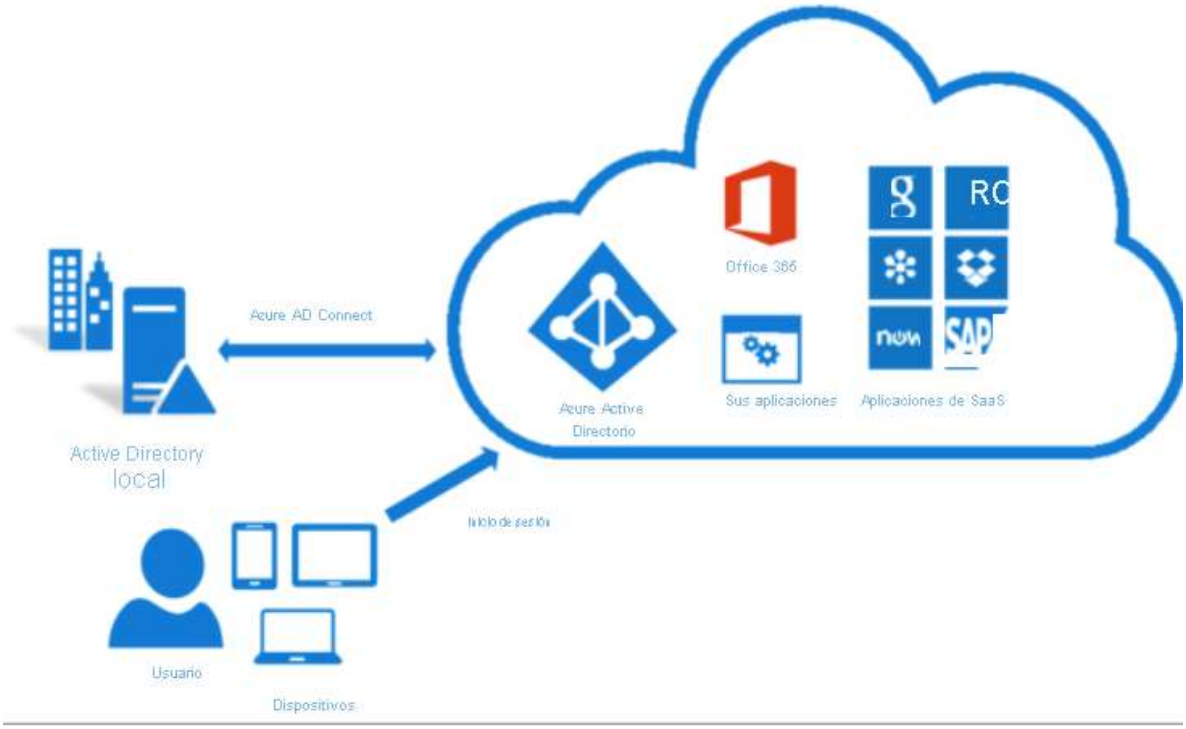
Implementación de Azure AD Connect

Azure AD Connect integrará sus directorios locales con Azure Active Directory. Esto le permite proporcionar una identidad común a los usuarios de aplicaciones de Microsoft 365, Azure y SaaS integradas con Azure AD.

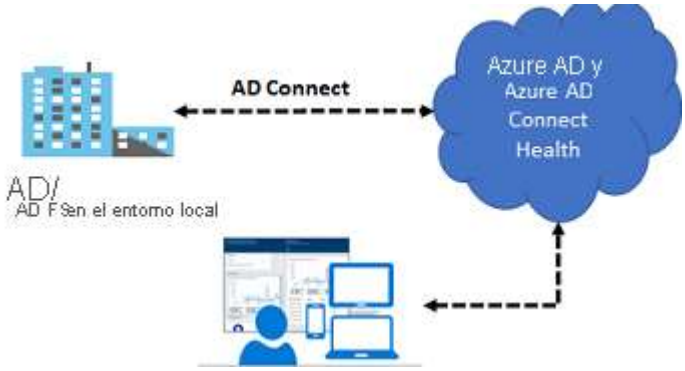


Azure AD Connect proporciona las siguientes características:

- **Sincronización de hash de contraseña**. Un método de inicio de sesión que sincroniza el hash de la contraseña de un usuario de AD local con Azure AD.
- **Autenticación de paso a través**. Un método de inicio de sesión que permite a los usuarios usar la misma contraseña en el entorno local y en la nube, pero no requiere la infraestructura adicional de un entorno federado.
- **Integración de federación**. La federación es una parte opcional de Azure AD Connect y puede utilizarse para configurar un entorno híbrido mediante una infraestructura local de AD FS. También proporciona funcionalidades de administración de AD FS, como la renovación de certificados e implementaciones de servidor de AD FS adicionales.
- **Sincronización**. Responsable de la creación de usuarios, grupos y otros objetos. También de asegurar que la información de identidad de los usuarios y los grupos de su entorno local coincide con la de la nube. Esta sincronización también incluye los códigos hash de contraseña.

- **Seguimiento de estado**. Azure AD Connect Health puede proporcionar una supervisión sólida y una ubicación central en Azure Portal para ver esta actividad.

Cuando se integran los directorios locales con Azure AD, aumenta la productividad de los usuarios, ya que hay una identidad común para acceder tanto a los recursos en la nube como a los locales. Sin embargo, esta integración crea el desafío de garantizar que este entorno es correcto, con el fin de que los usuarios puedan acceder de manera confiable a los recursos tanto a nivel local como en la nube desde cualquier dispositivo.



Azure Active Directory (Azure AD) Connect Health proporciona una sólida supervisión de la infraestructura de identidad local. Permite mantener una conexión confiable con Microsoft 365 y Microsoft Online Services. Esta confiabilidad se consigue al proporcionar funcionalidades de supervisión para los componentes de identidad clave. Además, hace que los puntos de datos clave sobre estos componentes sean fácilmente accesibles. Azure AD Connect Health le ayuda a:

- Supervisar los servidores AD FS, Azure AD Connect y los controladores de dominio de AD y obtener información sobre ellos.
- Supervisar las sincronizaciones que se producen entre las instancias de AD DS locales y Azure AD y obtener información de ellas.
- Supervisar la infraestructura de identidad local que se usa para acceder a Microsoft 365 u otras aplicaciones de Azure AD y obtener información sobre ella.

Con Azure AD Connect resulta sencillo acceder a los datos clave que necesita. Puede ver y actuar sobre alertas, configurar notificaciones por correo electrónico para alertas críticas y ver datos de rendimiento.

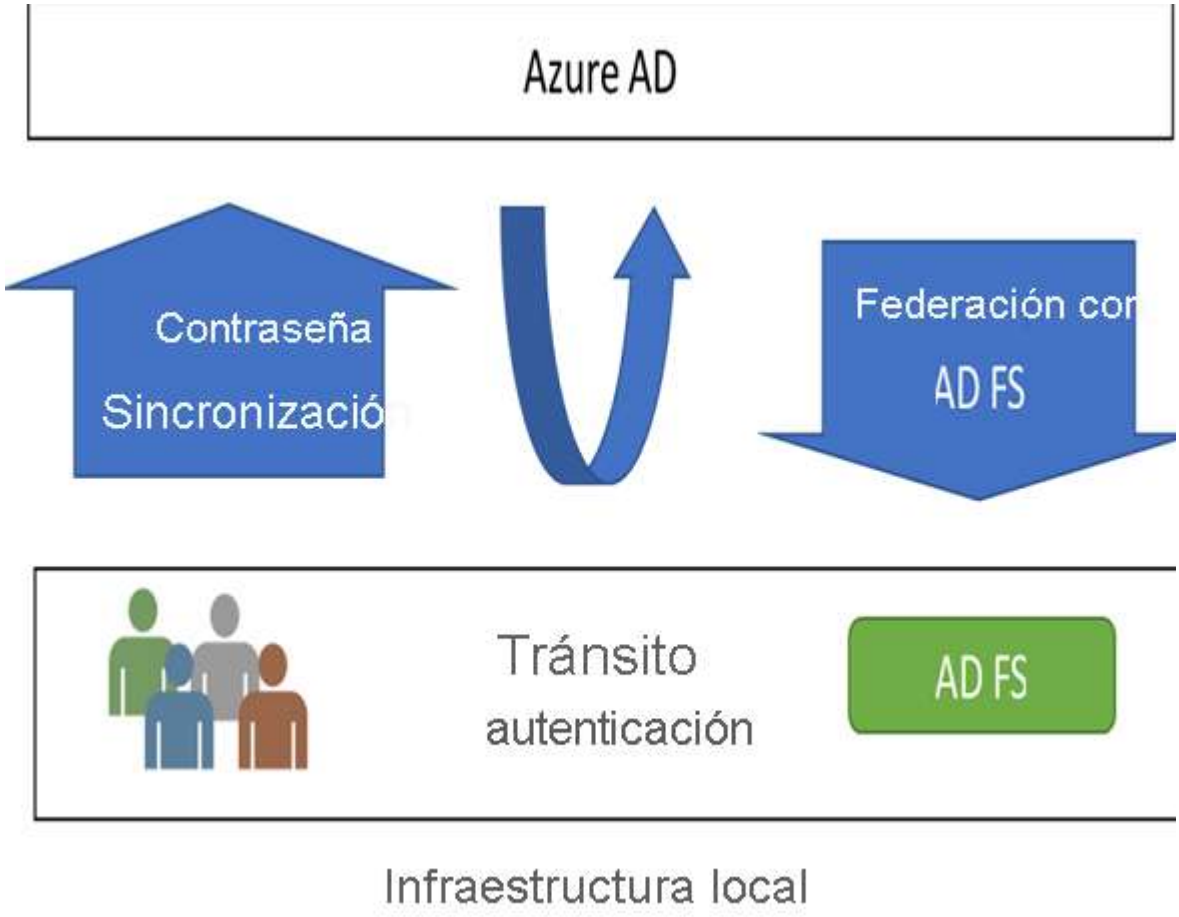
Importante

Para usar AD Connect Health, se instala un agente en cada uno de los servidores de sincronización locales.

Exploración de las opciones de autenticación

La elección de un método de autenticación de Azure AD es importante, ya que es una de las primeras decisiones importantes al trasladarse a la nube, pues será la base de su entorno en la nube y es difícil de cambiar más adelante.

Puede elegir la **autenticación en la nube**, que incluye sincronización de hash de contraseña de Azure AD y autenticación transferida de Azure AD. También puede elegir la **autenticación federada**, donde Azure AD deja el proceso de autenticación en manos de un sistema 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.



Resumen

- ¿Necesita la integración de Active Directory local? Si la respuesta es No, debe usar la autenticación solo en la nube.
- Si necesita la integración de Active Directory local, ¿necesita utilizar la autenticación en la nube y la protección con contraseña? ¿Sus requisitos de autenticación son compatibles de forma nativa con Azure AD? Si la respuesta es Sí, usaría la **sincronización de hash de contraseña + SSO de conexión directa**.
- Si necesita la integración de Active Directory local, pero no necesita utilizar la autenticación en la nube y la protección con contraseña, y sus requisitos de autenticación son compatibles de forma nativa con Azure AD, usaría **SSO de conexión directa de la autenticación transferida**.
- Si necesita la integración de Active Directory local, tiene un proveedor de federación existente y sus requisitos de autenticación NO son compatibles de forma nativa con Azure AD, entonces utilizaría la autenticación de **federación**.

Configuración de la sincronización de hash de contraseña (PHS)

Las probabilidades de que se quede bloqueado sin poder realizar su trabajo debido a una contraseña olvidada guarda relación con el número de contraseñas diferentes que tenga que recordar. Cuantas más contraseñas tenga que recordar, más probabilidades tiene de olvidar alguna. Las preguntas y llamadas para el restablecimiento de contraseñas y otros problemas relacionados con las mismas, son los temas que más recursos del departamento de soporte técnico utilizan.

La **sincronización de hash de contraseña** (PHS) es una característica que se utiliza para sincronizar las contraseñas de usuario de una instancia de Active Directory local con una instancia de Azure AD basada en la nube. Use esta característica para iniciar sesión en servicios de Azure AD como Microsoft 365, Microsoft Intune, CRM Online y Azure Active Directory Domain Services (Azure AD DS). Inicie sesión en el servicio con la misma contraseña que usa para iniciar sesión en la instancia local de Active Directory. La sincronización de hash de contraseñas lo ayuda a lo siguiente:

- Mejorar la productividad de los usuarios.
- Reducir los costos de soporte técnico.

