pero se recomienda empezar por los recursos más críticos (producción).

Implementación de la incorporación de Privileged Identity Management

Para usar PIM, necesita una de las licencias de pago o de prueba siguientes: Azure AD Premium P2, Enterprise Mobility + Security (EMS) E5 o Microsoft 365 M5.

Acceso de PIM



Al primer administrador global que use PIM en la instancia de Azure AD se le asignan automáticamente los roles de Administrador de seguridad y Administrador de roles con privilegios en el directorio. Este debe ser un usuario de Azure AD elegible. Los administradores de rol con privilegios son los únicos que pueden administrar las asignaciones de roles de directorio de Azure AD de los usuarios. Además, puede optar por ejecutar el asistente para seguridad, que le guiará a través de las experiencias de detección y asignación iniciales.

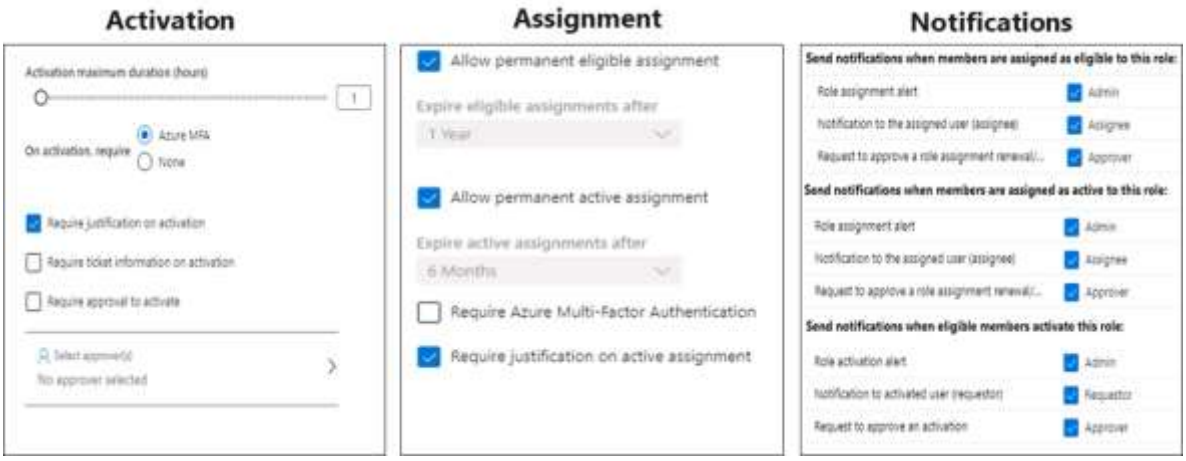
Los usuarios o los miembros de un grupo que tengan asignados los roles Propietario o Administrador de acceso de usuario, así como los administradores globales que habiliten la administración de suscripciones en Azure AD, son administradores de recursos. Estos administradores pueden asignar roles, configurar valores de los roles y revisar el acceso con PIM para los recursos de Azure.

Nadie más en la organización de Azure Active Directory (Azure AD) obtiene acceso de escritura de forma predeterminada, incluidos otros administradores globales. Otros administradores globales, administradores de seguridad y lectores de seguridad tienen acceso de solo lectura a Privileged Identity Management. Para conceder acceso a Privileged Identity Management, el primer usuario puede asignar a otros el rol **Administrador de roles con privilegios**.

Importante

Asegúrese de que siempre haya al menos dos usuarios en un rol de administrador de roles con privilegios, por si se diera el caso de que a un usuario se le impida el acceso o su cuenta se elimine.

