Introdución a kerberos

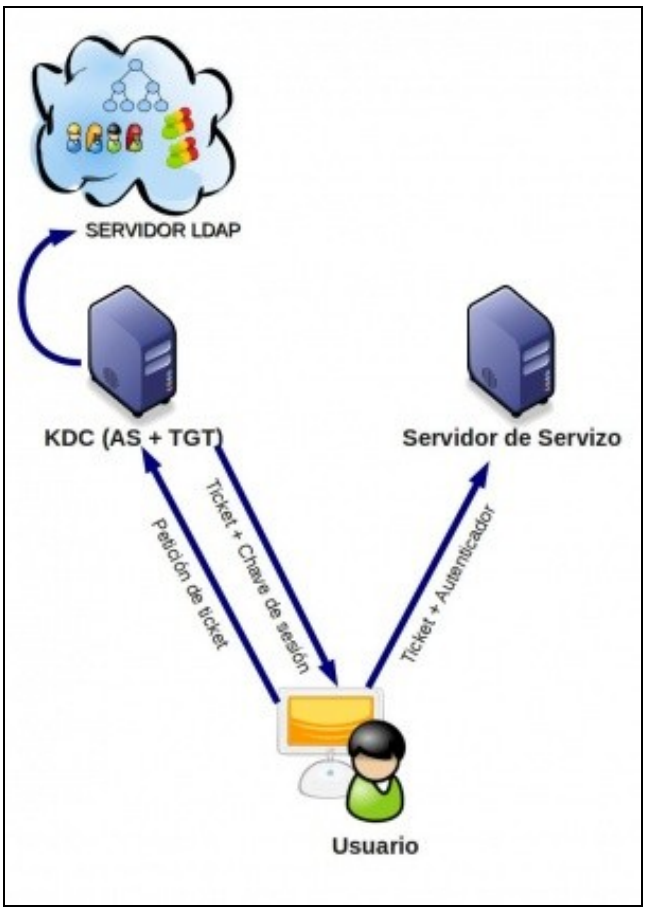


O Can Cerberos

- 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 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).
    - 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 descrifrar) 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.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez