一、介绍

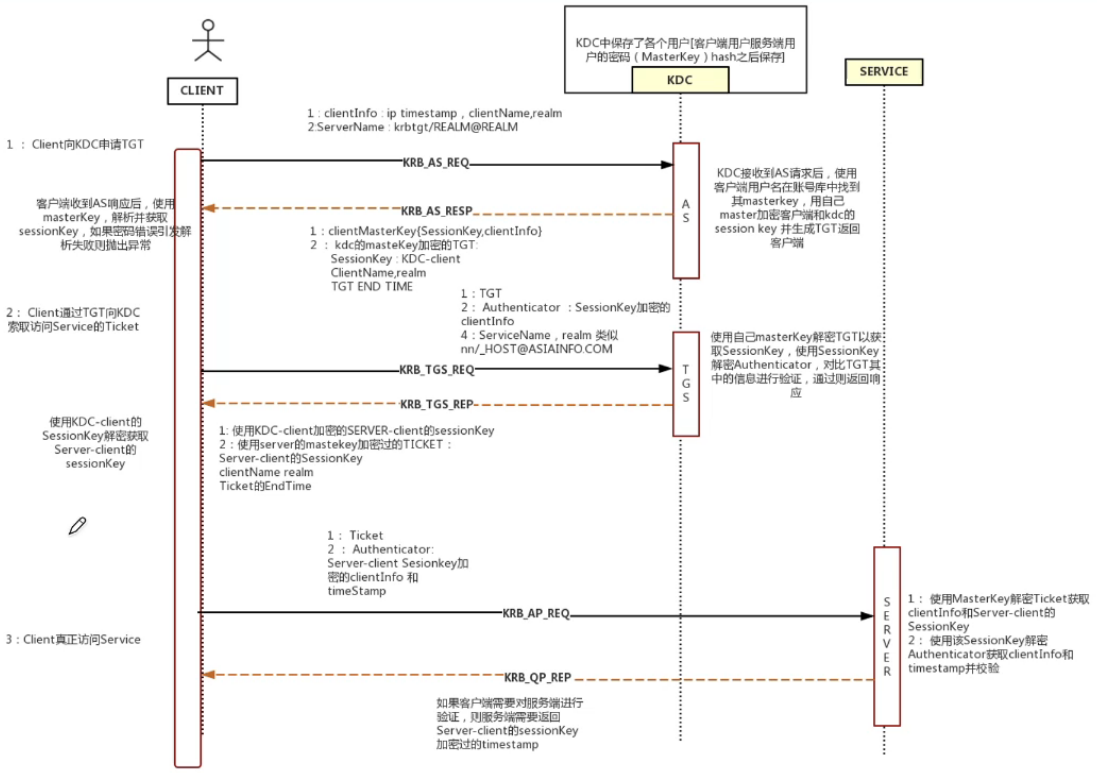
1、简介

Kerberos协议，允许某实体在非安全网络环境下通信，向另一个实体以一种安全的方式证明自己的身份。它的设计主要针对C/S（客户/服务器）模型，并提供了一系列交互认证--用户和服务器都能验证对方的身份。

2、功能

可用于保护网络实体免受窃听和重复攻击，基于对称密码学，并需要一个值得信赖的第三方。

二、协议框架



三、认证流程

1、相关概念

AS(Authentication Server)	认证服务器
KDC(Key Distribution Center)	密钥分发中心
TGT(Ticket Granting Ticket)	票据授权票据，票据的票据
TGS(Ticket Granting Server)	票据授权服务器
SS(Service Server)	特定服务提供端

2、形象化理解

1、张三需要用粮票去买粮，去买粮时需要证明你是你
2、先去认证中心证明你是你，认证中心开证明单（TGT）
3、拿着证明单（TGT）去粮票中心领取粮票，通过证明单认证你是你，发放粮票（ST）
4、拿着粮票（ST）去生活物资供给处领取粮食

四、协议缺陷

1、需要中心服务器的持续响应，当Kerberos服务器宕机时，没有人可以连接到服务器
2、Kerberos要求参与通信的主机的时钟同步。票据具有一定有效期
3、所有用户使用的密钥都存储在中心服务器中，危及服务器的安全的行为将危及所有用户的密钥
4、一个危险客户机将危及用户密码