¿Qué es Azure Active Directory?

Azure Active Directory (Azure AD) es el directorio y el servicio de administración de identidades de múltiples inquilinos de Microsoft. Azure AD combina servicios de directorio central, gobierno avanzado de identidad y administración de acceso a la aplicación. Azure AD también ofrece una plataforma enriquecida basada en estándares que permite a los desarrolladores entregar control de acceso a sus aplicaciones, basado en políticas y reglas centralizadas.

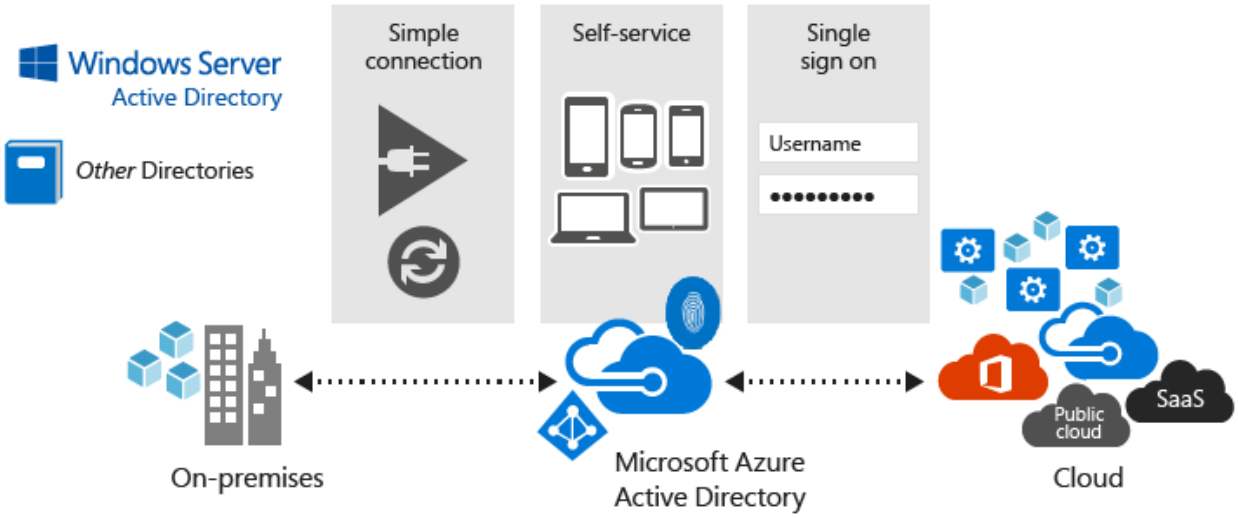
Para los administradores de TI, Azure AD ofrece una solución asequible y fácil de usar para brindar a los empleados y socios de negocios acceso de inicio de sesión único (SSO) a miles de aplicaciones SaaS en la nube como Office365, Salesforce.com, DropBox y Concur.

Para los desarrolladores de aplicaciones, Azure AD le permite concentrarse en crear su aplicación al hacerla rápida y sencilla de integrar con una solución de gestión de identidad de clase mundial utilizada por millones de organizaciones de todo el mundo.

Azure AD también incluye un conjunto completo de capacidades de administración de identidades que incluyen autenticación de múltiples factores, registro de dispositivos, administración de contraseñas de autoservicio, administración de grupos de autoservicio, administración de cuentas privilegiadas, control de acceso basado en roles, monitoreo de uso de aplicaciones, auditoría enriquecida y monitoreo de seguridad y alertando Estas capacidades pueden ayudar a proteger las aplicaciones basadas en la nube, agilizar los procesos de TI, reducir los costos y ayudar a garantizar que se cumplan los objetivos de cumplimiento corporativo.

Además, con solo cuatro clics , Azure AD se puede integrar con un Directorio Activo de Windows Server existente, brindando a las organizaciones la capacidad de aprovechar sus inversiones existentes en identidades locales para administrar el acceso a aplicaciones SaaS basadas en la nube.

