Descripción de Azure Active Directory

Azure Active Directory (Azure AD) es un servicio de administración de acceso y de identidades basado en la nube de Microsoft. Las organizaciones usan Azure AD para permitir que sus empleados, invitados y otros usuarios inicien sesión y tengan acceso a los recursos que necesitan, incluidos:

- Recursos internos, como las aplicaciones de la red corporativa y la intranet, junto con todas las aplicaciones en la nube que haya desarrollado su propia organización.
- Servicios externos, como Microsoft Office 365, Azure Portal y cualquier aplicación SaaS que use su organización.

Azure AD simplifica la forma en que las organizaciones administran la autorización y el acceso, ya que proporciona un sistema de identidad único para sus aplicaciones locales y en la nube. Igualmente, Azure AD se puede sincronizar con la instancia de Active Directory local existente, con otros servicios de directorio o se puede usar como un servicio independiente.

Azure AD también permite a las organizaciones habilitar de manera segura el uso de dispositivos personales, como dispositivos móviles y tabletas, y permitir la colaboración con clientes y asociados comerciales.

Los administradores de TI usan Azure AD para controlar el acceso a los recursos y a las aplicaciones corporativas, en función de los requisitos empresariales. También puede configurarse para requerir la autenticación multifactor cuando el usuario intenta acceder a recursos importantes de la organización. Además, Azure AD se puede usar para automatizar el aprovisionamiento de

usuarios entre una instancia de Windows Server AD existente y aplicaciones en la nube, incluyendo Microsoft 365. Por último, Azure AD proporciona herramientas eficaces que le ayudarán a proteger automáticamente las identidades y credenciales de los usuarios y a cumplir los requisitos de gobernanza de acceso de la empresa.

Los desarrolladores usan Azure AD como un enfoque basado en estándares para agregar el inicio de sesión único (SSO) a sus aplicaciones, de modo que los usuarios puedan iniciar sesión con credenciales ya existentes. Asimismo, Azure AD también proporciona varias API que permiten que los desarrolladores creen experiencias de aplicación personalizadas que usen los datos existentes de la organización.

Los suscriptores de servicios de Azure, Microsoft 365 o Dynamics 365 tienen acceso automático a Azure AD. Los usuarios de estos servicios pueden sacar provecho de los servicios de Azure AD incluidos y también pueden mejorar su implementación de Azure AD mediante la actualización a licencias Premium de Azure AD.

Descripción de las ediciones de Azure AD disponibles

Azure AD está disponible en cuatro ediciones: gratuita, aplicaciones de Office 365, Premium P1 y Premium P2.

Azure Active Directory Free. La versión gratuita le permite administrar usuarios y crear grupos, sincronizarse con la instancia local de Active Directory, crear informes básicos, configurar el cambio de contraseña de autoservicio para usuarios en la nube y habilitar el inicio de sesión único en Azure, Microsoft 365 y muchas otras aplicaciones populares de SaaS. La edición gratuita se incluye con las suscripciones a Office 365, Azure, Dynamics 365, Intune y Power Platform.

Aplicaciones de Office 365. La edición de Aplicaciones de Office 365 le permite hacer todo lo que se incluye en la versión gratuita, más la opción de restablecer la contraseña de autoservicio para usuarios en la nube y la reescritura de dispositivos, que ofrece una sincronización bidireccional entre directorios locales y Azure AD. La edición de Aplicaciones de Office 365 de Azure Active Directory se incluye en las suscripciones a Office 365 E1, E3, E5, F1 y F3.

Azure Active Directory Premium P1. La edición Premium P1 incluye todas las características de las ediciones Gratis y Aplicaciones de Office 365. También admite la administración avanzada, como grupos dinámicos, administración de grupos de autoservicio, Microsoft Identity Manager (un conjunto de administración local de identidades y acceso) y funcionalidades de reescritura en la nube, que permiten el restablecimiento de contraseña de autoservicio a los usuarios locales.

Azure Active Directory Premium P2. La versión P2 le ofrece todas las características de la edición Premium P1 y Azure Active Directory Identity Protection para facilitar el acceso condicional basado en riesgos a las aplicaciones y a los datos críticos de la empresa. Asimismo, la edición P2 también le proporciona la instancia de Privileged Identity Management que le permitirá detectar, restringir y supervisar a los administradores y su acceso a los recursos y proporcionar acceso de tipo "Just-in-Time" cuando sea necesario.

