Serie de e-books de Azure
Diseño de una estrategia de cloud híbrido

Microsoft

Administración de identidades y acceso

Abril de 2018

Índice

Introducción

01 /

Reunir las identidades de los usuarios

02 /

Implementar una identidad única para mejorar la capacidad de administración y reducir los costes

03 /

Mejorar la seguridad con identidades administradas fácilmente

04 /

Integrar nuevas aplicaciones en el sistema

Pasos siguientes

Introducción

El cloud ya es una realidad para las empresas. Tu empresa quiere que sus trabajadores puedan hacer su trabajo desde cualquier lugar, accediendo a todas las aplicaciones autorizadas, tanto si están alojadas localmente como en el cloud. De hecho, el 95 por ciento de las empresas ha adoptado una arquitectura de cloud en alguna parte de su negocio, de acuerdo con el informe *2017 State of the Cloud* de RightScale.[1]

Sin embargo, la transición al cloud lleva su tiempo y no todas las empresas han completado su transición de tres o cinco años. Además, es posible que tu empresa no quiera o no necesite mover toda su infraestructura al cloud público, lo que significa que un entorno de cloud híbrido es lo que en realidad existe.

Tanto si la dirección lo sabe como si no, probablemente tu empresa ya se haya embarcado en un proceso para conectar la infraestructura de aplicaciones interna y los servicios en el cloud. Casi dos tercios de las empresas ya han adoptado el camino híbrido, mientras que otro 18 por ciento busca una estrategia de cloud híbrido sin darse cuenta, según la encuesta *State of the Hybrid Cloud 2017* de Microsoft.[2]

1. RightScale. *2017 State of the Cloud*. 15 de febrero de 2017. Pág. 9. *https://www.rightscale.com/lp/state-of-the-cloud* [PDF]

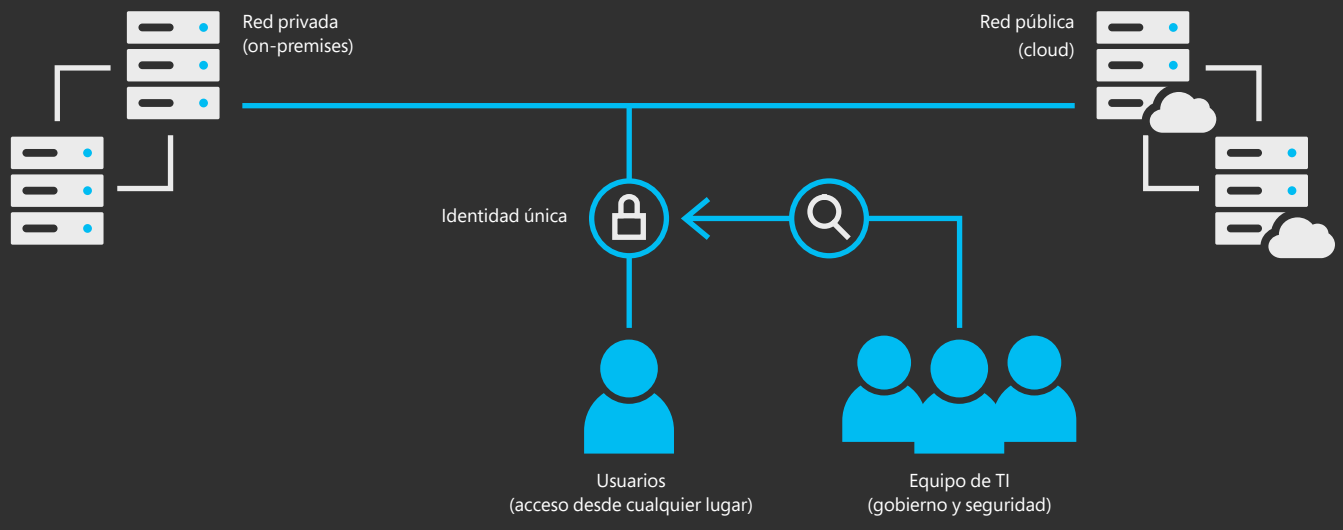
2. Microsoft. *State of the Hybrid Cloud 2017*. 12 de abril de 2017. Pág. 3. *https://info.microsoft.com/state-of-the-hybrid-cloud.html* [PDF]

El hecho de que el 18 por ciento de las empresas no se dé cuenta de que su infraestructura es una combinación de recursos on-premises y en el cloud significa que esas empresas no están haciendo los planes adecuados para administrar eficazmente los datos dentro de la red y los datos en el cloud.

Sin una planificación adecuada, la migración al cloud puede dar lugar (o puede haber dado lugar ya) a varias identidades para tus usuarios. Cada empleado puede tener credenciales corporativas internas, credenciales de inicio sesión para los servicios en el cloud autorizados por la empresa y algunas otras credenciales de inicio de sesión para los servicios de consumo en el cloud.

La eliminación de este laberinto de identidades es un gran paso adelante hacia la migración a una arquitectura estructurada en el cloud híbrido. Proporcionar a los empleados una identidad única permite el uso de funciones de inicio de sesión único en las redes privadas y públicas, simplifica la administración de las credenciales de acceso y mejora la seguridad al permitir la detección avanzada de intrusiones, como el **análisis de comportamiento de usuarios y entidades**. Una solución correctamente diseñada e implementada permitirá que tus empleados accedan a los recursos de la empresa desde cualquier lugar donde necesiten realizar su trabajo y, al mismo tiempo, permitirá a tu equipo regular ese acceso y proteger los datos críticos y los recursos confidenciales.