Si es cliente de Office 365, Azure o Dynamics CRM Online, es posible que no se dé cuenta de que ya está utilizando Azure AD. Todos los inquilinos de Office 365, Azure y Dynamics CRM ya son inquilinos de Azure AD. Siempre que lo desee, puede comenzar a usar ese inquilino para administrar el acceso a miles de otras aplicaciones en la nube con las que Azure AD se integra.1



¿Qué tan confiable es Azure AD?

El diseño de Azure AD de múltiples inquilinos, distribuido geográficamente y de alta disponibilidad, significa que puede confiar en él para sus necesidades comerciales más críticas. Al quedarse sin 28 centros de datos en todo el mundo con failover automatizado, tendrá la tranquilidad de saber que Azure AD es altamente confiable y que incluso si un centro de datos deja de funcionar, las copias de sus datos de directorio se publicarán en al menos dos más a nivel regional. centros de datos dispersos y disponibles para acceso instantáneo.

Para más detalles, vea Acuerdos de nivel de servicio .

Elige una edición

Todos los servicios comerciales de Microsoft Online se basan en Azure Active Directory (Azure AD) para iniciar sesión y otras necesidades de identidad. Si se suscribe a cualquiera de los servicios comerciales de Microsoft Online (por ejemplo, Office 365 o Microsoft Azure), obtiene Azure AD con acceso a todas las funciones gratuitas. Con la edición gratuita de Azure Active Directory, puede administrar usuarios y grupos, sincronizar con directorios locales, obtener un inicio de sesión único en Azure, Office 365 y miles de aplicaciones populares de SaaS como Salesforce, Workday, Concur, DocuSign, Google Apps , Box, ServiceNow, Dropbox y más.

Para mejorar su Azure Active Directory, puede agregar capacidades pagas utilizando las ediciones Azure Active Directory Basic, Premium P1 y Premium

P2. Las versiones pagas de Azure Active Directory se crean sobre su directorio gratuito existente, proporcionando capacidades de clase empresarial que abarcan autoservicio, monitoreo mejorado, informes de seguridad, autenticación multifactor (MFA) y acceso seguro para su fuerza de trabajo móvil.

Nota

Para ver las opciones de precios de estas ediciones, consulte los precios de **Azure Active Directory** . Azure Active Directory Premium P1, Premium P2 y Azure Active Directory Basic actualmente no son compatibles con China. Póngase en contacto con nosotros en el foro de Azure Active Directory para obtener más información.

- **Azure Active Directory Basic** : diseñada para trabajadores con necesidades de nube, esta edición brinda acceso a aplicaciones centradas en la nube y soluciones de administración de identidad de autoservicio. Con la edición básica de Azure Active Directory, obtiene características que mejoran la productividad y la reducción de costos, como administración de acceso basado en grupos, restablecimiento de contraseña de autoservicio para aplicaciones en la nube y proxy de aplicación de Active Directory de Azure (para publicar aplicaciones web locales utilizando Azure Active Directorio), todo respaldado por un SLA de nivel empresarial de 99.9 por ciento de tiempo de actividad.
- **Azure Active Directory Premium P1**- Diseñada para empoderar a las organizaciones con necesidades de gestión de acceso e identidad más exigentes, la edición Azure Active Directory Premium agrega funciones de administración de identidad a nivel empresarial con numerosas funciones y permite a los usuarios híbridos acceder sin problemas a las capacidades locales y en la nube. Esta edición incluye todo lo que necesita para administradores de identidad y trabajadores de la información en entornos híbridos para el acceso a aplicaciones, identidad de autoservicio y administración de acceso (IAM), protección de identidad y seguridad en la nube. Admite recursos avanzados de administración y delegación, como grupos dinámicos y administración de grupos de autoservicio. Incluye Microsoft Identity Manager (una suite de administración de identidades y accesos local) y brinda capacidades de escritura en la nube que permiten soluciones como el restablecimiento de contraseñas de autoservicio para sus usuarios locales.
- **Azure Active Directory Premium P2** : diseñada con una protección avanzada para todos sus usuarios y administradores, esta nueva oferta incluye todas las capacidades de Azure AD Premium P1, así como nuestra nueva protección de identidad y administración de identidad privilegiada. Azure Active Directory Identity Protection aprovecha miles de millones de señales

para proporcionar acceso condicional basado en el riesgo a sus aplicaciones y datos críticos de la compañía. También lo ayudamos a administrar y proteger cuentas privilegiadas con Azure Active Directory Privileged Identity Management para que pueda descubrir, restringir y monitorear a los administradores y su acceso a los recursos y proporcionar acceso justo a tiempo cuando sea necesario.

1

Nota

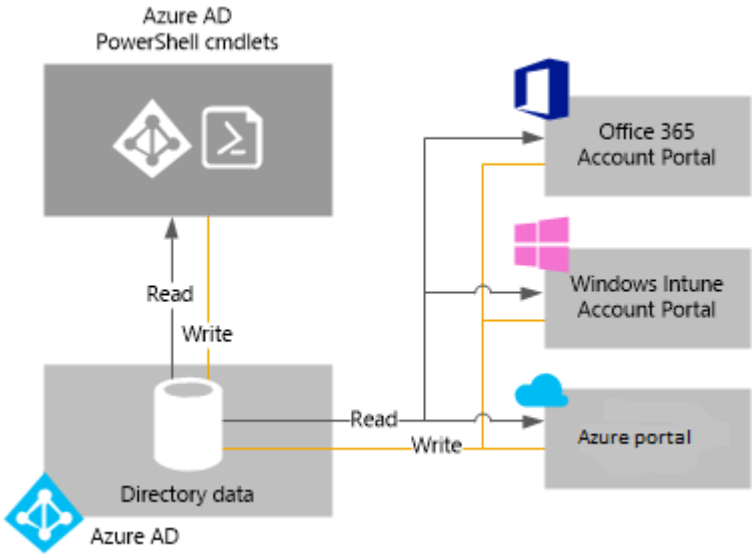
Varias capacidades de Azure Active Directory están disponibles a través de las ediciones de "pago por uso":

- Active Directory B2C es la solución de gestión de identidad y acceso para sus aplicaciones orientadas al consumidor. Para obtener más detalles, consulte Azure Active Directory B2C
- La Autenticación de múltiples factores de Azure se puede usar por usuario o por proveedores de autenticación. Para obtener más detalles, consulte ¿Qué es la Autenticación de múltiples factores de Azure?

Administre su directorio de Azure AD

¿Qué es un inquilino de Azure AD?

En Azure Active Directory (Azure AD), un inquilino es una instancia dedicada de un directorio de Azure AD que su organización recibe cuando se registra en un servicio en la nube de Microsoft, como Azure u Office 365. Cada directorio de Azure AD es distinto y está separado del resto Directorios de Azure AD. Al igual que un edificio de oficinas corporativas es un activo seguro específico solo para su organización, un directorio de Azure AD también se diseñó para ser un activo seguro para uso exclusivo de su organización. La arquitectura de Azure AD aísla los datos del cliente y la información de identidad para que los usuarios y administradores de un directorio de Azure AD no puedan acceder accidental o maliciosamente a los datos en otro directorio.



¿Cómo puedo obtener un directorio de Azure AD?

Azure AD proporciona el directorio central y las capacidades de administración de identidades detrás de la mayoría de los servicios en la nube de Microsoft, que incluyen:

- Azure
- Microsoft Office 365
- Microsoft Dynamics CRM en línea
- Microsoft Intune

Obtiene un directorio Azure AD cuando se registra para cualquiera de estos servicios en la nube de Microsoft. Puede crear directorios adicionales según sea necesario. Por ejemplo, puede mantener su primer directorio como un directorio de producción y luego crear otro directorio para pruebas o etapas.

Usar el directorio de Azure AD que viene con una nueva suscripción de Azure

Le recomendamos que use la cuenta de administrador que usó para su primer servicio cuando se registra para otros servicios de Microsoft. La información que proporciona la primera vez que se registra para obtener un servicio de Microsoft se usa para crear una nueva instancia de directorio de Azure AD para su organización. Si usa ese directorio para autenticar los intentos de inicio de sesión cuando se suscribe a otros servicios de Microsoft, puede usar las cuentas de usuario, las políticas, las configuraciones o la integración de directorios locales que configure en su directorio predeterminado.

Por ejemplo, si se registra para una suscripción a Microsoft Intune y luego sincroniza su Active Directory local con su directorio de Azure AD, puede suscribirse a otro servicio de Microsoft como Office 365 y obtener fácilmente los mismos beneficios de integración de directorios que usted. tener con Microsoft Intune.

Para obtener más información sobre la integración de su directorio local con Azure AD, consulte la integración de directorios con Azure AD Connect .

Asociar un directorio de Azure AD existente con una nueva suscripción de Azure

Puede asociar una nueva suscripción de Azure con el mismo directorio que autentica el inicio de sesión de una suscripción existente de Office 365 o Microsoft Intune. Para obtener más información sobre ese escenario, consulte Transferir la propiedad de una suscripción de Azure a otra cuenta.

Cree un directorio de Azure AD registrándose en un servicio de nube de Microsoft como organización

Si aún no tiene una suscripción a un servicio en la nube de Microsoft, puede usar uno de los siguientes enlaces para registrarse. Al registrarse para su primer servicio, se crea un directorio de Azure AD automáticamente.

- Microsoft Azure
- Oficina 365
- Microsoft Intune

Cómo cambiar el directorio predeterminado para una suscripción

1. Inicie sesión en el Centro de cuentas de Azure con una cuenta que sea el administrador de la cuenta de la suscripción para transferir la propiedad de la suscripción.
2. Asegúrese de que el usuario que desea ser el propietario de la suscripción se encuentre en el directorio de destino.
3. Haga clic en **Transferir suscripción** .
4. Especifique el destinatario. El destinatario recibe automáticamente un correo electrónico con un enlace de aceptación.
5. El destinatario hace clic en el enlace y sigue las instrucciones, incluida la introducción de su información de pago. Cuando el destinatario tiene éxito, la suscripción se transfiere.

6. El directorio predeterminado de la suscripción se cambia al directorio en el que se encuentra el usuario si la transferencia de propiedad de la suscripción se realiza correctamente.

Para obtener más información, consulte Transferir propiedad de suscripción Azure a otra cuenta

Administrar el directorio predeterminado en Azure

Cuando se registra en Azure, se asocia un directorio predeterminado de Azure AD con su suscripción. No hay costos por usar Azure AD y sus directorios son un recurso gratuito. Existen servicios pagados de Azure AD que tienen licencia por separado y ofrecen funcionalidades adicionales, como la marca de la empresa al iniciar sesión y el restablecimiento de contraseña de autoservicio. También puede crear un dominio personalizado utilizando un nombre DNS que posea en lugar del dominio predeterminado * .onmicrosoft.com.

¿Cómo puedo administrar los datos del directorio?

Para administrar una o más suscripciones de servicios en la nube de Microsoft, puede usar el centro de administración de Azure AD , el portal de la cuenta de Microsoft Intune o el Centro de administración de Office 365 para administrar los datos de directorio de su organización. También puede usar los cmdlets de Azure Active Directory PowerShell para ayudarlo a administrar los datos almacenados en Azure AD.

Desde cualquiera de estos portales (o cmdlets), puede:

- Crear y administrar cuentas de usuarios y grupos
- Administre los servicios en la nube relacionados para las suscripciones de su organización
- Configurar la integración local con los servicios de identidad y autenticación de Azure AD

1

El centro de administración de Azure AD, el Centro de administración de Office 365, el portal de cuenta de Microsoft Intune y los cmdlets de Azure AD leen y escriben en una sola instancia compartida de Azure AD que está asociada con el directorio de su organización. Cada una de esas herramientas actúa como una

interfaz de front-end que capta o cambia los datos de su directorio. Cuando cambia los datos de su organización utilizando cualquiera de los portales o cmdlets mientras está conectado en el contexto de uno de estos servicios, los cambios también se muestran en los otros portales la próxima vez que inicie sesión. Estos datos se comparten en los servicios en la nube de Microsoft. a lo que te suscribes

Por ejemplo, si utiliza el Centro de administración de Office 365 para impedir que un usuario inicie sesión, esa acción impide que el usuario inicie sesión en cualquier otro servicio al que su organización esté suscripta actualmente. Si ve la misma cuenta de usuario en el portal de la cuenta de Microsoft Intune, también verá que el usuario está bloqueado.

