193.ldapSMB3_SMB4AD

Emilio Cabo Gomis

Sumario

¿Que es Samba?

Es una implantación del protocolo para el compartido de ficheros e impresoras de Windows, previamente conocido como SMB. Este protocolo fue lanzado en el año 1992

Mediante el modelo cliente servidor permite a un cliente Windows conectarse a un servidor Samba (Linux) . Y así poder emplear un dominio Linux como si de un dominio Windows se tratara.

Diferencias entre Samba 3 y Samba 4

En Samba 4 se han añadido soporte para Active Directory y soporte para ser el Controlador de Dominio. Es decir, el servicio de Samba 4 puede realizar las funciones de un Windows 2000 Server o superior en un dominio de Windows.

Cuando en clase realizamos la implantación del protocolo LDAP realizamos también una implantación de un servidor DNS en el mismo servidor pero es un programa externo. En nuestro caso se trata de Bind9.

En Samba 4 el empleo de un servicio de DNS que resuelva los nombres del dominio y consultas de “mas rango” que necesiten consultas a servidores DNS más arriba en la jerarquía. Está integrado dentro del servicio Samba.

En la versión de Samba 4 se incluyen todas las características de las que gozaban todas las implementaciones previas de Samba. Es decir, tiene retro-compatibilidad.

KERBEROS

No podemos hablar del protocolo SAMBA4 sin hablar del protocolo de seguridad Kerberos.

Muchos de los protocolos implementados en internet no disponen de medidas de seguridad de encriptación. Medidas de seguridad como por ejemplo un Firewall son efectivas contra atacantes externos pero no contra atacantes que se encuentran dentro de la red protegida con un Firewall.

Kerberos es un protocolo de encriptación desarrollado con la finalidad de que un cliente pueda autenticarse contra un servidor. Una vez autenticado el cliente el protocolo Kerberos encriptará todas sus comunicaciones. Garantizando tanto la privacidad como la integridad de los datos durante sus operaciones. Por lo que si un cliente conectado a la red intentara “*sniffear”* el intercambio de paquetes entre el servidor y el cliente no sería capaz.

Este protocolo es abierto, muchos productos propietarios han empleado el protocolo abierto para implementarlo en sus productos. Un ejemplo de esto son los sistemas operativos Windows Server.

Estos implementan las extensiones y el protocolo de autenticación de la versión 5 de Kerberos para la autenticación de clave pública, el transporte de datos de autorización y la delegación. El servicio de Active Directory es uno de los servicios que se goza de este nivel de encriptado.

Elementos del protocolo Kerberos

Servidor de Autenticación Kerberos → Un a vez que el cliente introduce la contraseña en su máquina, esta genera una clave "HASH" que se envía al Servidor de Autenticación. Este es el servidor contra el que el cliente se autentica. Este Genera un Ticket-Granting Ticket (TGT) si el "HASH" de la contraseña se corresponde.

Servidor emisor de Tickets → El AS demuestra al Servidor emisor de Tickets que es el usuario que dice ser mediante la autenticación del Ticket-Granting Ticket (TGT). Este envía un ticket de servicio Kerberos El (TGS (Ticket Granting Service))para demostrar al Service Server (En nuestro caso el servidor LDAP); que puede hacer uso del servicio Kerberos.

Service Server: es el componente final en el proceso de autenticación Kerberos. Este servidor proporciona el servicio solicitado por el cliente una vez que se ha autenticado correctamente. En el contexto de Kerberos, el Service Server puede ser cualquier servidor que ofrezca un servicio específico, como un servidor LDAP, un servidor de archivos, o cualquier otro servicio de red. El servicio que ofrece el Service Center se encuentra encriptado con la clave de servicio correspondiente.

Migración

Los cambios enumerados anteriormente hacen que el proceso de cambio de Samba 3 a Samba 4 hacen que el cambio de una versión a otra sea algo trabajoso.

Debemos tener claro que existen dos tipos de Migraciones de Samba 3 a Samba 4. Podemos hacer la implementación de Samba 3 a Samba 4.

La diferencia entre NT4 y Active Directory (AD) radica en varios aspectos clave:

NT4 → Utiliza un modelo de dominio simple donde cada dominio es independiente y tiene su propio conjunto de usuarios y recursos. Tiene una administración muy limitada y menos flexible. No emplea Kerberos cómo método de autenticación,, sino otro medio de autenticación de usuarios.

AD→ Utiliza una estructura jerárquica que puede incluir múltiples dominios organizados en árboles y bosques, permitiendo una administración más centralizada y escalable. Ofrece

herramientas avanzadas de administración y políticas de grupo Utiliza Kerberos como protocolo de autenticación principal.

Bibliografía

SAMBA

https://www.samba.org/samba/what_is_samba.html

KERBEROS

https://web.mit.edu/Kerberos/

ZDNET

https://www.zdnet.com/home-and-office/networking/know-the-difference-between-active-directory-and-windows-nt-4-domains/.

MICROSOFT

https://learn.microsoft.com/es-es/entra/identity/domain-services/compare-identity-solutions.

Wikipedia

https://es.wikipedia.org/wiki/Kerberos#C%C3%B3mo_funciona