TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SERVICIOS DE AUTENTICACIÓN Y AUTORIZACIÓN

SEGURIDAD Y VIRTUALIZACION

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

GRUPO: 7US

PRESENTA:

RUFINO MENDOZA VAZQUEZ - 21620198

ANA MICHEL LEÓN LEÓN - 21620112

ROSA SALAZAR DOROTEO - 18620216

FERNANDA RUIZ HERAS - 21520151

DOCENTE

ING. EDWARD OSORIO SALINA

Tlaxiaco, Oax., 10 de Septiembre del 2024.

"Educación, ciencia y tecnología, progreso día con día"®

Contenido

Lista de Ilustraciones

Servicios de autenticación

La autenticación es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a recursos de la organización. El proceso de autenticación incluye tres pasos principales:

- Identificación: Los usuarios establecen quiénes son a través de un nombre de usuario, normalmente.
- Autenticación: Normalmente, los usuarios prueban que son quienes dicen ser al escribir una contraseña (algo que, supuestamente, solo conoce el propio usuario); sin embargo, para fortalecer la seguridad, muchas organizaciones también solicitan que prueben su identidad mediante algo que poseen (un teléfono o dispositivo de tokens) o algo que son (una huella dactilar o escáner facial).
- Autorización: El sistema comprueba que los usuarios tengan permisos para el sistema al que intentan acceder. (Microsoft, s.f.)

LDAP (Lightweight Directory Access Protocol)

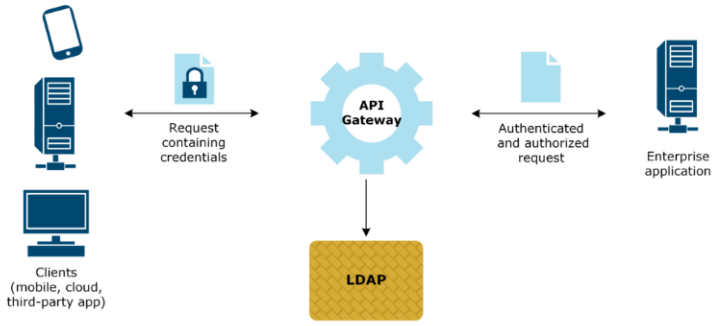

Ilustración 1.LDAP

Es un protocolo de la capa de aplicación TCP/IP que permite el acceso a un servicio de directorio ordenado y distribuido, para buscar cualquier información en un entorno de red.

Generalmente un servidor LDAP se encarga de almacenar información de autenticación, es decir, el usuario y la contraseña, para posteriormente dar acceso a otro protocolo o servicio del sistema.

Características:

- Modelo de Datos: LDAP utiliza un modelo jerárquico basado en árboles, donde la raíz del árbol puede representar la organización, y los nodos pueden representar unidades organizativas, usuarios, etc.
- Autenticación: LDAP no se encarga directamente de la autenticación de usuarios en el sentido estricto, sino que se usa para consultar datos de autenticación. Sin embargo, puede integrar métodos de autenticación como bind DN (distinguished name) y contraseñas.

- Uso Común: Se usa ampliamente en entornos corporativos para gestionar la información de usuarios y proporcionar una base para la autenticación y autorización.

Funcionamiento de un servidor LDAP

El funcionamiento de LDAP es bastante sencillo, ya que la comunicación es como cualquier otra comunicación entre un cliente y un servidor, tal y como ocurre en Windows con el Directorio Activo.

Los tres pasos más importantes de la comunicación:

- El cliente se conecta al servidor LDAP (el proceso se llama Directory System Agent) a través del puerto TCP/IP 389 para empezar la sesión LDAP.
- Se establece una conexión entre el cliente y el servidor.
- Se intercambian datos entre el servidor y el cliente.

Las dos acciones básicas que puede hacer un cliente al conectarse son dos:

- Leer información: para leer la información el cliente debe autenticarse, entonces intentará leer y obtener información del directorio, antes de realizar este paso el servidor se encargará de comprobar si ese usuario en concreto tiene la autorización de leer información.
- Modificar información: para modificar información el proceso es el mismo, pero el servidor comprobará si tenemos permisos de modificación en el servidor.