Exploración de las opciones de configuración de Privileged Identity Management



Configuración de activación

- **Duración de la activación**. Establezca el tiempo máximo, en horas, que un rol permanece activo antes de expirar. Este valor puede oscilar entre una y 24 horas.
- **Requerir autenticación multifactor en la activación**. Puede requerir que los usuarios aptos para un rol demuestren quiénes son con Azure Active Directory Multi-Factor Authentication (MFA) antes de poder activarse. La autenticación multifactor garantiza que el usuario sea quien dice ser con certeza razonable. Aplicar esta opción protege los recursos críticos en situaciones en las que es posible que la cuenta de usuario se haya puesto en peligro.
- **Requerir justificación**. Puede requerir que los usuarios escriban una justificación empresarial cuando se activen.
- **Se requiere aprobación para activar**. Si se establecen varios aprobadores, la aprobación se completa en cuanto uno de ellos aprueba o deniega. No se puede exigir la aprobación de al menos dos usuarios.

Configuración de la asignación

- **Permitir asignación elegible permanente**. Los administradores globales y los administradores de roles con privilegios pueden asignar una asignación elegible permanente. También se puede requerir que todas las asignaciones elegibles tengan una fecha de inicio y de finalización especificada.
- **Permitir asignaciones activas permanentes**. Los administradores globales y los administradores de roles con privilegios pueden realizar asignaciones elegibles activas.

También pueden requerir que todas las asignaciones activas tengan una fecha de inicio y de finalización especificada.

Nota

En algunos casos, es posible que quiera asignar un usuario a un rol durante un tiempo breve (por ejemplo, un día). En este caso, no es necesario que los usuarios asignados soliciten la activación. En este escenario, Privileged Identity Management no puede exigir la autenticación multifactor cuando el usuario usa su asignación de roles, porque ya está activa en el rol desde el momento en que se asigna.

Configuración de notificación

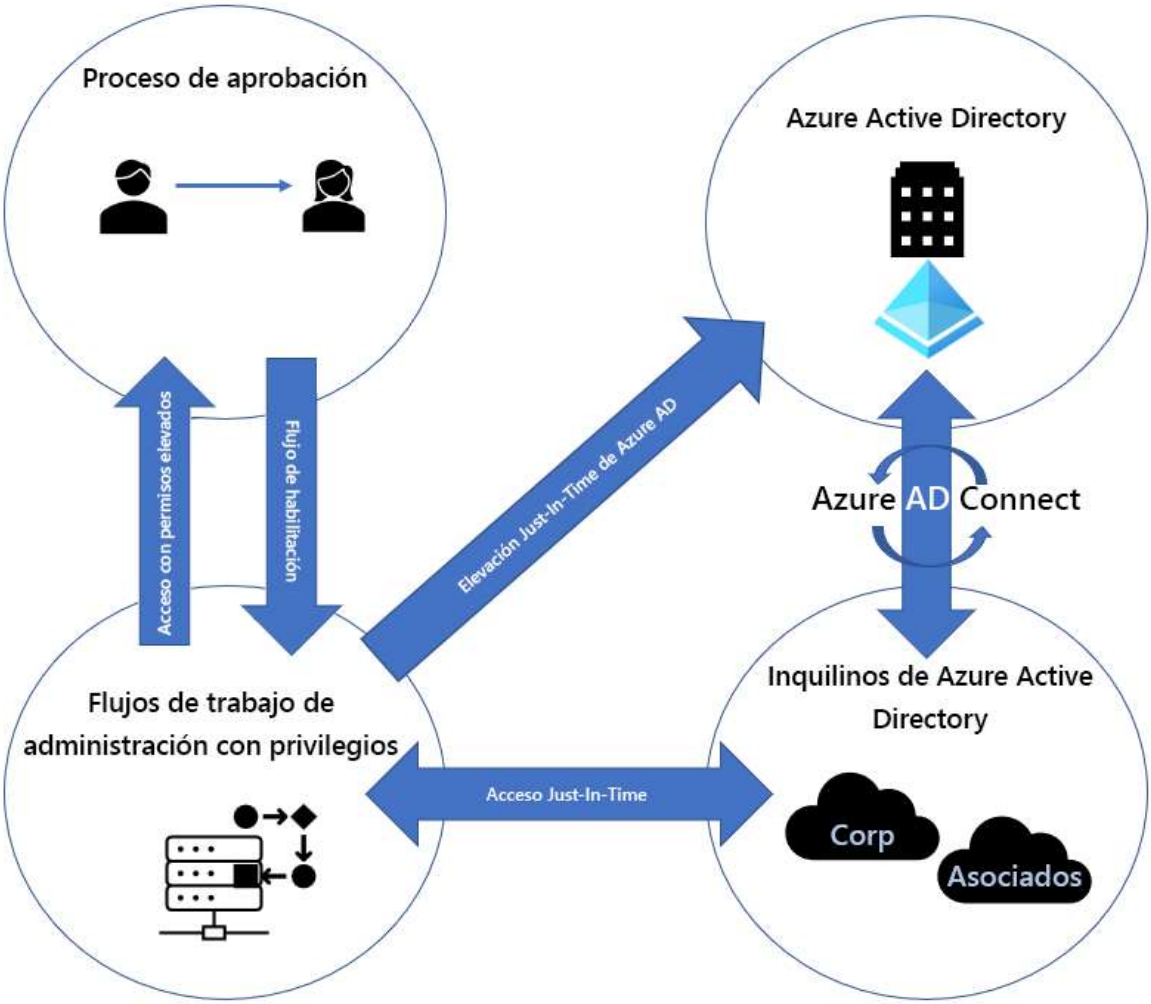
- Se pueden enviar notificaciones cuando los miembros estén asignados como elegibles o como activos en un rol y cuando el rol esté activado.
- Se pueden enviar notificaciones a los administradores, solicitantes y aprobadores.