Para obtener más información sobre cada una de las ediciones, visite la página de precios de Azure Active Directory.

También hay una opción para las **licencias de características**de "**Pago por uso**". Puede obtener otras licencias de características por separado, como la opción Negocio a cliente (B2C) de Azure Active Directory. B2C puede ayudarle a proporcionar soluciones de administración de acceso y de identidad para las aplicaciones orientadas al cliente. Para más información, consulte Documentación de Azure Active Directory B2C.

Descripción de los tipos de identidad de Azure AD

Azure AD administra distintos tipos de identidades: usuarios, entidades de servicio, identidades administradas y dispositivos. En esta unidad, se detallará cada tipo de identidad de Azure AD.

Usuario

Una identidad de usuario es una representación de algo que se administra mediante Azure AD. Los empleados e invitados se representan como usuarios en Azure AD. Si tiene varios usuarios con las mismas necesidades de acceso, puede crear un grupo. Los grupos se usan para conceder permisos de acceso a todos los miembros del grupo, en lugar de tener que asignar derechos de acceso individualmente.

La colaboración de negocio a negocio (B2B) de Azure AD es una característica de External Identities e incluye una funcionalidad para agregar usuarios invitados. Gracias a la colaboración B2B, una organización puede compartir aplicaciones y servicios de forma segura con usuarios invitados de otra organización.

En la siguiente guía interactiva, agregará un nuevo usuario a Azure Active Directory. Seleccione la imagen siguiente para empezar y siga las indicaciones que aparecen en pantalla.

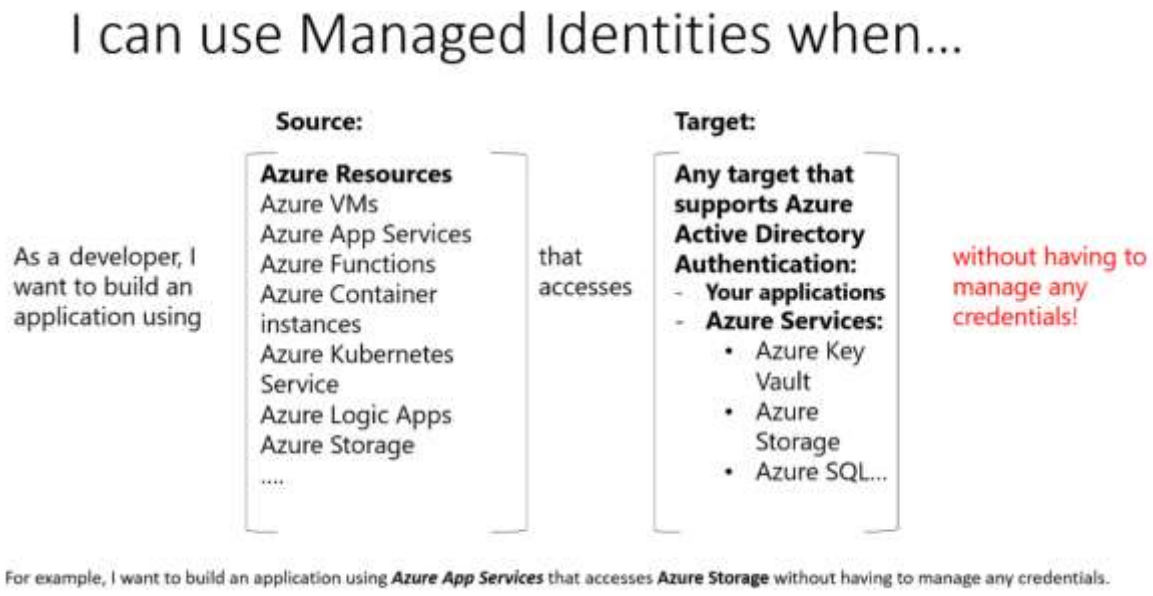
Entidad de servicio

Una entidad de servicio es, básicamente, una identidad para una aplicación. Para que una aplicación delegue su identidad y funciones de acceso a Azure AD, primero se debe registrar con Azure AD a fin de habilitar su integración. Una vez que se registra, se crea una entidad de servicio en cada inquilino de Azure AD donde se usa la aplicación. La entidad de servicio habilita características básicas como la autenticación y autorización de la aplicación en los recursos protegidos por el inquilino de Azure AD.

Para que las entidades de servicio puedan acceder a los recursos protegidos por el inquilino de Azure AD, los desarrolladores de aplicaciones deben administrar y proteger las credenciales.

Identidad administrada

Las identidades administradas son un tipo de entidad de servicio que se administran de forma automática en Azure AD y eliminan la necesidad de que los desarrolladores administren las credenciales. Las identidades administradas proporcionan una identidad para que la usen las aplicaciones al conectarse a recursos de Azure compatibles con la autenticación de Azure AD, sin costo adicional.



Para obtener una lista de los servicios de Azure que admiten identidades administradas, consulte la sección Más información de la unidad Resumen y recursos.

Hay dos tipos de identidades administradas: asignadas por el sistema y asignadas por el usuario.

Asignadas por el sistema. Algunos servicios de Azure permiten habilitar una identidad administrada directamente en una instancia de servicio. Cuando se habilita una identidad administrada asignada por el sistema, se crea una identidad en Azure AD que está vinculada al ciclo de vida de esa instancia de servicio. Por tanto, cuando se elimina el recurso, Azure elimina automáticamente la identidad. Por diseño, solo ese recurso de Azure puede usar esta identidad para solicitar tokens de Azure AD.

Asignadas por el usuario. También es posible crear una identidad administrada como un recurso independiente de Azure. Una vez que se crea una identidad administrada asignada por el usuario, puede asignarla a una o varias instancias de un servicio de Azure. En el caso de las identidades administradas asignadas por el usuario, la identidad se administra independientemente de los recursos que la utilicen.

En la tabla siguiente se resumen las diferencias entre las identidades administradas asignadas por el sistema y las que están asignadas por el usuario:

Propiedad	Identidad administrada asignada por el sistema	Identidad administrada asignada por el usuario
Creación	Se crea como parte de un recurso de Azure (por ejemplo, una máquina virtual de Azure o Azure App Service).	Se crea como un recurso de Azure independiente.
Ciclo de vida	Se comparte el ciclo de vida con el recurso de Azure. Si se elimina el recurso principal, se elimina también la identidad administrada.	Ciclo de vida independiente. Se debe eliminar explícitamente.
Uso compartido de recursos de Azure	No se puede compartir. Está asociada a un único recurso de Azure.	Se puede compartir. Una identidad administrada asignada por el usuario se puede asociar a más de un recurso de Azure.
Casos de uso comunes	Cargas de trabajo que contiene un único recurso de Azure. Cargas de trabajo para las que necesita identidades independientes, como una aplicación que se ejecuta en una sola máquina virtual.	Cargas de trabajo que se ejecutan en varios recursos y que pueden compartir una única identidad. Cargas de trabajo que necesitan autorización previa para un recurso seguro como parte de un flujo de aprovisionamiento. Cargas de trabajo donde los recursos se reciclan con frecuencia, pero los permisos deben permanecer coherentes. Por ejemplo, una carga de trabajo en la que varias máquinas virtuales tienen que acceder al mismo recurso.

Dispositivo

Un dispositivo es un producto de hardware, como los dispositivos móviles, los equipos portátiles, los servidores o las impresoras. Una identidad de dispositivo proporciona a los administradores información que pueden usar al tomar decisiones de acceso o configuración. Hay varias formas de configurar las identidades de dispositivo en Azure AD.

- **Dispositivos registrados en Azure AD**. El objetivo de los dispositivos registrados en Azure AD es proporcionar a los usuarios la compatibilidad con escenarios Bring Your Own Device (BYOD) o de dispositivos móviles. En estos escenarios, el usuario puede acceder a los recursos de la organización con un dispositivo personal. Los dispositivos registrados en

Azure AD se registran sin necesidad de que una cuenta de la organización inicie sesión en el dispositivo. Los sistemas operativos compatibles con los dispositivos registrados de Azure AD incluyen Windows 10 y versiones posteriores, iOS, Android y macOS.

- **Unido a Azure AD**. Un dispositivo unido a Azure AD es el que se une mediante una cuenta de la organización, que luego se usa para iniciar sesión en el dispositivo. Los dispositivos unidos a Azure AD suelen ser propiedad de la organización. Los sistemas operativos compatibles con dispositivos unidos a Azure AD incluyen Windows 10 o versiones posteriores (excepto Home Edition) y máquinas virtuales con Windows Server 2019 que se ejecutan en Azure.
- **Dispositivos unidos a Azure AD híbrido**. Las organizaciones con implementaciones locales de Active Directory existentes se pueden beneficiar de algunas de las funcionalidades proporcionadas por Azure AD mediante la implementación de dispositivos unidos a Azure AD híbrido. Estos dispositivos están unidos a la instancia local de Active Directory y Azure AD exige que la cuenta de la organización inicie sesión en el dispositivo.