Identidad única



por ciento de las empresas utilizan Active Directory

Los trabajadores de la empresa promedio utilizan

300
aplicaciones SaaS

1.400
servicios

Una **administración de identidades** eficaz requiere que tu empresa disponga de bases sólidas para la identidad y las credenciales de cada empleado. Más del 90 por ciento de las empresas usan, por ejemplo, Active Directory como parte de su infraestructura de Windows. La vinculación de los servicios de directorio y de identidad on-premises con funciones de inicio de sesión único es el proceso natural para mejorar la infraestructura de cloud híbrido de una empresa. Una identidad común vincula a los empleados con los recursos on-premises y en el cloud, y ofrece a la dirección visibilidad sobre el uso de los recursos de la red por parte de los empleados.

Habrá desafíos que resolver. Los empleados de una empresa promedio usan de forma colectiva más de 300 aplicaciones de software como servicio en el cloud, aunque algunas estimaciones aumentan esta cifra hasta los 1.400 servicios.[3] Es esencial crear una infraestructura que tenga la fiabilidad y escalabilidad necesarias para que los empleados puedan trabajar desde cualquier lugar, pero también la flexibilidad de añadir otros servicios de manera sencilla.

3. Anderson, Brad. "Success with Hybrid Cloud: Identity Management". Microsoft: blog de Enterprise Mobility. 3 de julio de 2014. *https://cloudblogs.microsoft.com/enterprisemobility/2014/07/03/success-with-hybrid-cloud-identity-management*

01 /

Reunir las identidades de los usuarios

Desafíos del cloud híbrido
Consideraciones clave
Soluciones basadas en Azure
Recursos adicionales

Desafíos del cloud híbrido

La integración de los controles de identidad y acceso para las aplicaciones on-premises y en el cloud es una tarea desalentadora. Tus empleados esperarán una interfaz de usuario única en el área de trabajo corporativa, independientemente de si los recursos de ese área están on-premises o en el cloud.

Puesto que el empleado usa de media 36 servicios en el cloud en el trabajo,[4] la creación de una sencilla interfaz para los usuarios no es una tarea fácil. Muchas aplicaciones requieren nombres de usuario y contraseñas específicos de la aplicación. Algunas pueden admitir sistemas de identidades empresariales comunes, mientras que otras pueden requerir algunas de otras API estándar de identidad, como SAML, OAuth y OpenID. Las aplicaciones heredadas pueden requerir código personalizado para que se puedan integrar en un entorno de cloud híbrido.

Ventajas

La identidad única elimina la necesidad de credenciales distintas para cada aplicación o inicio de sesión, y permite:

- Capacidad del equipo de TI de gestionar el acceso de los usuarios hasta el nivel de documento
- Una experiencia de usuario más productiva
- Un enfoque centralizado para administrar el acceso a los datos y aplicaciones críticos

4. Kohgadai, Ajmal. "12 Must-Know Statistics on Cloud Usage in the Enterprise". Skyhigh Networks. *https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise*

Consideraciones clave

Las empresas tienen normalmente dos opciones para administrar las identidades que se pueden usar on-premises o en el cloud: la sincronización de identidades o la identidad como servicio (IDaaS).

Si tu empresa nunca ha configurado una solución de IAM on-premises, depender de un servicio de identidad en el cloud, a veces llamado identidad como servicio (IDaaS), es la forma más sencilla de crear la infraestructura necesaria. Sin embargo, las aplicaciones heredadas pueden dificultar la conexión de dicha infraestructura a cada aplicación para proporcionar a cada trabajador la capacidad de acceder a los recursos necesarios. Para algunas empresas, esto se puede resolver con un proxy de aplicación, que conecta las identidades que residen completamente en el cloud con sus aplicaciones on-premises.

Si tu organización ya dispone de un servidor que administra el acceso on-premises a los recursos, ya sea Microsoft Active Directory, el protocolo Lightweight Directory Access de código abierto u otra tecnología, la sincronización de identidades con un servicio de directorio en el cloud puede constituir una forma sencilla de establecer una identidad única para cada usuario en todas las aplicaciones y servicios.

Una vez que hayas configurado la sincronización de identidades, puedes autenticar a los usuarios mediante tres métodos diferentes (para el inicio de sesión o la validación). Las empresas pueden sincronizar las contraseñas cifradas entre servidores on-premises y en el cloud. Esto permite a los empleados utilizar la misma contraseña para iniciar sesión en los servicios en el cloud y en las aplicaciones on-premises. Además, los servicios en el cloud pueden seguir autenticando y proporcionando acceso a los usuarios aunque se produzca alguna interrupción en el entorno on-premises.

Para las empresas que no pueden almacenar contraseñas cifradas en el cloud debido a requisitos del sector o normativas gubernamentales, existen otras dos opciones. El uso de la autenticación basada en agentes proporciona a los empleados la posibilidad de iniciar sesión una vez y autenticarse tanto en aplicaciones on-premises como en servicios en el cloud mediante un agente on-premises. El uso de una solución de identidad federada permite el inicio de sesión único mediante un servidor de identidad federada on-premises o en el cloud. Este enfoque de administración de identidad y acceso permite a tus empleados iniciar sesión en un único servidor y hacer que ese servidor transmita su identidad a los servicios públicos y privados.

