CRH安全多租户系统

——邢为栋

组成

01

Kerberos

02

Ranger

Kerberos简介

麻省理工研发了网络认证协议，该协议以希腊神话中的三头守卫神犬kerberos命名

Kerberos网络认证协议可用于防窃听、防replay攻击、保护数据完整性等场合

而其主要特征便是访问控制

kerberos的三个头

Client

发出请求
客户端

KDC

密钥分配中心
（Key
Distribution
Center）

Server

接收请求
服务端

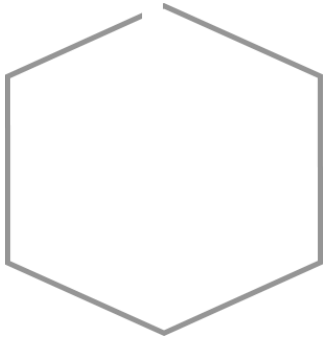
KDC

Client-A

A/Passwd——>key

Client-D

D/Passwd——>key



Client-B

B/Passwd——>key

Server-E

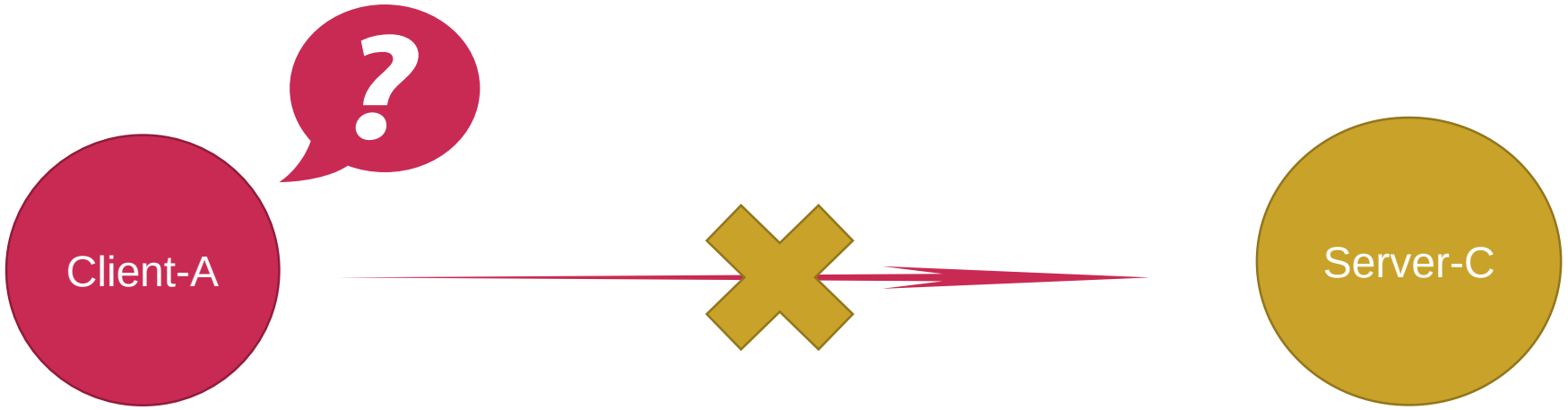
E/Passwd——>key

Server-C

C/Passwd——>key

.....

.....