¿Cómo funciona?

En segundo plano, el componente de sincronización de contraseñas toma el hash de contraseña del usuario de Active Directory local, lo cifra y lo pasa como una cadena a Azure. Azure descifra el hash cifrado y almacena el hash de contraseña como un atributo de usuario en Azure AD.

Cuando el usuario inicia sesión en un servicio de Azure, el cuadro de diálogo de desafío de inicio de sesión genera un hash de la contraseña del usuario y pasa ese hash a Azure. A continuación, Azure compara el hash con el de la cuenta de ese usuario. Si los dos hashes coinciden, las dos contraseñas también deben coincidir y el usuario recibe acceso al recurso. El cuadro de diálogo ofrece la posibilidad de guardar las credenciales para que la próxima vez que el usuario acceda al recurso de Azure no se le solicite.

Importante

Es importante entender que se trata de **un mismo inicio de sesión**, no de un inicio de sesión único. El usuario sigue autenticándose en dos servicios de directorio distintos, aunque con el mismo nombre de usuario y contraseña. Esta solución proporciona una alternativa sencilla a una implementación de AD FS.

Implementación de autenticación transferida (PTS)

La **autenticación transferida (PTA) de Azure AD** es una alternativa a la sincronización de hash de contraseñas de Azure AD, y proporciona la misma ventaja de la autenticación en la nube a las organizaciones. PTA permite que se pueda iniciar sesión tanto en las aplicaciones basadas en la nube como en las locales con la misma cuenta de usuario y contraseña. Cuando los usuarios inician sesión con Azure AD, la autenticación transferida valida las contraseñas de los usuarios directamente con la instancia local de Active Directory de la organización.

Ventajas de las características

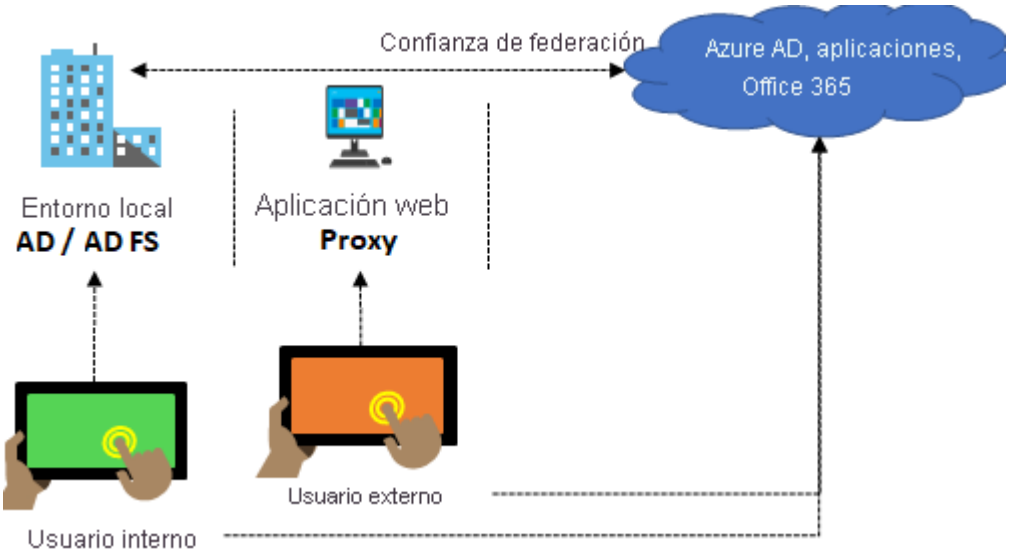
- Admite el inicio de sesión de usuario en todas las aplicaciones basadas en explorador web y en las aplicaciones cliente de Microsoft Office que usan la autenticación moderna.
- Los nombres de usuario de inicio de sesión pueden ser el nombre de usuario predeterminado local (userPrincipalName) u otro atributo configurado en Azure AD Connect (conocido como Id. alternativo).
- Funciona perfectamente con características de acceso condicional como Azure Active Directory Multi-Factor Authentication para ayudar a proteger a los usuarios.
- Se integra con la administración de contraseñas de autoservicio basada en la nube, incluida la escritura diferida de contraseñas en Active Directory local y la protección con contraseña mediante la prohibición de contraseñas usadas habitualmente.
- Se admiten entornos de varios bosques si hay relaciones de confianza de bosque entre los bosques de AD y si el enrutamiento de sufijos de nombre está configurado correctamente.
- PTA es una característica gratuita y no necesita ninguna edición de pago Azure AD para usarla.
- PTA se puede habilitar a través de Azure AD Connect.
- PTA usa un agente local ligero que escucha y responde a las solicitudes de validación de contraseñas.
- La instalación de varios agentes proporciona una alta disponibilidad de las solicitudes de inicio de sesión.
- PTA protege las cuentas locales frente a ataques de fuerza bruta a las contraseñas en la nube.