Para determinar el mejor enfoque, tu equipo necesita saber cómo utilizan los empleados los recursos y los servicios de la compañía, qué tecnologías heredadas necesitan integrarse en el servicio de IAM y desde dónde suelen trabajar los empleados. Por esa razón, invita a usuarios clave a las sesiones de planificación, creación e implementación de servicios de AM.

Existen también otras consideraciones. Las personas están empezando a traer sus propias identidades, ya sea de las redes sociales o de una tecnología específica, como Fast Identity Online (FIDO), OAuth u OpenID Connector. Incluso la tecnología basada en blockchain está comenzando a atraer la atención. Estos enfoques de identidad podrían acelerar el registro de los usuarios y reducir la carga de administración de identidades, especialmente para los usuarios externos.

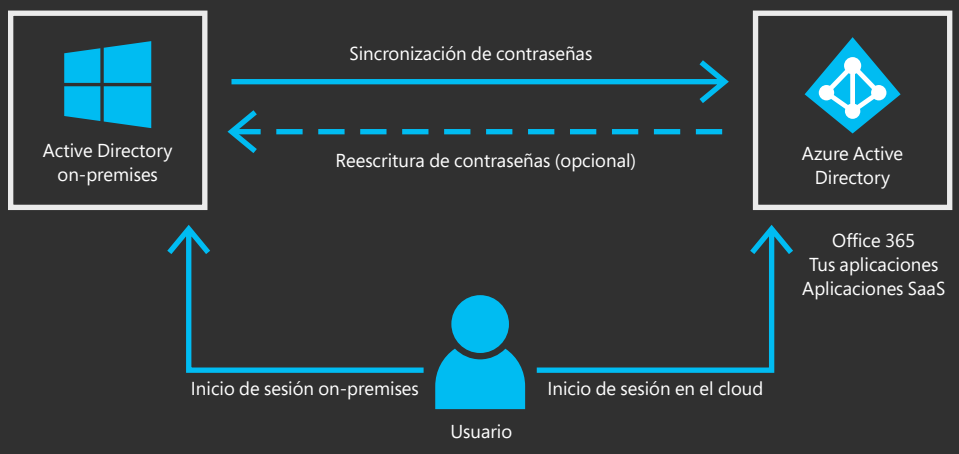
Soluciones basadas en Azure

Microsoft proporciona soluciones para tu empresa, independientemente de en qué etapa del ciclo de adopción del cloud híbrido se encuentre.

Si tu empresa ya tiene un servidor de Active Directory existente, la integración de Active Directory y Azure Active Directory es esencial para proporcionar una excelente experiencia a los usuarios finales. Con la **autenticación de sincronización de hashes de contraseña**, los empleados pueden iniciar sesión fácilmente en los sistemas externos mediante credenciales de AD on-premises. Los hashes de contraseña se replican en Azure Active Directory, lo que permite una única experiencia de inicio de sesión único para ofrecer acceso a los servicios en el cloud.

Autenticación de sincronización de hashes de contraseña

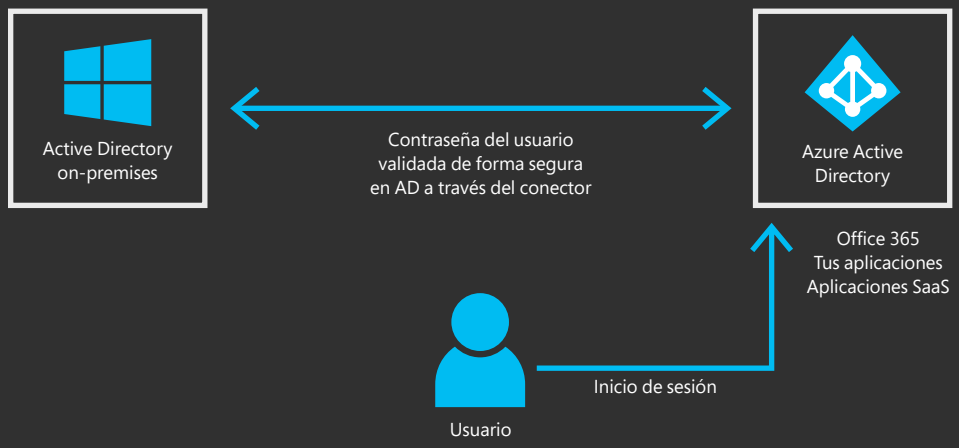
El servicio Azure AD Connect es la forma más sencilla de mantener una única base de datos de identidad autorizada, capaz de comprobar los cambios en el servicio Active Directory on-premises y actualizar automáticamente Azure AD. Aunque los usuarios seguirán necesitando mantener contraseñas distintas para los recursos en el cloud, esto se puede solucionar sincronizando también los hashes de contraseña.



Las empresas que no puedan almacenar contraseñas (ni siquiera hashes) en el cloud público deben usar la **autenticación de paso a través**, que permite un inicio de sesión único para obtener acceso a los recursos privados y en el cloud público. El usuario inicia sesión en Azure Active Directory, que luego autentica la información con la instancia de Active Directory de la empresa mediante un agente on-premises.