LDAP también nos permite intercambiar información entre varios servidores, si en un servidor nos autenticamos y éste no tiene la información necesaria, se puede realizar esta consulta a otro servidor que tengamos en la misma red local, para comprobar si efectivamente tenemos esta información o no. Es algo parecido a lo que ocurre con los servidores DNS, que van preguntando uno a otro subiendo por el árbol hasta llegar a los root servers. (Luz, 2024)

RADIUS (Remote Authentication Dial-In User Service)

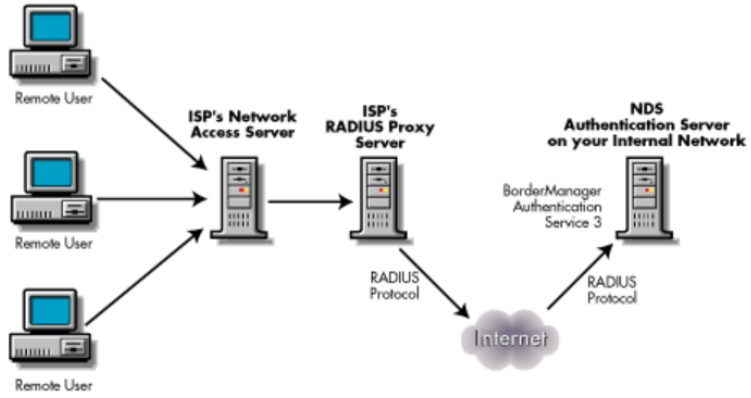

Ilustración 2.RADIUS

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Básicamente es un software de dominio público que identifica usuarios que acceden de forma remota a un servidor, permitiendo asignarles direcciones de red de forma dinámica. (Pablo Dafontes Iglesias)

Características:

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

- Autenticación y Autorización: RADIUS maneja la autenticación de usuarios y puede también gestionar la autorización al determinar qué servicios están disponibles para el usuario autenticado.
- Contabilidad: RADIUS puede realizar un seguimiento de las actividades del usuario, como el tiempo de conexión y el uso de recursos.
- Protocolo UDP: Utiliza UDP (User Datagram Protocol) para la comunicación entre el cliente RADIUS y el servidor RADIUS, lo que puede afectar la fiabilidad en comparación con protocolos basados en TCP.
- Uso Común: Es común en redes inalámbricas, acceso remoto, y VPNs (Redes Privadas Virtuales).

Proceso de autenticación

Los pasos que tiene que seguir un usuario para demostrar su identidad a través de este acceso son los siguientes:

1. El usuario llama al RAS y le comunica nombre de usuario y password, iniciando las negociaciones PPP. RADIUS 10
2. En esta etapa RAS actúa sólo como intermediario, pasando la información de autenticación al RADIUS Server.

3. Si RADIUS puede autenticar al usuario emite una respuesta de aceptación, junto con la información requerida por el RAS para dar vía libre a la conexión (IP, NetWare Network number). Si no puede autenticar al usuario, le envía una notificación con el motivo.
4. Con la información remitida por RADIUS, RAS completa la negociación PPP, permitiendo la conexión a la red o denegando el acceso (Pablo Dafontes Iglesias)

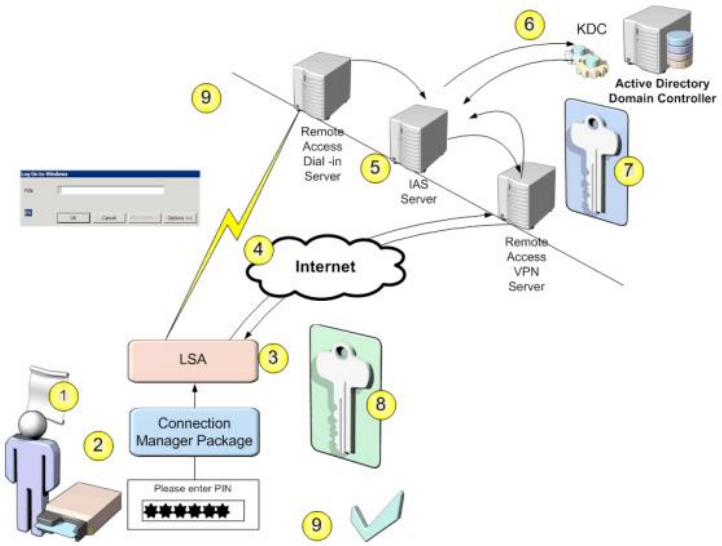

Ilustración 3.Proceso de Autenticación Radius

TACACS+ (Terminal Access Controller Access-Control System Plus)

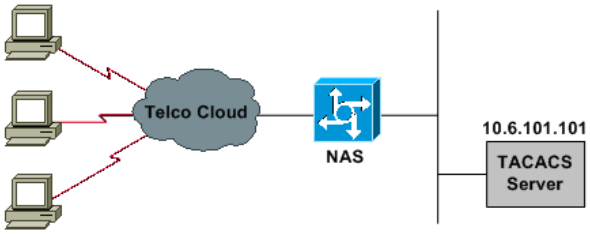

Ilustración 4.TACACS

Es un protocolo de autenticación de red que ofrece una solución para el control de acceso y la gestión de sesiones de usuarios en dispositivos de red. A diferencia de RADIUS, TACACS+ proporciona una separación más clara entre autenticación, autorización y contabilidad.