¿Cómo puedo agregar y administrar múltiples directorios?

Puede agregar un directorio de Azure AD en Azure Portal . Complete la información y seleccione **Crear** .

Puede gestionar cada directorio como un recurso completamente independiente: cada directorio es un compañero, con todas las funciones y lógicamente independiente de otros directorios que usted administra; no hay una relación padre-hijo entre directorios. Esta independencia entre directorios incluye independencia de recursos, independencia administrativa e independencia de sincronización.

- **La independencia de los recursos** . Si crea o elimina un recurso en un directorio, no tiene ningún impacto en ningún recurso en otro directorio, con la excepción parcial de usuarios externos. Si usa un dominio personalizado 'contoso.com' con un directorio, no se puede usar con ningún otro directorio.
- **Independencia administrativa** . Si un usuario que no es administrador del directorio 'Contoso' crea un directorio de prueba 'Prueba', entonces:
    - Los administradores del directorio 'Contoso' no tienen privilegios administrativos directos en el directorio 'Prueba', a menos que un administrador de 'Prueba' les conceda específicamente estos privilegios. Los administradores de 'Contoso' pueden controlar el acceso al directorio 'Prueba' en virtud de su control de la cuenta de usuario que creó 'Prueba'.
    - Si asigna o quita una función de administrador para un usuario en un directorio, el cambio no afecta ninguna función de administrador que el usuario pueda tener en otro directorio.

- **Independencia de sincronización** . Puede configurar cada inquilino de Azure AD de forma independiente para obtener datos sincronizados de una sola instancia, la herramienta de sincronización de directorios de Azure AD Connect.

A diferencia de otros recursos de Azure, sus directorios no son recursos secundarios de una suscripción de Azure. Por lo tanto, si cancela o permite que expire su suscripción a Azure, aún puede acceder a los datos de su directorio mediante Azure AD PowerShell, la API de Azure Graph u otras interfaces, como el Centro de administración de Office 365. También puede asociar otra suscripción con el directorio.

Cómo prepararse para eliminar un directorio de Azure AD

Un administrador global puede eliminar un directorio de Azure AD del portal. Cuando se elimina un directorio, todos los recursos que están contenidos en el directorio también se eliminan. Verifique que no necesita el directorio antes de eliminarlo.

Nota

Si el usuario inició sesión con una cuenta de trabajo o escuela, el usuario no debe intentar borrar su directorio de inicio. Por ejemplo, si el usuario inició sesión como joe@contoso.onmicrosoft.com, ese usuario no puede eliminar el directorio que tiene contoso.onmicrosoft.com como su dominio predeterminado.

Azure AD requiere que se cumplan ciertas condiciones para eliminar un directorio. Esto reduce el riesgo de que la eliminación de un directorio afecte negativamente a usuarios o aplicaciones, como la capacidad de los usuarios para iniciar sesión en Office 365 o acceder a recursos en Azure. Por ejemplo, si un directorio para una suscripción se elimina involuntariamente, los usuarios no pueden acceder a los recursos de Azure para esa suscripción.

Las siguientes condiciones están marcadas:

- El único usuario en el directorio debe ser el administrador global que debe eliminar el directorio. Cualquier otro usuario debe ser eliminado antes de que el directorio pueda ser eliminado. Si los usuarios están sincronizados desde el sitio, entonces la sincronización debe estar desactivada y los usuarios deben eliminarse en el directorio de la nube mediante Azure Portal o los cmdlets de Azure PowerShell. No es necesario eliminar grupos o contactos, como los contactos agregados desde el Centro de administración de Office 365.

