Definición de autenticación y autorización

Autenticación

La autenticación es el proceso de demostrar que una persona es quien dice ser. Cuando alguien compra un artículo con una tarjeta de crédito, es posible que tenga que mostrar una forma adicional de identificación. De esta manera, demuestra que es la persona cuyo nombre aparece en la tarjeta. En este ejemplo, el usuario puede mostrar el DNI, que sirve como forma de autenticación y verifica su identidad.

Si desea acceder a un equipo o un dispositivo, se encontrará con un tipo de autenticación similar. Es posible que se le pida que escriba un nombre de usuario y una contraseña. El nombre de usuario indica quién es, pero no es suficiente por sí solo para concederle acceso. Cuando lo combina con la contraseña, que solo usted debe conocer, obtiene acceso a los sistemas. El nombre de usuario y la contraseña, juntos, son una forma de autenticación. A veces, la autenticación se abrevia como AuthN.

Autorización

Cuando autentique a un usuario, tendrá que decidir adónde puede ir y qué se le permite ver y tocar. Este proceso se denomina autorización.

Supongamos que quiere pasar la noche en un hotel. Lo primero que hará es ir a la recepción para iniciar el "proceso de autenticación". Una vez que el recepcionista haya comprobado quién es, le dará una tarjeta-llave y ya podrá dirigirse a su habitación. Piense en la tarjeta-llave como el proceso de autorización. La tarjeta-llave solo le permitirá abrir las puertas y los ascensores a los que puede acceder, como la puerta de su habitación.

En términos de ciberseguridad, la autorización determina el nivel de acceso o los permisos de una persona autenticada a los datos y los recursos. A veces, la autorización se abrevia como AuthZ.

Definición de identidad como perímetro de seguridad principal

La colaboración digital ha cambiado. Los empleados y asociados ahora necesitan colaborar y acceder a los recursos de la organización desde cualquier lugar, en cualquier dispositivo y sin que ello afecte a su productividad. También se ha producido una aceleración en el número de personas que trabajan desde casa.

La seguridad de la empresa debe adaptarse a esta nueva realidad. El perímetro de seguridad ya no se puede ver como la red local. Ahora se extiende a:

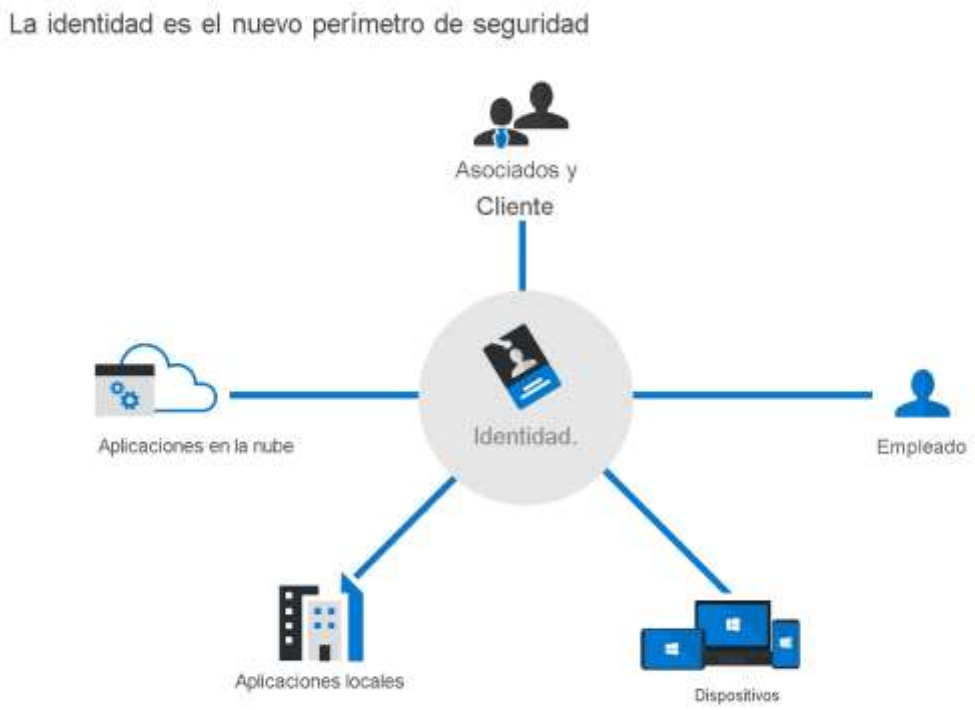
- Aplicaciones SaaS para cargas de trabajo críticas para la empresa que se pueden hospedar fuera de la red corporativa.
- Los dispositivos personales que los empleados usan para tener acceso a los recursos corporativos (BYOD o Bring Your Own Device) mientras trabajan desde casa.
- Los dispositivos no administrados que usan los asociados o clientes al interactuar con los datos corporativos o colaborar con los empleados

- Internet de las cosas, conocido como dispositivos IoT, instalado en la red corporativa y dentro de las ubicaciones de los clientes.