Importante

Esta característica se puede configurar sin usar un servicio de federación para que cualquier organización, independientemente del tamaño, pueda implementar una solución de identidad híbrida. La autenticación transferida no solo sirve para el inicio de sesión de usuario, sino que permite que una organización use otras características de Azure AD, como la administración de contraseñas, el control de acceso basado en rol, las aplicaciones publicadas y las directivas de acceso condicional.

Implementación de la federación con Azure AD

La federación es una colección de dominios que han establecido confianza. El nivel de confianza puede variar, pero normalmente incluye la autenticación y casi siempre la autorización. Una federación típica podría incluir un número de organizaciones que han establecido confianza para el acceso compartido a un conjunto de recursos.



Puede federar el entorno local con Azure AD y usar esta federación para la autenticación y autorización. Este método de inicio de sesión garantiza que toda la autenticación de usuarios tiene lugar de forma local. Este método permite a los administradores implementar niveles más rigurosos de control de acceso.

Importante

Si opta por usar Federación con Servicios de federación de Active Directory (AD FS), tiene la posibilidad de configurar la sincronización de hash de contraseñas como copia de seguridad en caso de error en la infraestructura de AD FS.

Exploración del árbol de decisión de autenticación

La elección del método de autenticación correcto es la primera preocupación para las organizaciones que desean mover sus aplicaciones a la nube. Esta decisión no debe tomarse a la ligera por las razones siguientes:

- Es la primera decisión de una organización que quiere trasladarse a la nube.
- El método de autenticación es un componente esencial de la presencia de una organización en la nube. Esto es debido a que controla el acceso a todos los datos y recursos que hay en ella.
- Es la base de todas las demás características avanzadas de seguridad y experiencia de usuario en Azure AD.

La identidad es el nuevo plano de control de la seguridad de TI, de modo que la autenticación se convierte en el guardián de acceso de una organización al nuevo mundo de la nube. Las organizaciones necesitan un plano de control de identidad que fortalezca su seguridad y mantenga las aplicaciones en la nube a salvo de intrusos.