Implementación de un flujo de trabajo de Privileged Identity Management

Ahora, al configurar Azure AD PIM para administrar los roles de acceso con privilegios elevados en Azure AD, tenemos acceso JIT a más de 28 roles con privilegios configurables. También podemos supervisar el acceso, auditar las elevaciones de las cuentas y recibir alertas adicionales a través de un panel de administración en Azure Portal.

El acceso con privilegios elevados incluye los roles de trabajos que necesitan un mayor acceso, incluidos el soporte técnico, los administradores de recursos, los propietarios de recursos, los administradores de servicios y los administradores globales. El acceso basado en roles se administra en el nivel de recurso. Dado que las cuentas de acceso con privilegios elevados pueden utilizarse de forma incorrecta si están en peligro, racionalizamos las nuevas solicitudes de acceso con privilegios elevados y llevamos a cabo una nueva atestación periódica para los roles con privilegios elevados.

A continuación se muestra un diagrama del flujo de trabajo de acceso elevado.



Acceso de administrador JIT

Anteriormente, podíamos asignar un empleado a un rol administrativo a través de Azure Portal o de Windows PowerShell y ese empleado sería un administrador permanente; su acceso elevado permanecería activo en el rol asignado.

Con Azure AD PIM se introdujo el concepto de administradores permanentes y elegibles en Azure AD y Azure. Los administradores permanentes tienen conexiones de roles con privilegios elevados persistentes, mientras que los administradores elegibles tienen acceso con privilegios solo cuando lo necesitan. El rol de administrador elegible está inactivo hasta que el empleado necesita acceso; en ese momento, se realiza un proceso de activación y se convierte en administrador activo durante un período de tiempo establecido. Hemos dejado de usar los administradores permanentes para las cuentas individuales con nombre, aunque tenemos algunas cuentas de servicio automatizadas que siguen usando el rol.

Activación de rol en Azure Active Directory

Azure AD PIM usa roles administrativos, como el de administrador de inquilinos y el administrador global, para administrar el acceso temporal a diversos roles. Con Azure AD PIM, puede agregar o

quitar administradores permanentes o elegibles en cada rol para administrarlos. Azure AD PIM incluye varios roles de Azure AD integrados, así como de Azure, que podemos administrar.

Para activar un rol, un administrador elegible inicializa Azure AD PIM en Azure Portal y solicita la activación de rol por tiempo limitado. La activación se solicita mediante la opción Activate my role (Activar mi rol) en Azure AD PIM. Los usuarios que solicitan la activación deben cumplir las directivas de acceso condicional para asegurarse de que proceden de ubicaciones y dispositivos autorizados y sus identidades deben comprobarse mediante la autenticación multifactor.