Autenticación de paso a través

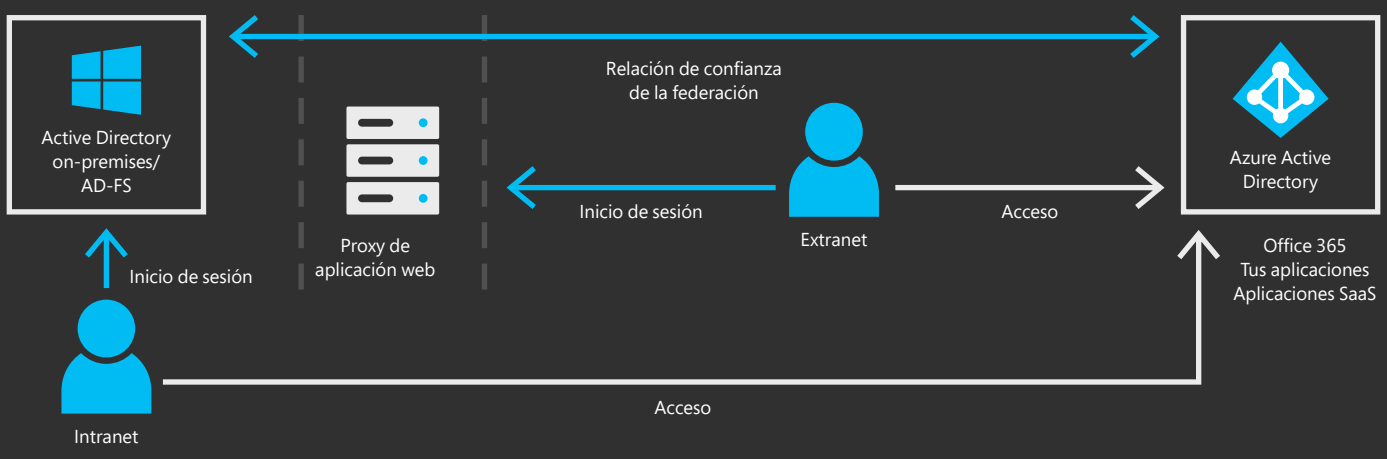
Esta solución de validación de contraseñas permite que los dispositivos on-premises se conecten a los recursos en el cloud mediante las credenciales corporativas, lo que resuelve muchos de los problemas de cumplimiento de la sincronización de identidades. Azure AD pasa las credenciales al servidor de Active Directory on-premises para validar al usuario. A diferencia de la autenticación federada, la empresa no tiene que mantener servidores en una zona perimetral.



Una tercera opción es permitir que los usuarios on-premises inicien sesión mediante servicios de identidad federada implementados on-premises. Con la **autenticación federada**, puedes ofrecer a los usuarios la capacidad de iniciar sesión en servicios basados en Azure AD con las credenciales de la empresa. Mientras los usuarios permanecen en la red, no tienen que iniciar sesión en otros servicios. Azure AD se puede utilizar para la federación con proveedores de identidad de terceros, como Ping Federate, Centrify y otros a través de Azure AD Connect.

Autenticación federada

Con este método de autenticación, la empresa se compromete a proporcionar un servicio de identidad a los empleados. Un servicio de identidad on-premises proporciona funciones de inicio de sesión único a través de Active Directory Federation Services (AD FS). La autenticación federada permite niveles de control de acceso personalizados y más rigurosos. Sin embargo, la disponibilidad de la infraestructura federada se vuelve extremadamente importante: si los usuarios no pueden conectarse a Internet, al controlador de dominio o a los servidores federados, no pueden iniciar sesión en los servicios en el cloud.



Para las empresas que no tienen una instancia de Active Directory on-premises, Azure Active Directory puede actuar como el almacén de información de los empleados, como si se tratara de un proveedor de IDaaS. En este rol, Azure Active Directory proporciona una experiencia de inicio de sesión único para Office 365, SharePoint Online y Exchange y, al mismo tiempo, permite conexiones con servicios externos como LinkedIn, Salesforce y otras 2000 aplicaciones SaaS. En el futuro, los sistemas de identidad pueden converger en este modelo, donde las identidades y las aplicaciones están alojadas y administradas de forma segura en el cloud y solo un número limitado de personas tiene acceso directo a la red corporativa.

La clave para maximizar la productividad de los empleados es crear una experiencia de interfaz de usuario sencilla para ellos.

Debido a que algunos usuarios podrían sentirse confusos si Windows envía un mensaje de advertencia de seguridad y una instrucción de autenticación, el equipo de TI puede utilizar un objeto de directiva de grupo para asignar servicios en el cloud específicos a la zona corporativa (véase Recursos adicionales a continuación). Asimismo, Azure permite la personalización para ofrecer una experiencia más coherente. Desde el punto de vista del usuario, los servicios integrados de identidad ofrecen funciones de autoservicio, como restablecimientos de contraseñas y administración de perfiles y grupos de usuarios, en la infraestructura en el cloud y on-premises.

Otra ventaja de la integración de identidades radica en que la implementación de la autenticación multifactor (AMF) resulta mucho más sencilla. El servicio Azure Authenticator puede añadir un factor adicional de autenticación, como una llamada telefónica, un código secreto o el uso de la aplicación móvil Azure AMF, a distintas tecnologías on-premises, como soluciones Citrix, puertas de acceso de escritorio remoto o redes privadas virtuales. Los usuarios pueden gestionar totalmente la configuración de Azure Authenticator específica del usuario.