El registro y la unión de dispositivos a Azure AD proporciona a los usuarios el inicio de sesión único (SSO) a los recursos en la nube. Además, los dispositivos que están unidos a Azure AD se benefician de la experiencia de inicio de sesión único en los recursos y aplicaciones que dependen de la instancia de Active Directory local.

Los administradores de TI pueden usar herramientas como Microsoft Intune, un servicio basado en la nube que se centra en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM), para controlar cómo se usan los dispositivos de una organización. Consulte Microsoft Intune para obtener más información.

Descripción de los tipos de identidades externas

Hoy en día el mundo se mueve gracias a la colaboración y al trabajo con personas tanto dentro como fuera de su organización. Esto significa que a veces necesitará proporcionar acceso a las aplicaciones o a los datos de su organización a usuarios externos.

Azure AD External Identities es un conjunto de capacidades que permiten a las organizaciones permitir el acceso a usuarios externos, como clientes o asociados. Los clientes, asociados y otros usuarios invitados pueden "traer sus propias identidades" para iniciar sesión.

Esta capacidad para los usuarios externos se habilita a través de la compatibilidad de Azure AD con proveedores de identidades externos como otros inquilinos de Azure AD, Facebook, Google o proveedores de identidades de empresa. Los administradores pueden configurar la federación con proveedores de identidades para que los usuarios externos puedan iniciar sesión con sus cuentas empresariales o sociales existentes, en lugar de crear una nueva cuenta solo para la aplicación.

Existen dos identidades externas de Azure AD External Identities: B2B y B2C.

- La colaboración B2B le permite compartir sus aplicaciones y recursos con usuarios externos.

- En cambio, B2C es una solución de administración de identidades para aplicaciones de consumidor que están orientadas al cliente.

Colaboración B2B

La colaboración B2B le permite compartir las aplicaciones y los servicios de la organización con usuarios invitados de otras organizaciones, a la vez que mantiene el control sobre sus propios datos. La colaboración B2B usa un proceso de invitación y canje. También puede habilitar los flujos de usuario de registro de autoservicio para permitir que los usuarios externos se suscriban a aplicaciones o recursos por sí mismos. Una vez que el usuario externo ha canjeado su invitación o ha completado el registro, se representa en el mismo directorio que los empleados, pero con un tipo de usuario de invitado. Como invitado, ahora puede acceder a los recursos con sus credenciales.