Para ayudar a proteger las transacciones a la vez que se habilita la movilidad, se usa Azure AD PIM para personalizar las variables de activación de roles en Azure, incluido el número de intentos de inicio de sesión, el período de tiempo que el rol se activa después del inicio de sesión y el tipo de credenciales que se requiere (como el inicio de sesión único o la autenticación multifactor).

En Microsoft, cuando un individuo se une a un equipo o cambia de equipo, puede que necesite derechos administrativos para el nuevo rol de negocio. Por ejemplo, puede que alguien se una a un equipo en el que su cuenta de usuario vaya a requerir derechos de acceso con privilegios de administrador de Exchange Online en el futuro. Ese usuario realiza una solicitud y, a continuación, el administrador la valida, al igual que hace un propietario de servicio. Con esas aprobaciones, se notifica a los administradores de Core Services Engineering and Operations (CSEO, anteriormente Microsoft IT) en el rol de Administrador de roles con privilegios. Un administrador CSEO usa Azure AD PIM a través de Azure Portal para hacer que ese usuario sea elegible para el rol. Después, el usuario puede utilizar Azure AD PIM para activar el rol.

Seguimiento del uso de roles con privilegios mediante el panel

Un panel en Azure Portal ofrece una vista centralizada de lo siguiente:

- Alertas que señalan oportunidades para mejorar la seguridad.
- Número de usuarios asignados a cada rol con privilegios.
- Número de administradores elegibles y permanentes.
- Revisiones de acceso en curso.

Se puede realizar un seguimiento de la forma en que los empleados y los administradores usan sus roles con privilegios mediante la visualización del historial de auditoría o la configuración de una revisión de acceso normal. Ambas opciones están disponibles a través del panel de PIM en Azure Portal.

El registro de auditoría de PIM realiza un seguimiento de los cambios en las asignaciones de roles con privilegios y del historial de activación de roles. Se usa el registro de auditoría para ver todas las asignaciones y activaciones de usuario en un período especificado. El historial de auditoría nos ayuda a determinar, en tiempo real, qué cuentas no han iniciado sesión recientemente o si los empleados han cambiado de roles.

Las revisiones de acceso las puede realizar un revisor asignado o bien los empleados pueden revisarse a sí mismos. Esta es una forma eficaz de supervisar quién sigue necesitando acceso y quién puede quitarse.

Revisaremos los datos que se recopilan y el equipo de supervisión evaluará la mejor forma de configurar alertas de supervisión para que se nos informe sobre los cambios fuera de banda; por ejemplo, si se crean demasiados roles de administrador para un recurso de Azure. La información también nos ayuda a determinar si la configuración de tiempo de elevación actual es adecuada para los distintos roles de administrador con privilegios.

Al igual que todas las organizaciones, queremos minimizar el número de personas que tienen acceso a la información segura o a los recursos, ya que de esta manera se reduce la posibilidad de que usuarios malintencionados obtengan acceso a ellos o de que algún usuario autorizado haga algo involuntariamente que pueda afectar a los recursos confidenciales. Sin embargo, nuestros usuarios aún tienen que realizar operaciones con privilegios en aplicaciones de Azure AD, Azure, Microsoft 365 y SaaS. Podemos proporcionar a los usuarios acceso con privilegios para recursos de Azure, como las suscripciones, y Azure AD. Es necesario supervisar lo que hacen nuestros usuarios con sus privilegios de administración. Se utiliza Azure AD PIM para mitigar el riesgo de derechos de acceso excesivos, innecesarios y mal usados.

En Azure AD, usamos Azure AD PIM para administrar los usuarios que asignamos a roles organizativos de Azure AD integrados, como el de Administrador global. En Azure, usamos Azure AD PIM para administrar los usuarios y grupos que asignamos a través de roles de RBAC de Azure, incluidos el de Propietario y Colaborador.