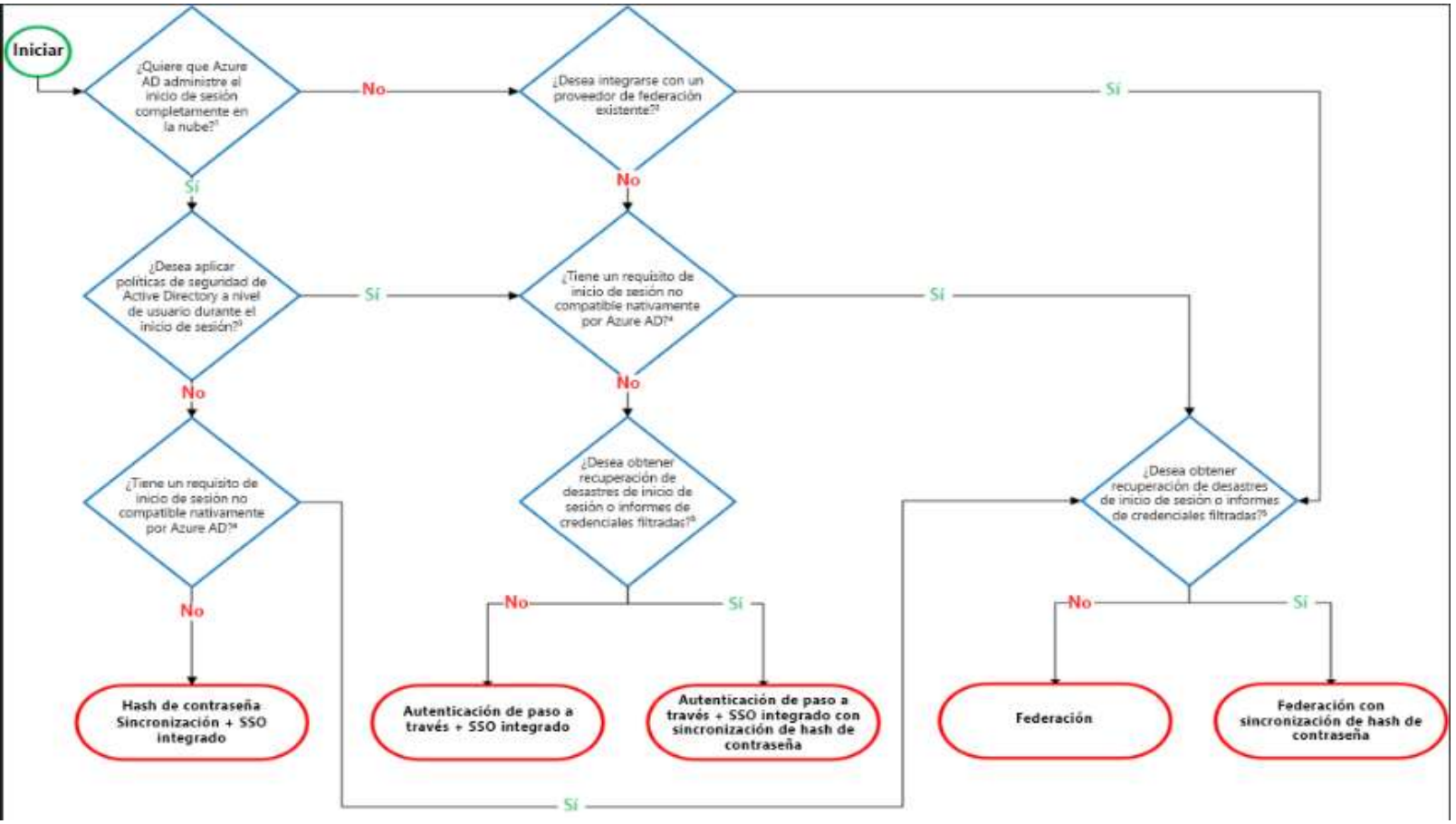
Métodos de autenticación

Autenticación en la nube: al elegir este método de autenticación, Azure AD controla el proceso de inicio de sesión de los usuarios. Junto con el inicio de sesión único (SSO) completo, los usuarios pueden iniciar sesión en las aplicaciones en la nube sin tener que volver a escribir sus credenciales. Con la autenticación en la nube puede elegir entre dos opciones:

- Sincronización de hash de contraseña de Azure AD
- Autenticación de paso a través de Azure AD

Autenticación federada: cuando se elige este método de autenticación, Azure AD deja el proceso de autenticación en manos de un sistema 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. El sistema de autenticación puede proporcionar requisitos adicionales de autenticación avanzada. Algunos ejemplos son la autenticación basada en tarjetas inteligentes o la autenticación multifactor de terceros.

Árbol de decisión



Detalles sobre las preguntas de decisión:

1. Azure AD puede controlar el inicio de sesión de los usuarios sin tener que depender de los componentes locales para comprobar las contraseñas.
2. Azure AD puede entregar el inicio de sesión de usuario a un proveedor de autenticación de confianza como AD FS de Microsoft.
3. Si tiene que aplicar directivas de seguridad de Active Directory a nivel de usuario, como la cuenta expirada, cuenta deshabilitada, contraseña expirada, cuenta bloqueada y horas de inicio de sesión de cada usuario, Azure AD requiere algunos componentes locales.
4. Las características de inicio de sesión no son compatibles de forma nativa con Azure AD:
    - Inicio de sesión con tarjetas inteligentes o certificados.
    - Inicio de sesión con el servidor de MFA de forma local.
    - Inicio de sesión con una solución de autenticación de terceros.
    - Solución de autenticación local de varios sitios.

5. Azure AD Identity Protection requiere la sincronización del hash de contraseña, independientemente de qué método de inicio de sesión elija, para proporcionar el informe Usuarios con credenciales filtradas. Las organizaciones pueden conmutar por error a la sincronización del hash de contraseña si se produce un error en su método principal de inicio de sesión y se ha configurado antes del evento de error.