Recursos adicionales

Microsoft: prácticas recomendadas para el cloud híbrido
https://blogs.technet.microsoft.com/hybridcloudbp/2016/07/12/hybrid-cloud-identity-ad-and-azuread/

Consideraciones de diseño de identidades híbridas
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-hybrid-identity-design-considerations-overview

02 /

Implementar una identidad única para mejorar la capacidad de administración y reducir los costes

Ventajas

La administración de una identidad única para cada usuario en el cloud permite:

- Un aprovisionamiento y desaprovisionamiento más eficiente y rentable del acceso de los empleados a los servicios empresariales
- Más seguridad mediante la captura completa del comportamiento de los usuarios en el cloud
- Mayor visibilidad de las tendencias de uso, lo que permite una mejor presupuestación de los recursos

Desafíos del cloud híbrido

La creación de una identidad única para cada usuario en un entorno de cloud híbrido promete una gestión más eficiente de los servicios on-premises y en el cloud, pero la complejidad de la tarea puede estancar fácilmente el proyecto.
Las empresas tienen que lidiar con las complejidades de registrar cada usuario con cada aplicación, administrar de forma segura esas credenciales y hacer que todo ese proceso sea sencillo para los empleados. En función de las características de la implementación, la dificultad puede ser aún mayor si no todas las aplicaciones utilizan el mismo protocolo o estándar.

Para implementar correctamente un modelo de administración de identidades en el cloud híbrido, este debe ampliarse a un gran número de empleados y aplicaciones, así como proporcionar una experiencia de inicio de sesión único. Las identidades deben sincronizarse o federarse entre los usuarios on-premises y las aplicaciones SaaS, y tienen que integrarse con diferentes servicios y protocolos.

El acceso a menudo no es una disyuntiva: la infraestructura debe admitir una serie de roles de usuario que conceder, pero limitar el acceso a determinados recursos. Como los roles, los recursos, las aplicaciones y las identidades siempre están cambiando, el equipo querrá tener una infraestructura de administración flexible. Cuando se supervise y analice el uso de las aplicaciones y el comportamiento de los usuarios en busca de anomalías, mejorará tanto la seguridad como la capacidad de administración de la infraestructura.

Consideraciones clave

Para administrar eficazmente las identidades y la infraestructura de directorio, debes centrarte en tres áreas: implementación, operaciones y análisis.

Inicialmente, tu equipo, a partir de las aportaciones de los directivos, debería definir un conjunto de objetivos y una visión para implementar un sistema de administración de identidades, incluida la posibilidad de adoptar una solución integral o la identificación de aplicaciones o servicios heredados que no estarán cubiertos. Deberías considerar también un conjunto diverso de casos de uso y una estrategia en la que se tenga en cuenta a una gran variedad de usuarios para conocer los factores que podrían afectar a los empleados.

Los reglamentos, por ejemplo, pueden complicar cualquier implementación en el cloud, en función de cómo la empresa maneje la información de identidad. El Reglamento General Europeo de Protección de Datos (GDPR) impone multas cuantiosas a las empresas que no protegen los datos de los ciudadanos europeos. El GDPR y otras normativas deberán tenerse en consideración a la hora de determinar si los datos de identidad se pueden alojar en el cloud.

Para evitar mayores problemas, implementa tu solución de IAM en etapas, realizando pequeñas pruebas piloto mientras mantienes suficientes redundancias para garantizar que los servicios de identidad actuales estén disponibles. (La sección Recursos adicionales contiene un buen ejemplo). Los servicios básicos deben adoptarse primero, vinculando después otros servicios populares según sea necesario.

El funcionamiento de los servidores y servicios de administración de identidades y acceso es muy específico de la tecnología adoptada. Entre las consideraciones clave se incluyen las siguientes:

- **Disponibilidad:** la infraestructura en el cloud debería aplicar la redundancia adecuada para garantizar que los servicios estén disponibles cuando se necesiten y desde donde los empleados realizan su trabajo
- **Replicación:** asegúrate de que la empresa realiza una copia de seguridad de los datos de identidades y los registros de acceso (el almacén de identidades) con la frecuencia necesaria

Una vez que los servicios en el cloud estén implementados y las operaciones estén bien gestionadas, asegúrate de medir el rendimiento. Tu equipo de TI puede medir el rendimiento del sistema y cualquier mejora (o deterioro) como resultado de la adopción de la infraestructura de identidad híbrida.

Inicialmente, el equipo debe centrarse en las ineficiencias actuales y determinar un conjunto de métricas que puedan medir el progreso, o el retroceso, en el rendimiento general. Un ejemplo de una métrica clave es el tiempo medio que se tarda en aprovisionar y desaprovisionar a los usuarios, y si ese tiempo disminuye con la migración al inicio de sesión único.

Los restablecimientos de contraseñas a menudo causan interrupciones importantes tanto para los usuarios como para la administración de TI. Al medir el impacto de los restablecimientos de contraseña, es probable que puedas mostrar la mejora que las identidades únicas pueden aportar a la empresa.

Soluciones basadas en Azure

La centralización de la administración de identidades es una ventaja importante para implementar la administración de identidades y acceso en un cloud híbrido.

La centralización de la administración de identidades es una ventaja importante para implementar la administración de identidades y acceso en un cloud híbrido. En los servicios en el cloud de Microsoft, esto se puede hacer mediante la federación de identidades para permitir un verdadero inicio de sesión único a través de Azure Active Directory Federation Services (AD FS) o utilizando Azure AD Connect para sincronizar las contraseñas entre las instalaciones on-premises de Active Directory Azure AD.