Características:

- Autenticación, Autorización y Contabilidad: TACACS+ gestiona la autenticación de usuarios y la autorización de sus accesos, además de proporcionar contabilidad.

- Protocolo TCP: Utiliza TCP (Transmission Control Protocol) para asegurar la entrega fiable de los datos.
- Encriptación: TACACS+ encripta toda la comunicación entre el cliente y el servidor, proporcionando una mayor seguridad en comparación con RADIUS, que solo encripta las contraseñas.
- Uso Común: Se usa principalmente en entornos donde se necesita una administración detallada y segura de los accesos a los dispositivos de red.

Kerberos

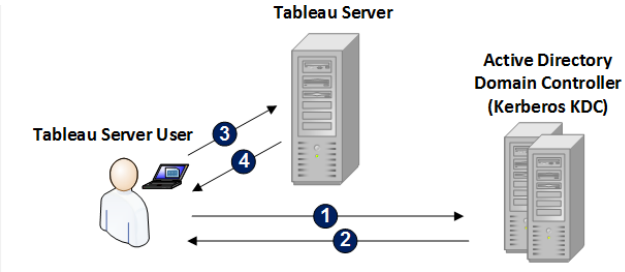

Ilustración 5.Kerberos

Es un protocolo de autenticación de red que utiliza criptografía para proporcionar autenticación de usuarios y servicios en una red insegura. Fue desarrollado en el MIT como parte del proyecto Athena y se basa en el concepto de "tickets" para autenticar a los usuarios.

Características:

- Modelo de Tickets: Los usuarios reciben un "ticket" de autenticación del servidor de autenticación Kerberos (KAS). Este ticket es luego presentado a los servicios que el usuario quiere usar para obtener un "ticket de servicio" que permite el acceso.
- Criptografía: Utiliza criptografía simétrica para la autenticación de usuarios y servicios, asegurando que las contraseñas no se transmitan a través de la red.
- Servidores de Kerberos: Incluye un servidor de autenticación (AS) y un servidor de concesión de tickets (TGS), además de los servicios que proporcionan acceso.
- Uso Común: Ampliamente utilizado en entornos Windows Active Directory y en sistemas UNIX/Linux para manejar la autenticación de red de manera segura y eficiente.

Servicios de autorización

ACL (Access Control List)

Son un mecanismo de autorización que define qué usuarios o grupos tienen acceso a un recurso específico y qué tipo de acceso tienen (lectura, escritura,

ejecución, etc.). Las ACL se aplican a nivel de objeto (por ejemplo, archivos, directorios, impresoras) y especifican permisos para cada usuario o grupo.

Características:

- Listas de Permisos: Cada recurso tiene una lista asociada que contiene entradas para cada usuario o grupo y sus permisos correspondientes.
- Estática: Las ACL son generalmente estáticas, es decir, los permisos no cambian dinámicamente en función de atributos contextuales.
- Control de Acceso Granular: Permite especificar permisos precisos para diferentes usuarios o grupos en recursos individuales.

Ventajas:

- Simplicidad: Fácil de implementar y entender, especialmente para sistemas de archivos y recursos simples.
- Granularidad: Ofrece un control detallado sobre el acceso a recursos específicos.
- Compatibilidad: Ampliamente soportado por muchos sistemas operativos y aplicaciones.

Desventajas:

- Escalabilidad: Puede ser difícil de gestionar a gran escala debido a la complejidad de mantener listas extensas.
- Rigidez: Menos flexible en comparación con otros modelos de control de acceso, ya que los permisos no se adaptan a contextos dinámicos.
- Gestión: Requiere una administración manual de las listas, lo que puede llevar a errores y inconsistencias.

RBAC (Role-Based Access Control)

Es un modelo de autorización en el que el acceso a los recursos se controla mediante roles definidos en el sistema. Los usuarios se asignan a roles y cada rol tiene permisos específicos asociados.

Características:

- Roles Definidos: Los permisos se asignan a roles en lugar de a usuarios individuales. Los usuarios adquieren permisos al ser asignados a roles.
- Permisos Basados en Roles: Los roles tienen permisos específicos para realizar ciertas acciones.
- Jerarquía de Roles: Los roles pueden tener jerarquías y heredar permisos de otros roles.