?
Client-A
Server-C

Client-A：嘿！C，借我一支笔

。。。。。。

Client-A：嘿！C

Server-C：干嘛

Client-A：借我一支笔

Server-C：你谁啊

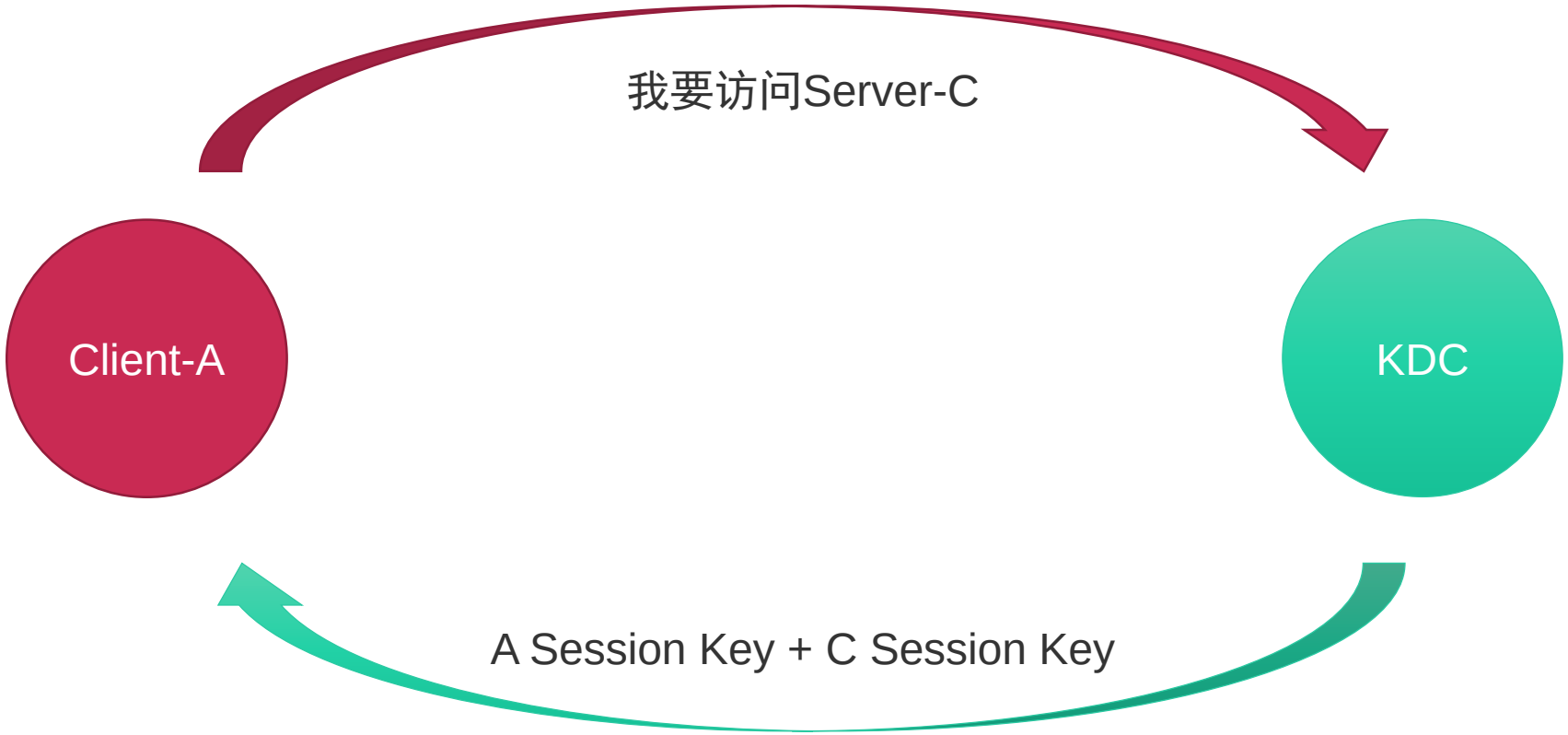
Client-A：对啊，我谁

Server-C：你说你是A 啊，拿出证明来

Client-A：证明？

Client-A（心想）：是 呢


我从哪里来
我是我，但我
又是谁
我到哪里去
Client-A
我现在在
干嘛
想起来了，我要找C借一支笔，但是
我得证明我是我，看来得找人了


我要访问Server-C
Client-A
KDC
A Session Key + C Session Key

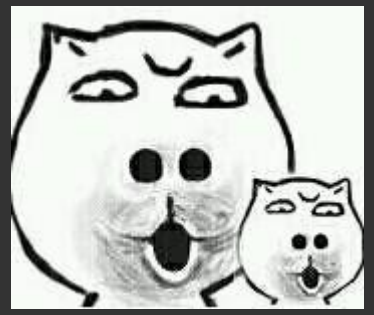
Client-A：嘿！KDC，我是A，我要找C借一支笔，你给我个证明

KDC：哦，是A啊，稍等

Client-A：你相信我是A？

KDC：你说你是A，我就认为你是A咯。这里是两个带锁的盒子，红色的是A的，黄色的是C，A的钥匙可以打开A的盒子，C的钥匙可以打开C的盒子。用A的钥匙打开A的盒子后，将A的一些信息放进去，然后和C的盒子一起交给C，等到C验证信息后，相信你是A了，就会把笔借给你了