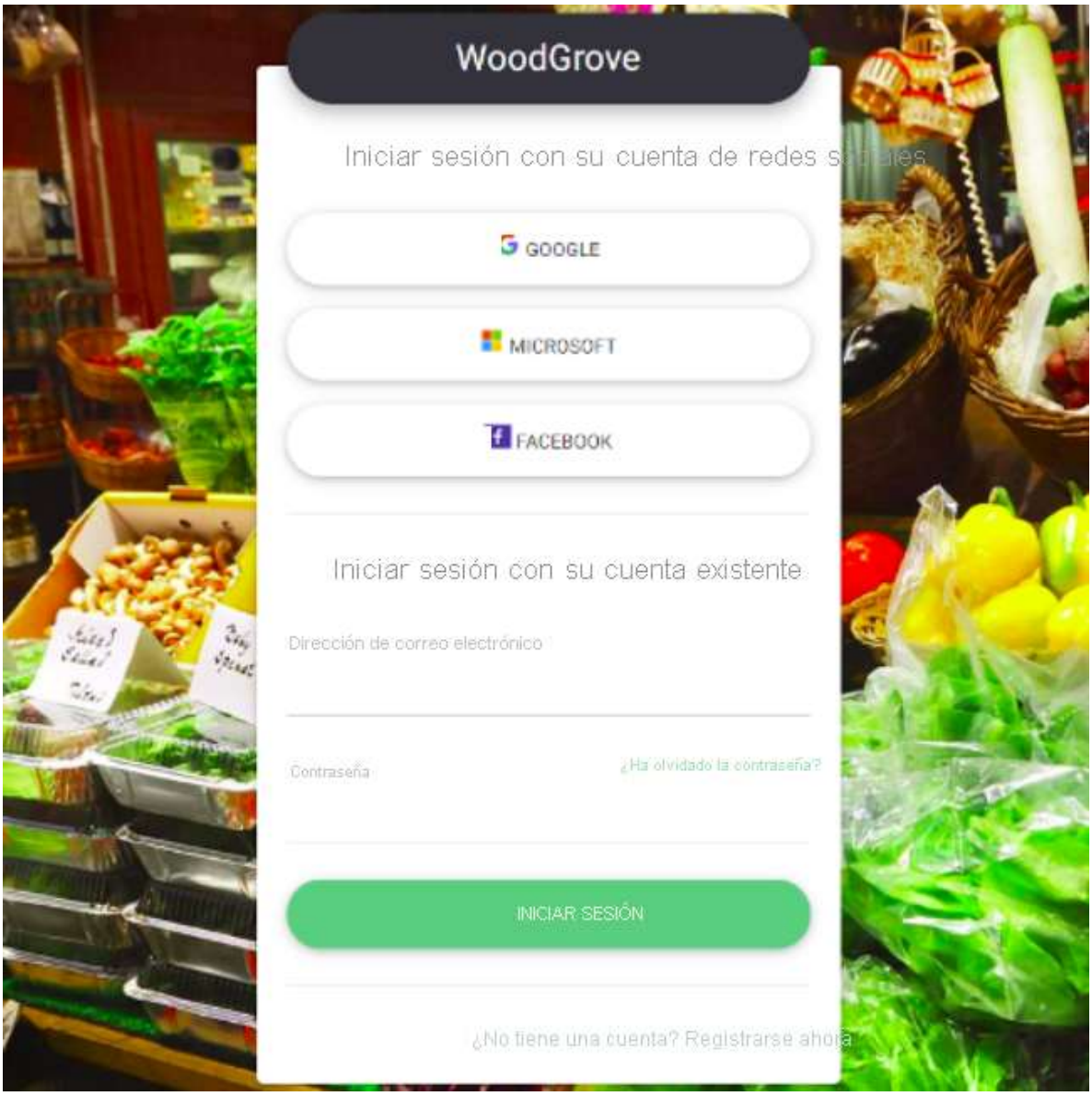
Los usuarios invitados pueden administrarse de la misma manera que los empleados, se pueden agregar a los mismos grupos, etc. Con B2B, se admite el inicio de sesión único en todas las aplicaciones conectadas a Azure AD.

Administración de acceso de B2C

Azure AD B2C es una solución de administración de acceso de identidades de cliente (CIAM). Azure AD B2C permite a los usuarios externos iniciar sesión con sus identidades de cuenta de redes sociales, de empresa o locales preferidas, para obtener un inicio de sesión único en las aplicaciones. Azure AD B2C admite millones de usuarios y miles de millones de autenticaciones al día. Asimismo, se encarga del escalado y la seguridad de la plataforma de autenticación, de la supervisión y del control automático de amenazas, como la denegación del servicio, la difusión de contraseñas o los ataques por fuerza bruta.

Gracias a Azure AD B2C, los usuarios externos se administran en el directorio de Azure AD B2C, de forma independiente del directorio de asociados y empleados de la organización. Igualmente, se admite el inicio de sesión único para aplicaciones que sean propiedad de los clientes dentro del inquilino de Azure AD B2C.

Azure AD B2C es una solución de autenticación que puede personalizar con su marca para que se fusione con sus aplicaciones web y móviles.



Azure AD External Identities es una característica de las ediciones de Azure AD Premium P1 y P2, y los precios se basan en función de los usuarios activos mensuales. Para obtener más información, consulte Precios de Azure AD