Ventajas:

- Escalabilidad: Facilita la gestión de permisos en grandes organizaciones al permitir la administración centralizada de roles.
- Simplificación: Reduce la complejidad al asociar permisos a roles en lugar de a usuarios individuales.
- Consistencia: Asegura que los usuarios con el mismo rol tengan el mismo nivel de acceso.

Desventajas:

- Rigidez: Puede no ser flexible suficiente para situaciones donde el acceso depende de condiciones dinámicas o contextuales.
- Rol Dinámico: La asignación de roles y permisos puede volverse compleja en organizaciones con múltiples roles y jerarquías.
- Cambio de Rol: Cambios en la estructura de roles pueden requerir ajustes significativos en los permisos.

ABAC (Attribute-Based Access Control)

El Control de Acceso Basado en Atributos (ABAC) utiliza atributos de sujetos (usuarios), objetos (recursos) y el contexto (como la hora del día) para tomar decisiones de acceso. Las políticas de acceso son definidas mediante una combinación de estos atributos.

Características:

- Políticas Basadas en Atributos: Las decisiones de acceso se basan en atributos de los usuarios, recursos y el contexto de la solicitud.
- Flexibilidad: Permite una gestión más dinámica y contextual del acceso.
- Reglas Complejas: Las políticas pueden ser complejas y expresadas mediante combinaciones de atributos.

Ventajas:

- Flexibilidad y Dinamismo: Permite la implementación de políticas de acceso complejas y adaptativas basadas en una variedad de atributos.
- Contexto: Puede considerar el contexto en el que se realiza una solicitud de acceso (hora, ubicación, etc.).
- Granularidad: Ofrece una gestión de permisos muy detallada y específica.

Desventajas:

- Complejidad: La configuración y gestión de políticas puede ser compleja y requiere un entendimiento detallado de los atributos y sus combinaciones.
- Rendimiento: Las decisiones de acceso pueden requerir evaluaciones complejas que impacten el rendimiento.

- Requerimientos Técnicos: Puede requerir soporte especializado y herramientas avanzadas para su implementación.

PBAC (Policy-Based Access Control)

Es un modelo que se basa en políticas definidas para autorizar el acceso a los recursos. Estas políticas definen reglas que determinan si un acceso debe ser concedido o denegado, y pueden basarse en una combinación de atributos y condiciones.

Características:

- Políticas Definidas: Las decisiones de acceso son tomadas según políticas predefinidas que pueden considerar diversos factores.
- Reglas: Las políticas pueden incluir reglas sobre quién puede acceder a qué, bajo qué condiciones.
- Adaptabilidad: Las políticas pueden ser ajustadas y actualizadas para adaptarse a nuevas necesidades.

Ventajas:

- Flexibilidad: Permite la definición de políticas detalladas y adaptables para gestionar el acceso.
- Centralización: La gestión de acceso se realiza a través de un sistema centralizado de políticas.
- Adaptabilidad: Las políticas pueden ser modificadas para responder a cambios en los requisitos de acceso.

Desventajas:

- Complejidad en la Implementación: La creación y mantenimiento de políticas complejas puede ser difícil y requiere una planificación detallada.
- Evaluación de Políticas: La evaluación de políticas puede impactar el rendimiento del sistema, especialmente si las políticas son muy detalladas.
- Requerimientos de Herramientas: Puede necesitar herramientas y plataformas especializadas para gestionar políticas de acceso eficientemente.

Conclusión

Los servicios de autenticación y autorización permiten a las organizaciones implementar un control de acceso robusto y adaptable, Integrar estos servicios de manera efectiva ayuda a garantizar la seguridad, la eficiencia operativa y el cumplimiento de las políticas internas y normativas externas, protegiendo así la integridad y confidencialidad de los datos y recursos.

Bibliografía

Luz, S. D. (23 de Mayo de 2024). *Para qué sirve el protocolo LDAP y cómo funciona*. Obtenido de Redes Zone: https://www.redeszone.net/tutoriales/servidores/que-es-ldap-funcionamiento/#538404-funcionamiento-de-un-servidor-ldap

Microsoft. (s.f.). *Microsoft*. Obtenido de https://www.microsoft.com/es-mx/security/business/security-101/what-is-authentication#:~:text=La%20autenticaci%C3%B3n%20es%20el%20proceso,a%20recursos%20de%20la%20organizaci%C3%B3n.

Pablo Dafontes Iglesias, C. P. (s.f.). *RADIUS: Seguridad en Sistemas de Información.* Obtenido de http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/11%20-%20Radius.pdf