En cualquier caso, los servicios de inicio de sesión único deben ser capaces de aumentar la productividad y la seguridad de los usuarios. Al implementar las funciones de administración de contraseñas de Azure, tus empleados pueden administrar y restablecer sus propias contraseñas, lo que aumenta la facilidad de uso y permite al equipo de administración realizar un seguimiento de la actividad de restablecimiento como un control de seguridad.

Para mejorar la seguridad y cumplir con determinadas reglamentaciones del sector, las cuentas pueden estar protegidas por un segundo factor de autenticación. Azure Multi-Factor Authentication ofrece a los usuarios diferentes formas de proporcionar un segundo factor (por ejemplo, por teléfono, mensaje de texto o aplicación móvil) y reduce las probabilidades de que las credenciales atacadas conlleven un riesgo adicional. Además de las identidades, el equipo puede restringir aún más el acceso a servidores y datos confidenciales adoptando el concepto de "privilegios mínimos" mediante controles de acceso basados en rol y asignando derechos limitados a los usuarios que no son administradores.

El equipo de TI también desempeña un papel en la formación de los desarrolladores para que usen los mecanismos de autenticación proporcionados por los servicios de identidad utilizando protocolos estándar del sector, como OAuth 2.0 y OpenID Connect. La empresa debe adoptar una política que establezca que todas las aplicaciones y servicios externos deben registrarse en Azure AD. (En la sección Recursos adicionales y en el capítulo 4 se ofrece más información).

Recursos adicionales

Aspectos básicos de la administración de identidades de Azure
https://docs.microsoft.com/azure/active-directory/identity-fundamentals

Introducción a Azure Multi-Factor Authentication en el cloud
https://docs.microsoft.com/azure/active-directory/authentication/howto-mfa-getstarted

Uso del control de acceso basado en roles para administrar el acceso a los recursos de la suscripción de Azure
https://docs.microsoft.com/azure/role-based-access-control/role-assignments-portal

Programa de gestión de identidades y acceso de la Universidad de Harvard
http://iam.harvard.edu/files/iam/files/iam_program_plan.pdf [PDF]

Escenarios de autenticación para Azure AD
https://docs.microsoft.com/azure/active-directory/develop/authentication-scenarios

03 /

Mejorar la seguridad con identidades administradas fácilmente

Desafíos del cloud híbrido

Consideraciones clave

Soluciones basadas en Azure

Recursos adicionales

Mientras una solución híbrida de administración de identidades correctamente implementada reporta dividendos en cuanto a productividad y facilidad de gestión en general, la asignación de una identidad única a los usuarios proporciona beneficios importantes en materia de seguridad.

Puesto que el robo de credenciales constituye una fuente de ataques importante, la supervisión de las identidades en busca de un uso anómalo es una consideración de seguridad clave para los clouds híbridos.

Ventajas

Un sistema que asigna a los usuarios una identidad única tanto en servicios on-premises como en el cloud permite:

- Mayor seguridad mediante políticas que requieren una contraseña segura y un segundo factor de autenticación para todas las credenciales de usuario
- Mayor capacidad para detectar actividades de usuario sospechosas
- Menor tiempo de reacción a los incidentes

Desafíos del cloud híbrido

Las contraseñas han fracasado estrepitosamente como un medio escalable de gestionar la seguridad basada en la identidad. Los empleados eligen a menudo contraseñas poco seguras y reutilizan la misma contraseña en diferentes aplicaciones y servicios en el cloud. Mientras tanto, los equipos de TI deben lidiar con la administración de políticas de contraseñas —y el cumplimiento de esas políticas—, así como con la falta de visibilidad de las identidades múltiples de cada empleado.

Un sistema de inicio de sesión único permite saber cómo los usuarios —tanto si son empleados o personal subcontratado como clientes— acceden a los recursos y datos corporativos. Una solución de administración de identidades centralizada simplifica enormemente la recopilación de información, pero los equipos de TI deben seguir analizando los datos y creando alertas para el uso anómalo.

Aunque es posible que tu empresa ya haya implementado análisis del comportamiento de los usuarios y las entidades, ampliar la cobertura fuera de la red de la empresa para incorporar servicios en el cloud puede no ser una tarea sencilla. Los proveedores de servicios en el cloud normalmente solo permiten a las empresas controlar la seguridad desde un panel central que forma parte del servicio. Es posible que tu organización necesite evaluar a los proveedores de servicios en el cloud en función de si permiten recopilar la información mediante software o servicios de supervisión de terceros.

Consideraciones clave

Una mayor seguridad suele equivaler a mayores molestias para los usuarios finales, pero una infraestructura de inicio de sesión correctamente estructurada junto con la administración de la identidad y el acceso ofrece más seguridad, además de mayor facilidad de uso para los empleados y para la empresa.

Las contraseñas seguras y MFA proporcionan beneficios importantes en materia de seguridad. Sin embargo, estos beneficios se pueden incrementar emparejando los análisis de datos con los registros de actividad de los usuarios para proteger a la empresa de las intrusiones y del ataque a los datos. La supervisión de usuarios — especialmente en cuentas de alto riesgo y reguladas— puede reportar dividendos importantes a tu programa de seguridad.

Para aprovechar la información, tu equipo debe realizar un seguimiento de las métricas correctas y tener implementada una plataforma de análisis adecuada.