Descripción del concepto de identidad híbrida

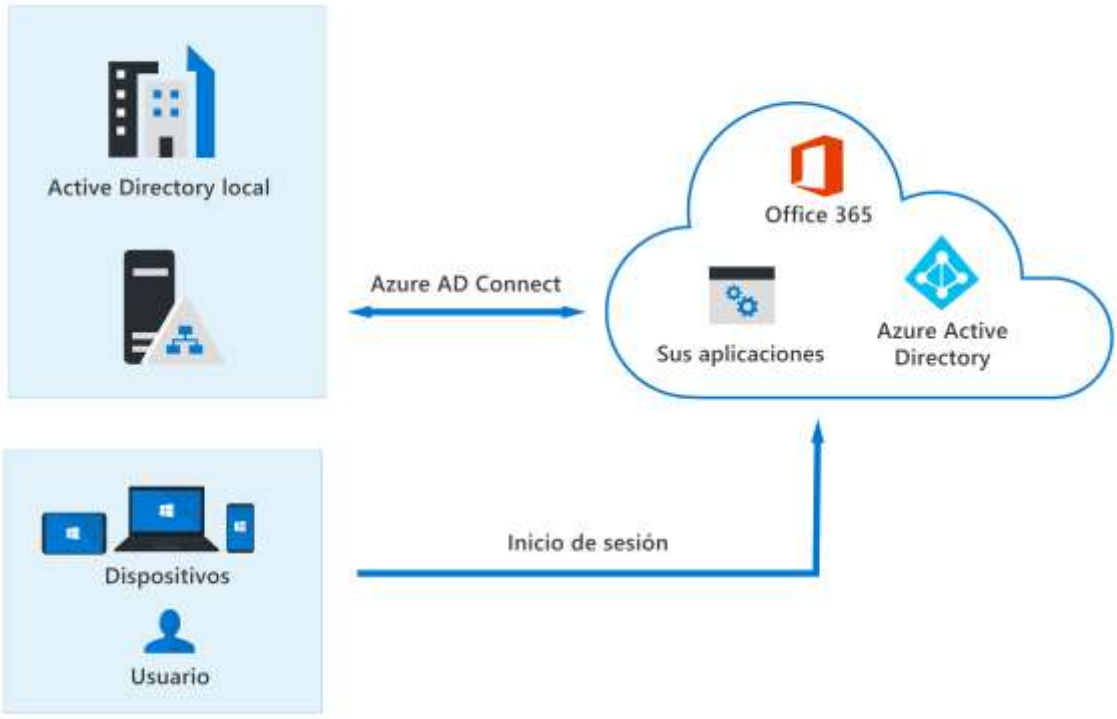
Muchas organizaciones son una combinación de aplicaciones locales y en la nube. Independientemente de si una aplicación está hospedada en el entorno local o en la nube, los usuarios esperan y exigen un acceso sencillo. Las soluciones de identidad de Microsoft abarcan funcionalidades locales y basadas en la nube. Estas soluciones crean una identidad de usuario común para la autenticación y autorización en todos los recursos, independientemente de la ubicación. A esto lo llamamos **identidad híbrida**.

Una consideración importante para las organizaciones que operan en un entorno mixto en la nube y local (modelo híbrido) consiste en determinar el método de autenticación adecuado para su

solución de Azure AD. Es una decisión importante en el recorrido de una organización a la nube y sobre cómo los usuarios iniciarán sesión y accederán a las aplicaciones. Es la base de la infraestructura de TI moderna de la organización sobre la que las organizaciones crearán su solución de seguridad, identidad y administración de acceso mediante Azure AD. Por último, una vez que se establece un método de autenticación, resulta más difícil de cambiar porque puede interrumpir la experiencia de inicio de sesión de los usuarios. En lo que respecta a la autenticación de identidades híbridas, Microsoft ofrece varias maneras de autenticarse.

- Sincronización de hash de contraseña de Azure AD.
- Autenticación transferida de Azure AD
- Autenticación federada

Estas opciones de autenticación híbrida, descritas a continuación, necesitan una instancia local de Active Directory. Además, se necesita Azure AD Connect, una aplicación de Microsoft local que se ejecuta en un servidor y actúa como puente entre Azure AD y la instancia local de Active Directory.