El modelo de seguridad tradicional basado en el perímetro ya no es suficiente. La identidad se ha convertido en el nuevo perímetro de seguridad que permite a las organizaciones proteger sus recursos.

Pero ¿qué significa una identidad? Una identidad es el conjunto de aspectos que definen o caracterizan a alguien o algo. Por ejemplo, la identidad de una persona incluye la información que usa para autenticarse, como su nombre de usuario y contraseña, y su nivel de autorización.

Una identidad puede estar asociada a un usuario, una aplicación, un dispositivo o cualquier otra cosa.



Cuatro pilares de una infraestructura de identidad

La identidad es un concepto que abarca todo un entorno, por lo que las organizaciones deben pensar en ello en general. Hay una colección de procesos, tecnologías y directivas para administrar identidades digitales y controlar cómo se usan para tener acceso a los recursos. Pueden organizarse en cuatro pilares fundamentales que las organizaciones deben tener en cuenta al crear una infraestructura de identidad.

- **Administración**. La administración consiste en la creación y la administración o gobernanza de identidades para los usuarios, dispositivos y servicios. Como administrador, puede administrar cómo y en qué circunstancias pueden cambiar las características de las identidades (se pueden crear, actualizar y eliminar).

- **Autenticación**. El pilar de autenticación indica cuánto necesita saber un sistema de TI sobre una identidad para tener pruebas suficientes de que realmente son quienes dicen ser. Implica el acto de solicitar a un usuario credenciales legítimas.
- **Autorización**. El pilar de autorización trata sobre el procesamiento de los datos de identidad entrante para determinar el nivel de acceso de una persona o servicio autenticado dentro de la aplicación o servicio al que quiere obtener acceso.
- **Auditoría**. El pilar de auditoría consiste en realizar un seguimiento de quién realiza qué, cuándo, dónde y cómo. La auditoría incluye la creación de informes, alertas y gobernanza de identidades en profundidad.

Direccionar cada uno de estos cuatro pilares es clave para una solución completa y sólida de identidad y control de acceso.

Descripción del rol del proveedor de identidades

Autenticación moderna es un término genérico para los métodos de autenticación y autorización entre un cliente, como un portátil o un teléfono, y un servidor, como un sitio web o una aplicación. En el centro de la autenticación moderna está el rol del *proveedor de identidades*. Un proveedor de identidades crea, mantiene y administra la información de identidad al tiempo que proporciona servicios de autenticación, autorización y auditoría.

Con la autenticación moderna, quien proporciona todos los servicios, incluidos todos los servicios de autenticación, es un proveedor de identidades central. El proveedor de identidades almacena y administra de forma centralizada la información que se usa para autenticar el usuario en el servidor.

Con un proveedor de identidades central, las organizaciones pueden establecer directivas de autenticación y autorización, supervisar el comportamiento de los usuarios, identificar actividades sospechosas y reducir los ataques malintencionados.

Vea este vídeo para obtener más información sobre la autenticación moderna y cómo funciona con un proveedor de identidades central.

Como se ve en el vídeo, gracias a la autenticación moderna, el cliente se comunica con el proveedor de identidades mediante la asignación de una identidad que se puede autenticar. Cuando se ha comprobado la identidad (que puede ser un usuario o una aplicación), el proveedor de identidades emite un *token de seguridad* que el cliente envía al servidor.

El servidor valida el token de seguridad a través de su *relación de confianza* con el proveedor de identidades. Mediante el uso del token de seguridad y la información que contiene, el usuario o la aplicación accede a los recursos necesarios en el servidor. En este escenario, el proveedor de identidades almacena y administra el token y la información que contiene. El proveedor de identidades centralizado proporciona el servicio de autenticación.

Microsoft Azure Active Directory es un ejemplo de un proveedor de identidades basado en la nube. Otros ejemplos son Twitter, Google, Amazon, LinkedIn y GitHub.

Inicio de sesión único

Otra funcionalidad fundamental de un proveedor de identidades y "autenticación moderna" es la compatibilidad con el inicio de sesión único (SSO). Con el SSO, el usuario inicia sesión una vez y esa credencial se usa para tener acceso a varias aplicaciones o recursos. A la acción de configurar el SSO para que funcione entre varios proveedores de identidades se le conoce como federación.

Descripción del concepto de servicios de directorio y Active Directory

En el contexto de una red de equipos, un directorio es una estructura jerárquica que almacena información acerca de los objetos de la red. Un servicio de directorio almacena los datos del directorio y los pone a disposición de los usuarios de red, los administradores, los servicios y las aplicaciones.