- No puede haber aplicaciones en el directorio. Cualquier aplicación debe ser eliminada antes de que el directorio pueda ser eliminado.
- No se pueden vincular proveedores de autenticación de múltiples factores al directorio.
- No puede haber suscripciones para ningún servicio en línea de Microsoft como Microsoft Azure, Office 365 o Azure AD Premium asociado con el directorio. Por ejemplo, si se creó un directorio predeterminado para usted en Azure, no puede eliminar este directorio si su suscripción a Azure todavía se basa en este directorio para la autenticación. Del mismo modo, no puede eliminar un directorio si otro usuario ha asociado una suscripción con él.

¿Qué es el registro de autoservicio para Azure Active Directory?

11/03/2017

2 minutos para leer

Colaboradores

Este artículo explica el registro de autoservicio y cómo admitirlo en Azure Active Directory (Azure AD). Si desea tomar el control de un nombre de dominio de un inquilino de Azure AD no administrado, consulte Asumir un directorio no administrado como administrador .

¿Por qué usar el registro de autoservicio?

Obtenga clientes a los servicios que desean más rápido

Crear ofertas basadas en correo electrónico para un servicio

Cree flujos de suscripción basados en correo electrónico que permitan a los usuarios crear identidades rápidamente utilizando sus alias de correo electrónico de trabajo fáciles de recordar

Un directorio de Azure AD creado por el autoservicio se puede convertir en un directorio administrado que se puede usar para otros servicios

Términos y definiciones

Registro de autoservicio : este es el método mediante el cual un usuario se registra en un servicio en la nube y tiene una identidad creada automáticamente para ellos en Azure AD en función de su dominio de correo electrónico.

Directorio de Azure AD no administrado : este es el directorio donde se crea esa identidad. Un directorio no administrado es un directorio que no tiene administrador global.

Usuario verificado por correo electrónico : este es un tipo de cuenta de usuario en Azure AD. Un usuario que tiene una identidad creada automáticamente después de registrarse para una oferta de autoservicio se conoce como un usuario verificado por correo electrónico. Un usuario verificado por correo electrónico es un miembro habitual de un directorio etiquetado con creationmethod = EmailVerified.

¿Cómo controlo la configuración de autoservicio?

Los administradores tienen dos controles de autoservicio hoy. Ellos pueden controlar si:

Los usuarios pueden unirse al directorio por correo electrónico.

Los usuarios pueden licenciarse para aplicaciones y servicios.

¿Cómo puedo controlar estas capacidades?

Un administrador puede configurar estas capacidades mediante los siguientes parámetros de Azure AD cmdlet Set-MsolCompanySettings:

AllowEmailVerifiedUsers controla si un usuario puede crear o unirse a un directorio no administrado. Si establece ese parámetro en $ false, ningún usuario verificado por correo electrónico puede unirse al directorio.

AllowAdHocSubscriptions controla la capacidad de los usuarios para realizar registros de autoservicio. Si establece ese parámetro en $ false, ningún usuario puede realizar el registro de autoservicio.

¿Cómo funcionan los controles?

Estos dos parámetros se pueden usar en conjunto para definir un control más preciso sobre el registro de autoservicio. Por ejemplo, el siguiente comando permitirá a los usuarios realizar el registro de autoservicio, pero solo si esos usuarios ya tienen una cuenta en Azure AD (en otras palabras, los usuarios que necesitarían una cuenta verificada por correo electrónico para crear primero no pueden realizar auto-servicio). registro de servicio):

Dupdo

```
    Set-MsolCompanySettings -AllowEmailVerifiedUsers $false -AllowAdHocSubscriptions
$true
```

El siguiente diagrama de flujo explica las diferentes combinaciones de estos parámetros y las condiciones resultantes para el registro de directorio y autoservicio.

Para obtener más información y ejemplos de cómo usar estos parámetros, vea Set-MsolCompanySettings .