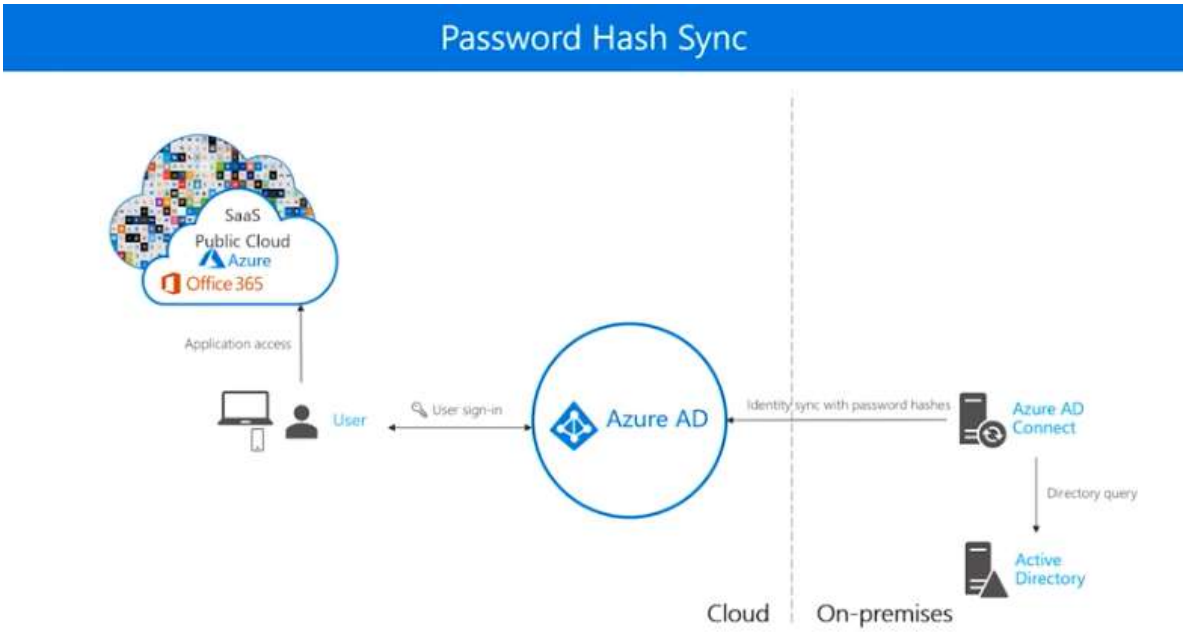


Sincronización de hash de contraseña de Azure AD. La sincronización de hash de contraseña de Azure AD es la manera más sencilla de habilitar la autenticación para los objetos de directorio local en Azure AD. Los usuarios pueden iniciar sesión en los servicios de Azure AD con el mismo nombre de usuario y la misma contraseña que usan para hacerlo en su instancia local de Active Directory. Azure AD controla el proceso de inicio de sesión de los usuarios.

El servicio de dominio de Active Directory (AD DS) almacena contraseñas en forma de representación de valor de hash de la contraseña de usuario real. Con la sincronización de hash de

contraseñas de Azure AD, el hash de contraseña se extrae de la instancia local de Active Directory mediante Azure AD Connect. Se aplica seguridad adicional al hash de contraseña y, después, se sincroniza con el servicio de autenticación de Azure Active Directory. Cuando un usuario intenta iniciar sesión en Azure AD y escribe su contraseña, la contraseña se ejecuta con el mismo algoritmo de hash y seguridad adicional que se ha aplicado a la versión almacenada en Azure AD, como parte de la sincronización. Si el resultado coincide con el valor de hash almacenado en Azure AD, el usuario ha escrito la contraseña correcta y se autentica.

Con la sincronización de hash de contraseña, Azure AD Connect garantiza que el hash de contraseña se sincronice entre la instancia local de Active Directory y Azure AD. Esto permite que la autenticación del usuario se realice en Azure AD, y no en la propia instancia de Active Directory de la organización. Una ventaja de este enfoque es que la sincronización de hash de contraseña proporciona autenticación en la nube de alta disponibilidad. Los usuarios locales pueden autenticarse con Azure AD para acceder a aplicaciones basadas en la nube, incluso si la instancia local de Active Directory deja de funcionar.