Client-A：




Client-A
我带着证明来了
Server-C

Ranger简介

Ranger，Hadoop生态森林的护林员

Ranger旨在为企业Hadoop生态系统提供全方位的安全访问

在企业大数据应用中，潜在的是在多租户环境下运行多个任务，那么必然出现资源隔离与共享的需求，而Ranger便是因此而生

Ranger可以提供访问控制策略，这些策略可以可以控制到文件、文件夹、数据库、表以及列

并且，Ranger还拥有深度审计功能

Ranger主要构成

admin portal

提供给安全管理员的中心界面。

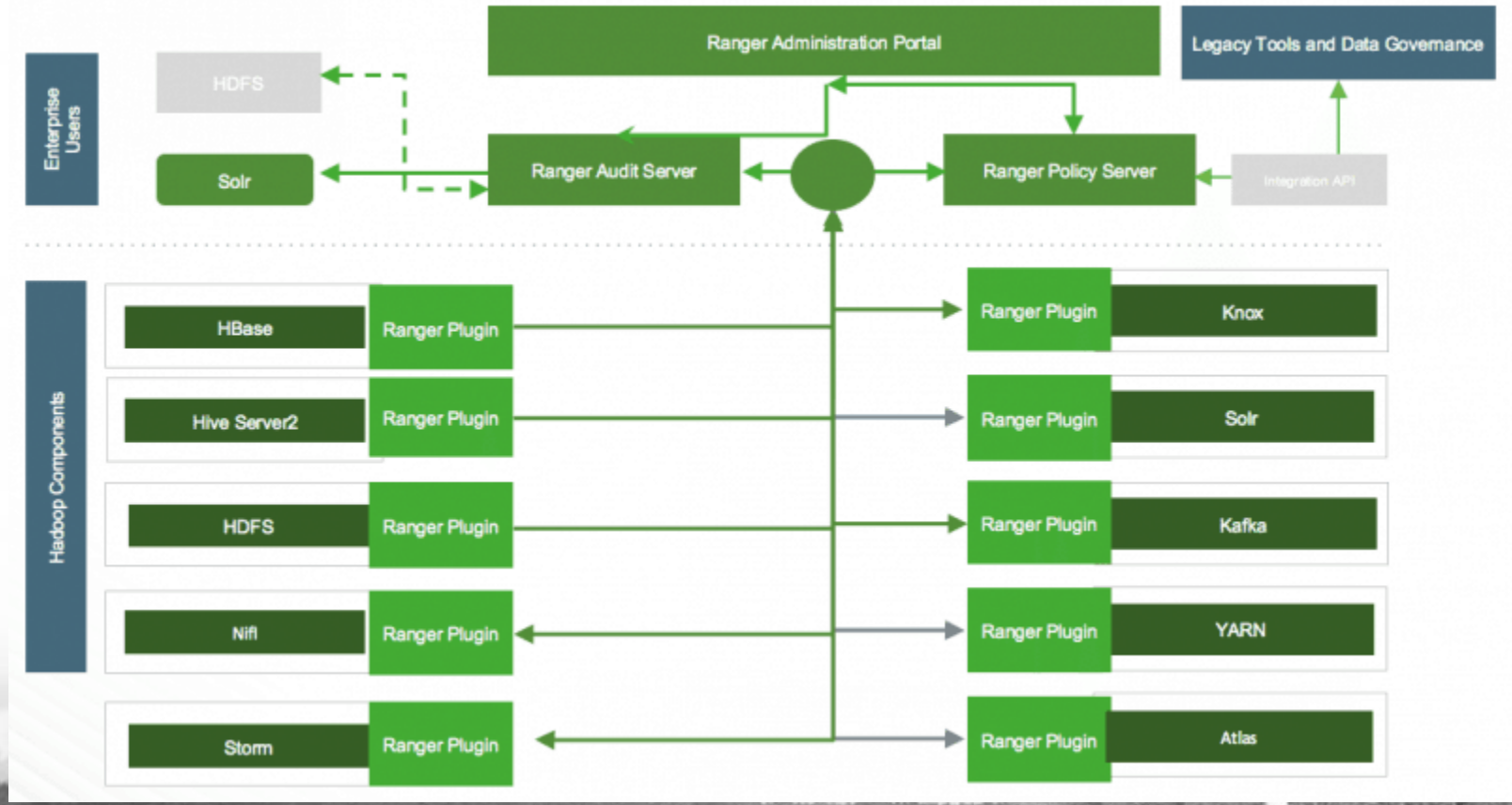
User group sync

提供一个用户同步功能用来获取来自Unix，LDAP或者Active Directory的用户和组

Plugins

轻量级的Java程序，内嵌到每个集群组件的进程中

原理图


Ranger Administration Portal
Legacy Tools and Data Governance
Enterprise Users
HDFS
Solr
Ranger Audit Server
Ranger Policy Server
Integration API
Hadoop Components
HBase
Ranger Plugin
Hive Server2
Ranger Plugin
HDFS
Ranger Plugin
Nifi
Ranger Plugin
Storm
Ranger Plugin
Ranger Plugin
Knox
Ranger Plugin
Solr
Ranger Plugin
Kafka
Ranger Plugin
YARN
Ranger Plugin
Atlas

HDFS文件访问

场景：现在有一个用户D，这个用户想要访问HDFS文件系统上的目录CRH，但是CRH目录的用户及用户组是hdfs:hdfs，那么用户D如果想在CRH目录下读写文件就会受到权限被拒绝的限制，这时，用户D就去找Ranger安全管理员，请求对CRH目录的读写权限，然后Ranger安全管理员就给用户D生成一个策略来保证这个权限，之后，用户D就可以在CRH目录下读写文件了

场景模拟

访客——用户D

访客D的朋友——用户hdfs

生态公园——HDFS文件系统

生态公园入口——CRH目录(hdfs:hdfs)

CRH区域景观——CRH目录下的文件及文件夹

HIVE数据库访问

场景：HIVE仓库现在有一个数据库CRH，数据库CRH里面有一张表redoop，表redoop里面有一个列name

现有一用户E根据需求，需要通过jdbc访问数据库CRH中表redoop的列name，但是用户E直接访问列name，会受到权限被拒绝的限制，因此，用户E需要向Ranger安全管理员申请权限，来访问列name

场景模拟

访客——用户E

生态公园——HIVE仓库

交通工具——jdbc

生态公园入口——CRH数据库

CRH区域景观——CRH数据库下的表

景观特定区域——redoop表

特定的树——name列


THANK YOU