Introdución e características de Samba4

Sumario

Características de Samba4

- Samba4 é unha nova versión de Samba publicada a finais do ano 2012 e que supón un cambio moi importante sobre a versión anterior.

- Como principais novidades podemos destacar:
  - ♦ Implementación dos servizos do *Active Directory* de Windows: Desta forma, o servizo de Samba4 pode realizar as funcións dun Windows 2000 Server ou superior nun dominio Windows. Para acadalo, inclúe unha implementación integrada do servizo LDAP e do servidor distribución de chaves (KDC) de kerberos.
  - ♦ Como parte integral do Directorio Activo de Windows, Samba4 precisa facer uso do servizo de DNS para poder realizar as funcións do controlador do dominio. Para facelo, permítense dúas opcións:
    - ◊ Utilizar un servizo de DNS integrado no servizo Samba4, moi útil para os casos máis simples nos que simplemente queremos ter un servidor de DNS que resolva os nomes dos equipos do dominio e redirixa o resto das peticións a servidores de DNS externos.
    - ◊ Utilizar un servidor de DNS externo, como BIND. Isto interesaranos cando precisemos funcións avanzadas do servizo de DNS que o servidor integrado en Samba4 non permita.

Introdución a Kerberos

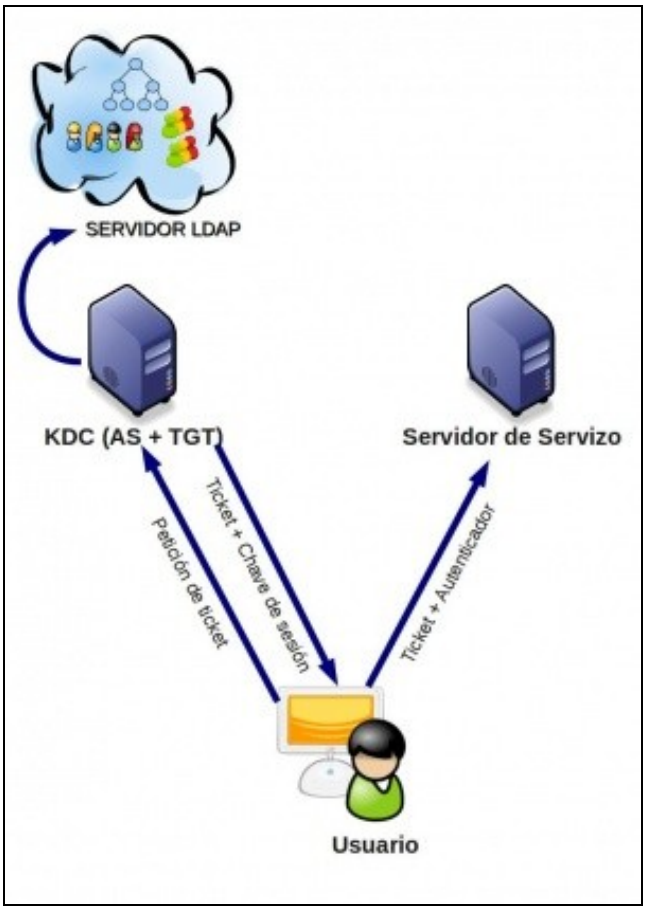
O Can Cerberos

- Dos tres principais compoñentes de Samba4 (LDAP, DNS e Kerberos), Kerberos é o único que supón unha novidade xa que ata o de agora non formaba parte dos compoñentes do noso dominio. Imos por iso a facer unha breve introdución ao funcionamento e compoñentes básicos deste protocolo.

- Kerberos (http://web.mit.edu/Kerberos) é un protocolo de autenticación, deseñado para ofrecer unha autenticación segura a aplicacións cliente-servidor baseándose en algoritmos de cifrado de chave privada.

- Recibe o seu nome do personaxe mitolóxico grego *Kerberos* (ou Can Cerberos), un monstro de tres cabezas que gardaba a porta de Hades, para que os mortos non saíran e os vivos non puidesen entrar.

- Con kerberos, o cliente pode demostrar a súa identidade ao servidor, e viceversa. Despois disto, tamén permite utilizar mecanismos de cifrado para garantir a privacidade e a integridade da información intercambiada entre eles.