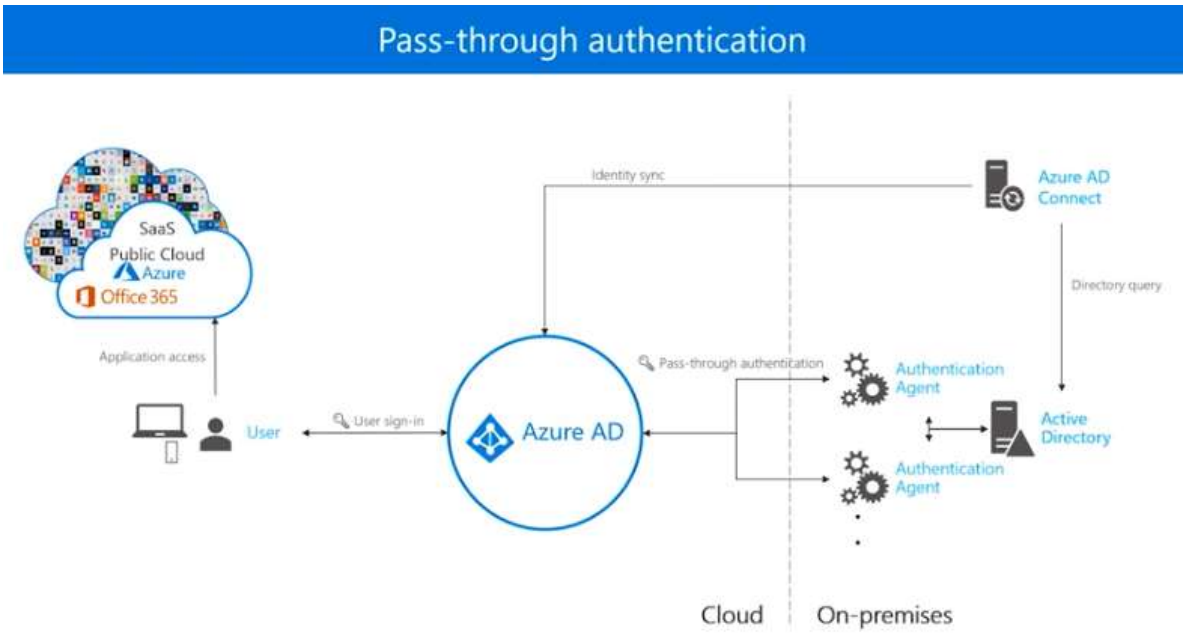


Autenticación de paso a través de Azure AD. La autenticación transferida de Azure AD permite a los usuarios iniciar sesión en aplicaciones locales y basadas en la nube con las mismas contraseñas, como la sincronización de hash de contraseña. Pero una diferencia clave es que cuando los usuarios inician sesión con la autenticación transferida de Azure AD, las contraseñas se validan directamente en la instancia local de Active Directory. La validación de las contraseñas no se produce en la nube. Esto puede ser un factor importante para las organizaciones que quieran aplicar sus directivas de seguridad y contraseñas de Active Directory locales.

La autenticación transferida de Azure AD también usa Azure AD Connect, pero tiene el requisito adicional de ejecutar uno o varios agentes de autenticación. Estos agentes actúan como intermediario entre Azure AD y la instancia local de Active Directory en el proceso de autenticación de los usuarios.

Cuando un usuario intenta acceder a una aplicación en la que todavía no ha iniciado sesión, se le redirigirá a la página de inicio de sesión de Azure AD para que escriba su nombre de usuario y contraseña. Azure AD cifrará la contraseña de usuario con la clave pública del Agente de autenticación. El Agente de autenticación local recupera el nombre de usuario y la contraseña cifrada de Azure AD, descifra la contraseña con su clave privada y valida el nombre de usuario y la contraseña en Active Directory. Active Directory evalúa la solicitud y proporciona una respuesta (correcto, error, contraseña expirada o usuario bloqueado) al agente, que luego se lo notifica a Azure AD. Si la respuesta indica que el proceso se ha realizado correctamente, Azure AD responderá con la autenticación del usuario.

El uso de agentes de autenticación que se ejecutan en un servidor significa que se necesita una superficie de infraestructura mayor, en comparación con la sincronización de hash de contraseña. Además, como la autenticación transferida se valida en la instancia local de Active Directory con dependencia de agentes de autenticación que se ejecutan en servidores, se debe tener en cuenta el software distribuido, redundante y el hardware para proporcionar solicitudes de inicio de sesión de alta disponibilidad. De lo contrario, si el centro de datos sufre una interrupción, la autenticación en los servicios de Microsoft 365 ya no sería posible.



Autenticación federada. La federación se recomienda como autenticación para las organizaciones que tienen características avanzadas que no se admiten actualmente en Azure AD, incluido el inicio de sesión con tarjetas inteligentes o certificados, con un servidor local de autenticación multifactor (MFA) o mediante una solución de autenticación de terceros.

En la autenticación federada, Azure AD delega el proceso de autenticación a un sistema independiente de autenticación de confianza como, por ejemplo, una instancia local de Servicios de federación de Active Directory (AD FS), para validar la contraseña del usuario. Este método de inicio de sesión garantiza que toda la autenticación de usuarios tiene lugar de forma local.

La autenticación federada usa Azure AD Connect, pero también necesita servidores adicionales para admitir la federación, lo que da lugar a una superficie de infraestructura mayor.

Las organizaciones que deciden usar la federación con Servicios de federación de Active Directory (AD FS) tienen la posibilidad de configurar la sincronización de hash de contraseña como copia de seguridad en caso de error en la infraestructura de AD FS.