Active Directory (AD) es un conjunto de servicios de directorio desarrollados por Microsoft como parte de Windows 2000 para redes locales basadas en dominio. El servicio más conocido de este tipo es Active Directory Domain Services (AD DS). Almacena información sobre los miembros del dominio, incluidos los dispositivos y los usuarios, comprueba sus credenciales y define sus derechos de acceso. Un servidor que ejecuta AD DS es un controlador de dominio.

AD DS es un componente central de las organizaciones con una infraestructura de TI local. AD DS ofrece a las organizaciones la capacidad de administrar varios sistemas y componentes de la infraestructura local mediante una única identidad por usuario. Sin embargo, AD DS no es compatible de forma nativa con los dispositivos móviles, las aplicaciones SaaS o las aplicaciones de línea de negocio que requieren métodos de *autenticación moderna*.

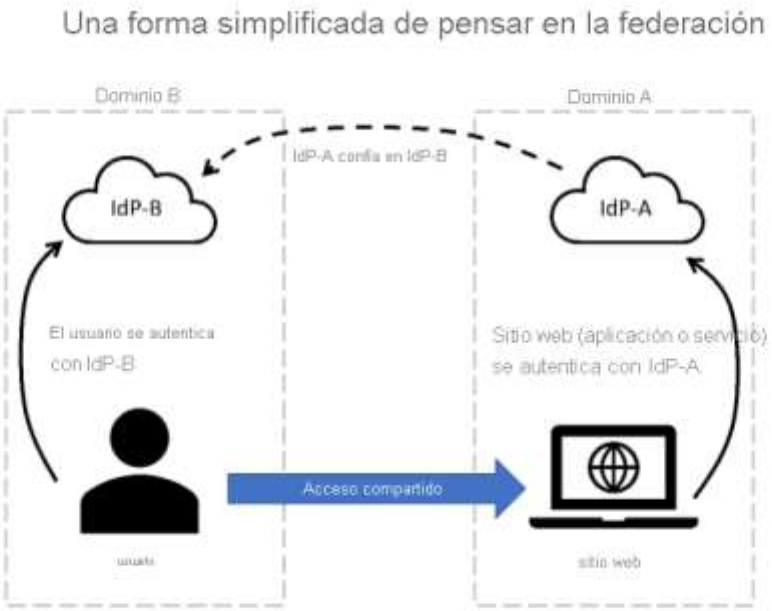
El crecimiento de Cloud Services, las aplicaciones SaaS y los dispositivos personales que se usan en el trabajo, ha dado como resultado la necesidad de la autenticación moderna y una evolución de las soluciones de identidad basadas en Active Directory.

Azure Active Directory es la siguiente evolución de las soluciones de administración de identidad y acceso. Proporciona a las organizaciones una solución de identidad como servicio (IDaaS) para todas sus aplicaciones en la nube y en el entorno local. En este curso, nos centraremos en Azure AD, el proveedor de identidades basado en la nube de Microsoft.

Para obtener más información sobre las diferencias entre los conceptos de Active Directory y Azure Active Directory, consulte la sección Más información de la unidad de resumen y recursos que redirige a la documentación.

Descripción del concepto de federación

La federación permite el acceso a los servicios a través de los límites de la organización o del dominio mediante el establecimiento de relaciones de confianza entre el proveedor de identidades del dominio correspondiente. Con la federación, no es necesario que un usuario mantenga un nombre de usuario y una contraseña diferentes al acceder a los recursos de otros dominios.



Aunque la función de los proveedores de identidad se describe en una nube, no es necesario que estén basados en la nube. La función de los proveedores de identidad puede ser local.

La manera simplificada de considerar este escenario de federación es la siguiente:

- El sitio web, en el dominio A, usa los servicios de autenticación del proveedor de identidades A (IdP-A).
- El usuario, en el dominio B, se autentica con el proveedor de identidades B (IdP-B).
- IdP-A tiene una relación de confianza configurada con IdP-B.
- Cuando el usuario, que desea acceder al sitio web, proporciona sus credenciales, el sitio web confía en el usuario y permite el acceso. Este acceso se permite debido a la confianza que ya se ha establecido entre los dos proveedores de identidades.

Con la federación, la confianza no siempre es bidireccional. Aunque IdP-A puede confiar en IdP-B y permitir que el usuario del dominio B tenga acceso al sitio web del dominio A, lo contrario no es cierto, a menos que se configure la relación de confianza.

Un ejemplo común de federación en la práctica es cuando un usuario inicia sesión en un sitio de terceros con su cuenta de redes sociales, como Twitter. En este escenario, Twitter es un proveedor de identidades y el sitio de terceros podría estar usando otro proveedor de identidades, como Azure AD. Hay una relación de confianza entre Azure AD y Twitter.