El objetivo de combinar el análisis de los registros de acceso debería ser agrupar los análisis predictivos con el control de acceso para crear controles de seguridad flexibles, lo que se conoce también como "acceso condicional basado en riesgos". Si la actividad anómala procede de la identidad de un usuario, se puede restringir el privilegio hasta que el usuario confirme su identidad con un segundo factor. El análisis de los eventos debe realizarse en tiempo real a través de un producto de administración de la información de seguridad y eventos (SIEM) o análisis de registros.

Es importante elegir las métricas correctas. Estas son algunas de ellas, que pueden ofrecer visibilidad sobre la seguridad del cloud híbrido:

- El número de credenciales que utilizan el inicio de sesión único
- El número de servicios a los que acceden los empleados
- El número de cuentas huérfanas (las que parecen no tener usuario), especialmente para usuarios con privilegios

Soluciones basadas en Azure

Microsoft Azure te ofrece una serie de herramientas importantes para supervisar los intentos de acceso anómalos y mejorar la seguridad de tu red corporativa.

Las políticas de acceso condicional y los informes de anomalías de Azure AD Premium identificarán los intentos de los usuarios de iniciar sesión desde redes anónimas o desde varias ubicaciones, registrará los intentos de los atacantes de usar scripts de fuerza bruta para adivinar las contraseñas y alertará al equipo de TI de cualquier intento de inicio de sesión desde dispositivos infectados y direcciones IP sospechosas. Todos los intentos de acceso se registran y un conjunto sencillo de informes puede presentar patrones de ataque específicos, como inicios de sesión fallidos, el acceso simultáneo desde diferentes ubicaciones y fuentes desconocidas.

La protección de identidad de Azure AD identifica activamente los riesgos más actuales en el panel del servicio y envía un resumen diario por correo electrónico. Al ajustar el nivel de riesgo, los profesionales de TI pueden buscar anomalías específicas o satisfacer los requisitos de cumplimiento.

Microsoft incluye también información de Azure AD en su tecnología Security Graph, que ayuda a las empresas a identificar eventos anómalos y posibles ataques utilizando las credenciales de los empleados. Microsoft Security Graph utiliza la tecnología de base de datos de gráficos de tu empresa para extraer rápidamente información de eventos y datos no estructurados.

Azure AD se integra también con los sistemas SIEM más populares, como Arcsight, QRadar y Splunk. Otros sistemas pueden tener conectores nativos que se pueden utilizar para importar archivos de registro de Azure. Al importar y analizar los registros, el sistema SIEM puede presentar un panel de eventos unificado que proporcione a los equipos de seguridad de la información aún más visibilidad sobre las posibles amenazas.

Recursos adicionales

Introducción a la integración de registro de Microsoft Azure
https://docs.microsoft.com/azure/security/security-azure-log-integration-overview

Procedimientos recomendados para la administración de identidades y la seguridad del control de acceso en Azure
https://docs.microsoft.com/azure/security/azure-security-identity-management-best-practices

Acceso condicional en Azure Active Directory
https://docs.microsoft.com/azure/active-directory/conditional-access/overview

04 /

Integrar nuevas aplicaciones en el sistema

Desafíos del cloud híbrido
Consideraciones clave
Soluciones basadas en Azure
Recursos adicionales

El empleado promedio utiliza 36 servicios en el cloud diferentes en el trabajo

Desafíos del cloud híbrido

El empleado promedio utiliza 36 servicios en el cloud diferentes en el trabajo, incluidos 9 servicios de colaboración, 6 servicios de intercambio de archivos y 5 servicios de intercambio de contenido. En total, la empresa tiene de media más de 1400 aplicaciones en el cloud para uso de los empleados.[6]

Cuando tu empresa empiece a adoptar una implementación de cloud híbrido más avanzada, estos servicios deben recibir soporte, junto con todo el software on-premises, además de integrarse en la infraestructura de IAM. Sin esta integración, la empresa podría exponer los datos y la propiedad intelectual a los ataques a través del robo de credenciales y la autenticación débil.

Los desarrolladores son un aliado clave en la integración de las aplicaciones en una solución de administración de identidades. Necesitarás formarlos y trabajar con ellos para conectar las aplicaciones existentes y las nuevas aplicaciones en el sistema de IAM. La identidad de los usuarios se usará a menudo para conectar las aplicaciones a través de API y microservicios con el fin de crear nuevas funciones, y los desarrolladores serán fundamentales para tus iniciativas.
Sin equipos de desarrollo a bordo y educados en las mejores prácticas de programación de la autenticación, los servicios en el cloud y las aplicaciones on-premises podrían ser susceptibles de sufrir ataques.

6. Kohgadai, Ajmal. "12 Must-Know Statistics on Cloud Usage in the Enterprise". Skyhigh Networks. *https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise*

Ventajas

Para obtener el máximo provecho del cloud, tu empresa debe integrar tantas aplicaciones como sea posible en sus servicios de identidad en el cloud híbrido. Esta integración:

- Permite a cada empleado acceder a las aplicaciones a través del servicio de inicio de sesión único
- Proporciona a la compañía visibilidad de cómo los empleados usan las aplicaciones
- Mejora la seguridad mediante la detección de actividades sospechosas, incluso en servicios fuera de la red de la empresa

Consideraciones clave

Como los empleados utilizan cada vez más una variedad de aplicaciones independientemente de dónde residan —on-premises o en el cloud—, la integración de esas aplicaciones de forma que puedan compartirse los datos en el área de trabajo y a través de procesos de colaboración es importante.

Los desarrolladores deben conocer los procedimientos recomendados para la autenticación de los usuarios a través del servicio de identidad elegido. Siempre que se desarrolle una nueva aplicación o se actualice una aplicación heredada, deben utilizar un proceso de codificación seguro, como el ciclo de vida de desarrollo de seguridad (SDL) de Microsoft. Todas las aplicaciones nuevas desarrolladas por la empresa o un tercero deben registrarse con el servidor de identidades.

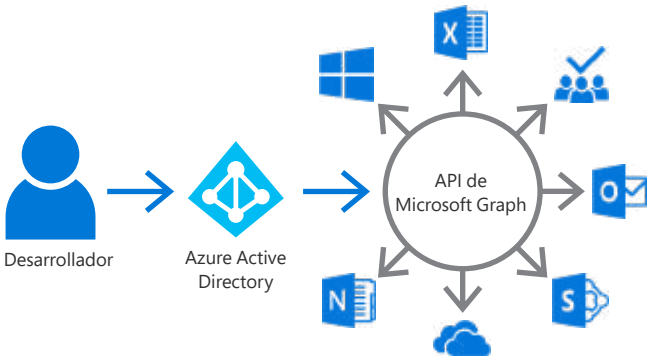
Las pruebas iterativas del código de autenticación también son fundamentales. Como la autenticación es una disciplina compleja, los desarrolladores deben utilizar una biblioteca o servicio para añadir la funcionalidad a una aplicación específica. Aun así, las aplicaciones deben probarse para garantizar que el código de autenticación se llame y se instancie correctamente.

Soluciones basadas en Azure

Azure AD requiere que los desarrolladores sigan las prácticas recomendadas.

Como la identidad se proporciona como un servicio, Azure AD puede exigir y exige que todas las aplicaciones externalicen la autenticación en Azure AD. Este requisito garantiza que Azure AD tenga la información que necesita para coordinar la comunicación con cualquier aplicación cuando se gestiona el inicio de sesión único o se intercambian tokens.

Tus desarrolladores deben registrar las aplicaciones con un inquilino de Azure AD para proporcionar información sobre las aplicaciones al servicio y recibir a cambio un identificador de aplicación. Al registrar la aplicación con la API de Microsoft Graph, otras aplicaciones también pueden solicitar acceso a las aplicaciones.



Tras el registro, los desarrolladores pueden vincular las aplicaciones utilizando la plataforma de consentimiento de Azure AD, basada en el estándar del sector OAuth 2.0. Una vez establecido el consentimiento, la aplicación cliente puede hacer llamadas a otras aplicaciones y compartir información según lo determinen los permisos concedidos.

Al integrarse con las aplicaciones, el equipo puede aumentar la seguridad utilizando el vencimiento de la sesión del usuario mediante el establecimiento de la duración del token emitido por Azure AD. Los desarrolladores pueden decidir utilizar esta duración en la aplicación o incluso reducir el tiempo para obligar a los usuarios a cerrar la sesión en función de un período de inactividad.

Los desarrolladores también pueden utilizar Azure AD como base de identidad para soluciones que no sean de Azure, reemplazando tecnologías como Kerberos o el Protocolo ligero de acceso a directorios (LDAP). Los programadores pueden utilizar Azure AD para establecer fácilmente el inicio de sesión único para las aplicaciones en el cloud y para consultar y modificar los datos de identidad alojados en el directorio.

Recursos adicionales

Guía para desarrolladores para aprovechar las funciones de identidad de las aplicaciones SaaS
https://docs.microsoft.com/azure/security/azure-security-identity-management-best-practices#guidedevelopers-to-leverage-identitycapabilities-for-saas-apps

Integración de aplicaciones con Azure Active Directory
https://docs.microsoft.com/azure/active-directory/develop/quickstart-v1-add-azure-ad-apps

¿Qué es el acceso y el inicio de sesión único en las aplicaciones con Azure Active Directory?
https://docs.microsoft.com/azure/active-directory/manage-apps/what-is-single-sign-on

Conexión de Azure AD Identity Protection con Azure Security Center
https://docs.microsoft.com/azure/security-center/security-center-partner-integration

Pasos siguientes

El cloud no es sencillo. Más de la mitad de los profesionales de TI encuentran complicado el cloud debido a su entorno complejo y casi la mitad carecen de los conocimientos para aprovechar al máximo el cloud híbrido.[7] La integración de las aplicaciones on-premises con los servicios en el cloud requiere prestar especial atención al diseño, la implementación y las operaciones.

Empezar a consolidar las identidades de los usuarios dentro de la red y en todos los servicios en el cloud de la empresa puede simplificar uno de los aspectos más complejos del cloud.

El objetivo de Microsoft es simplificar las arquitecturas de cloud híbrido con Azure. Como Azure Active Directory se conecta fácilmente con tu instancia on-premises de Active Directory, tu empresa puede aprovechar su arquitectura existente para avanzar rápidamente hacia un cloud híbrido más integrado.

Empezar ahora

Simplifica y protege tu entorno en el cloud con Azure

7. Microsoft. State of the Hybrid Cloud 2017. 12 de abril de 2017. Pág. 13. *https://info.microsoft.com/state-of-the-hybrid-cloud.html* [PDF]