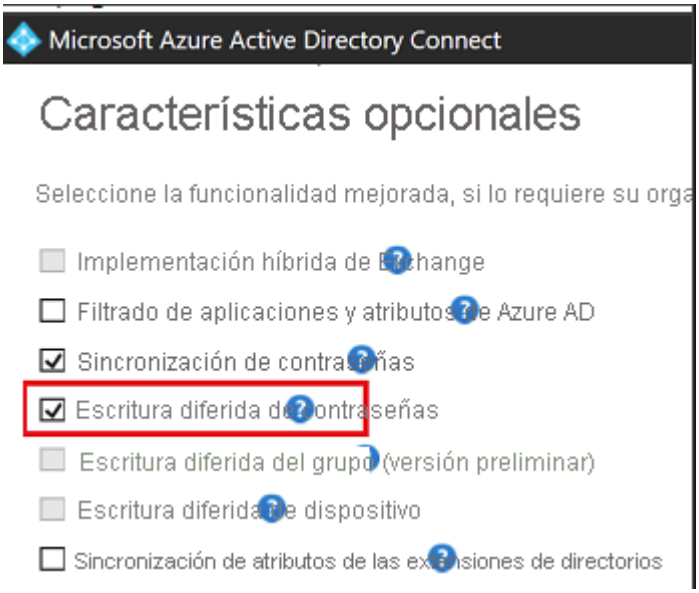
Importante

Este árbol de decisión está pensado como punto de partida para comprender las opciones, pero puede haber otras o incluso combinaciones de distintas opciones. Por ejemplo, puede utilizar Azure AD B2C y configurarlo para permitir el inicio de sesión de los usuarios para los inquilinos de Azure AD multiinquilinos, con o sin el soporte tradicional para el registro de autoservicio y los proveedores de identidad social.

Configurar la escritura diferida de contraseñas

ener una utilidad de restablecimiento de contraseña basada en la nube es genial, pero la mayoría de las empresas todavía tienen un directorio local donde se encuentran sus usuarios. ¿Cómo apoya Microsoft que se mantenga sincronizado el servicio tradicional Active Directory Domain Services (AD DS) con los cambios de contraseña en la nube?

La **escritura diferida de contraseñas** es una característica habilitada con Azure AD Connect que permite que los cambios de contraseña en la nube se vuelvan a escribir en un directorio local existente en tiempo real.



La escritura diferida de contraseñas ofrece:

- **Aplicación de las directivas de contraseña de las instancias locales de Active Directory Domain Services**. Cuando un usuario restablece su contraseña, se comprueba para asegurarse de que cumple la directiva de Active Directory local Domain Services antes de confirmarla en ese directorio. Esta revisión incluye la comprobación del historial, la complejidad, la antigüedad, los filtros de contraseña y cualquier otra restricción de contraseñas que haya definido en la instancia local de Active Directory Domain Services.
- **Información sin demora**. La escritura diferida de contraseñas es una operación sincrónica. Si la contraseña de un usuario no cumple la directiva o no se puede restablecer o modificar por algún motivo, a dicho usuario se le envía una notificación inmediatamente.
- **Admite cambios de contraseña desde el panel de acceso y Microsoft 365**. Cuando los usuarios federados o sincronizados con hash de contraseña vienen a cambiar sus contraseñas expiradas o no expiradas, esas contraseñas se escriben de nuevo en el entorno local de Active Directory Domain Services.
- **Admite la escritura diferida de contraseñas cuando un administrador las restablece desde Azure Portal**. siempre que un administrador restablece la contraseña de un usuario en Azure Portal y se trata de un usuario con federación o sincronización de hash de contraseñas, la contraseña se escribe en diferido en el entorno local. Esta funcionalidad no se admite actualmente en el Portal de administración de Office.
- **No requiere ninguna regla de firewall entrante**. la escritura diferida de contraseñas usa una retransmisión de Azure Service Bus como canal de comunicación subyacente. Toda la comunicación es de salida a través del puerto 443.

Importante

Para usar **autoservicio de restablecimiento de contraseña (SSPR)**, ya debe haber configurado Azure AD Connect en el entorno.