Esquema do protocolo kerberos

- Os compoñentes de kerberos son os seguintes:
  - O **Centro de Distribución de Chaves** (*Key Distriibution Center* ou *KDC*) que conta con dúas partes:
    - Un **servidor de autenticación** (*Authentication Server* ou *AS*), que usa unha base de datos na que almacena os contrasinais dos usuarios (no noso caso, esta base de datos será o servidor LDAP interno de Samba4).
    - Un **servidor emisor de tickets** (*Ticket Granting Server* ou *TGS*), que lle proporcionará ao cliente o *Ticket Granting Ticket* (*TGT*) que logo lle permitirá autenticarse no servizo.
  - O **servidor do servizo** (*Service Server* ou *SS*), que autenticará ao usuario co ticket emitido polo servidor kerberos.

- O funcionamento básico do protocolo é o seguinte:
  - O cliente solicita ao *KDC* un ticket e este lle devolverá dúas pezas: en primeiro lugar a chave de sesión que cifrará co contrasinal do usuario (e así asegúrase de que só se o usuario é válido poderá descifrala) e unha segunda peza coa chave de sesión de novo e o nome do usuario (que en kerberos recibe o nome de **principal**) cifrada co contrasinal do servizo ao que se pretende acceder (Esta segunda peza recibe o nome de Ticket de Servizo).
  - O cliente descifra a chave de sesión (xa que o ticket non o pode descifrar) e úsaa para cifrar a hora actual e algunha información máis formando un paquete chamado *autenticador*. Envía este paquete xunto coa ticket ao Servidor do Servizo.
  - O Servidor do Servizo descifra o ticket co seu contrasinal, obtendo a chave de sesión e o nome do usuario (principal) que se quere conectar. Usa a chave de sesión para descifrar o *autenticador* e extraer a hora que contén, dándose por satisfeito se a hora concorda (con un certo marxe) coa actual.

- A versión actual de kerberos é a 5.

Cambios na configuración de Samba4 con respecto a Samba3

- Para configurar un equipo con Samba4 como controlador de dominio en modo de directorio activo haberá que realizar un proceso de promoción (*provision*) do servizo a controlador de dominio onde se inicializarán as estruturas no LDAP, DNS e Kerberos necesarias para esta función (Proceso similar ao que se segue nun Windows Server para inicializar o Directorio Activo).

- Este proceso faise coa ferramenta **samba-tool**, ferramenta que tamén se utiliza para a configuración de múltiples aspectos do servizo de Samba4 (usuarios e grupos, políticas de contrasinais, DNS, políticas de grupo, etc.).

- Ademais, moitos aspectos de Samba4 pódense configurar utilizando as ferramentas de Windows de configuración do Directorio Activo (Ferramentas de Administración Remota do Servidor ou *RSAT*), que son as ferramentas que se utilizan para administrar un dominio Windows con un Windows Server como controlador de dominio.

Samba3 ou Samba4?

- Con toda esta información, a pregunta que cabe facernos é a seguinte. Por que opción optamos se queremos montar un dominio? Samba3 (ou Samba4 en modo NT4) ou Samba4 (en modo de directorio activo)?

- É evidente que Samba4 é unha versión que amplía e mellora as características de Samba3, e polo tanto acabará reemprazándoo paulatinamente. Porén, hoxe en día hai algunhas cuestións importantes que levan a que non optemos por Samba4 en todos os casos. Destacamos dúas:
    - A actualización de Samba3 a Samba4 non é, nin moito menos, automática. O cambio radical na estrutura do servizo fai que sexa necesario un proceso de migración (documentado en https://wiki.samba.org/index.php/Samba_Classic_Upgrade_%28NT4-style_domain_to_AD%29) e fará que teñamos que valorar no caso de que teñamos un dominio con Samba3 en produción se nos interesa ou non facer esa migración a Samba4.
    - A imposibilidade de usar un LDAP externo (da mesma forma que si podemos facer so servizo DNS), resulta un aspecto moi importante que pode facer que o cambio ou a implantación dun dominio con Samba4 non nos interese en función das circunstancias. O servidor LDAP incluído en samba non é unha implementación nin tan completa nin tan madura como pode ser OpenLDAP, e se temos outros servizos que usan o servizo de LDAP para a autenticación de usuarios pode ser que non funcionen correctamente con Samba4.

- En conclusión, se precisamos unha configuración máis avanzada do servidor LDAP para a autenticación de diversos servizos e os clientes Windows non teñen un peso moi importante, é moi probable que nos interese optar por un dominio con Samba3 e OpenLDAP. Pola contra, se buscamos opcións máis avanzadas de administración para os cliente Windows (políticas de grupo, políticas de contrasinais, etc.) e ferramentas de administración do dominio máis completas, seguramente Samba4 sexa a mellor opción.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez