

大数据安全实践

演讲大纲

- 安全问题背景
- 魅族大数据安全标准体系
- 魅族大数据平台安全架构
- 大数据安全技术
 - 魅族大数据安全技术体系
 - 用户认证与管理
 - 精细化权限控制
 - 元数据管理
 - 数据加密与密钥管理
 - 监控管理
- 魅族大数据安全管理系统
 - 通用权限系统产品架构设计与展示
 - 安全审计系统产品架构设计与展示
- 总结与展望

安全问题背景

数据、平台、业务快速发展

日新增行为记录	> 430亿	包括ERP、固件及80+业务线
日新增数据量	> 70TB	每年4~6x增长
数据规模	> 30PB	近4年累积
集群设备规模	2000+	Hadoop + Spark + HBase...

令人 烦恼 的安 全问 题

安全规范不完善

存在诸多安全漏洞

没有认证系统

不能够精细化控制数据权限

没有对数据进行透明有效管理

非法查阅敏感数据

异常非法操作（攻击者的挑战）

.....

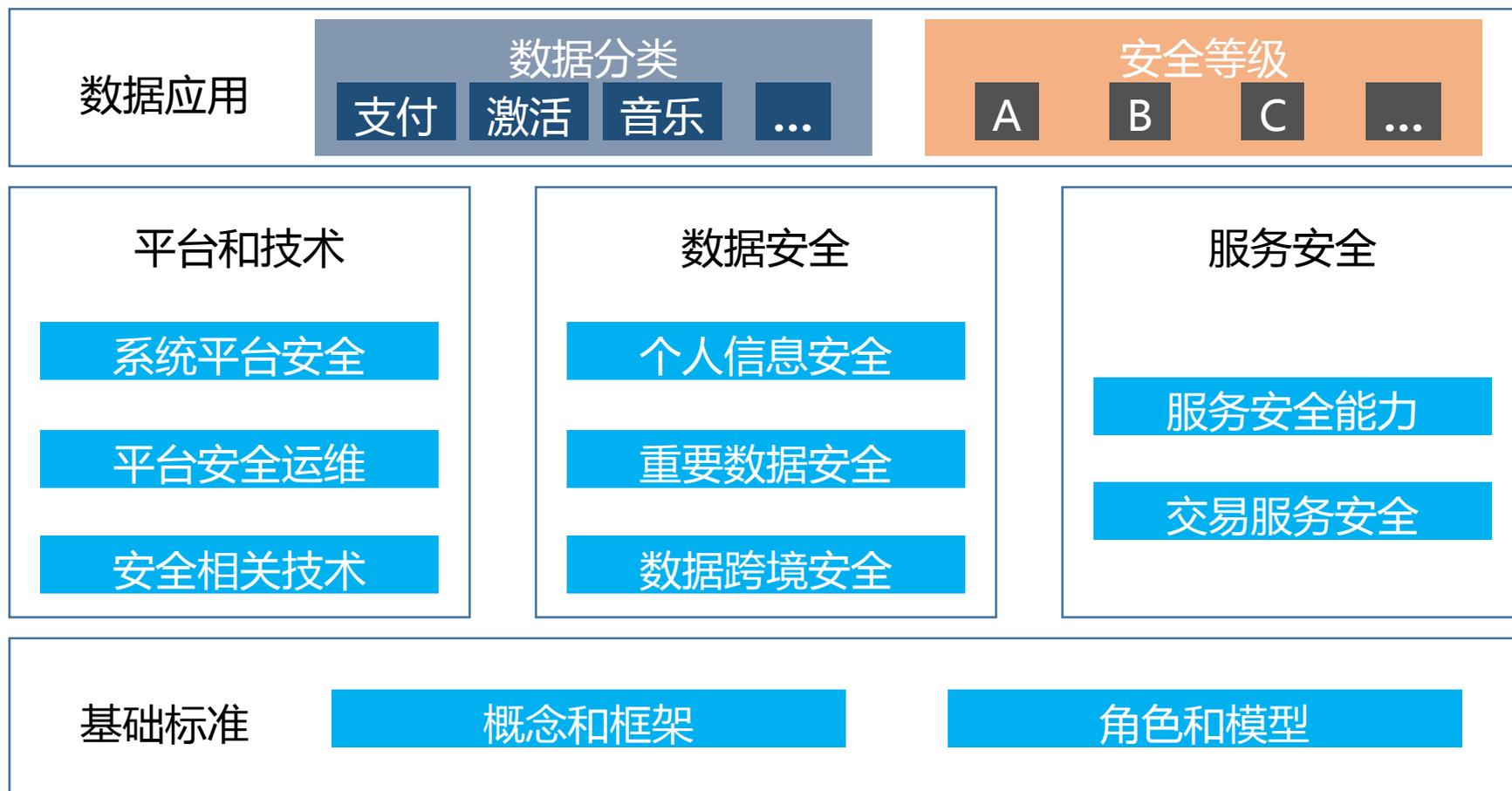
安全问题背景

大数据安全及标准化纳入国家发展战略

2017年4月，全国信息安全标准化技术委员会2017年第一次工作组“会议周”在武汉召开。会上，《**大数据安全标准化白皮书**》正式发布。

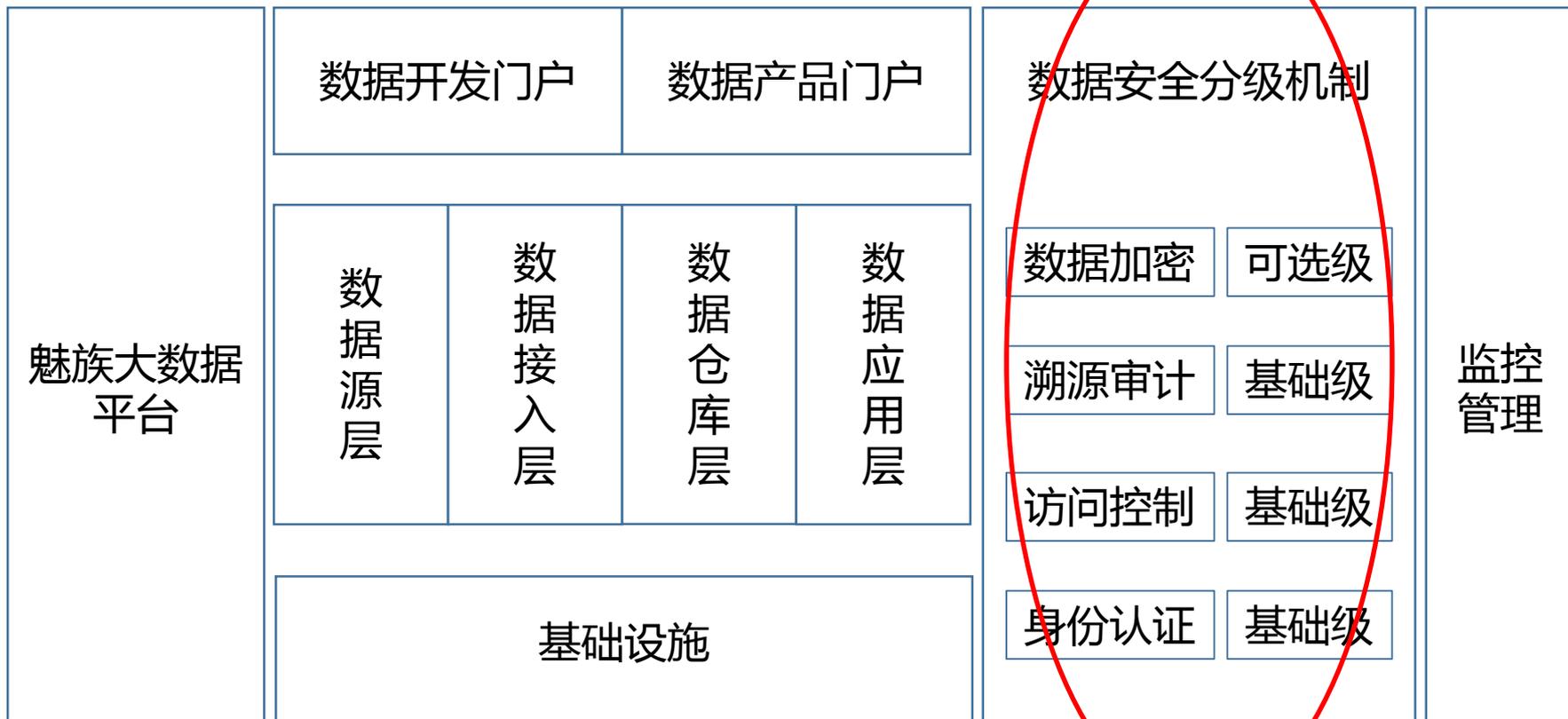
大数据安全标准体系

魅族大数据安全标准体系



大数据平台安全架构

魅族大数据平台安全架构

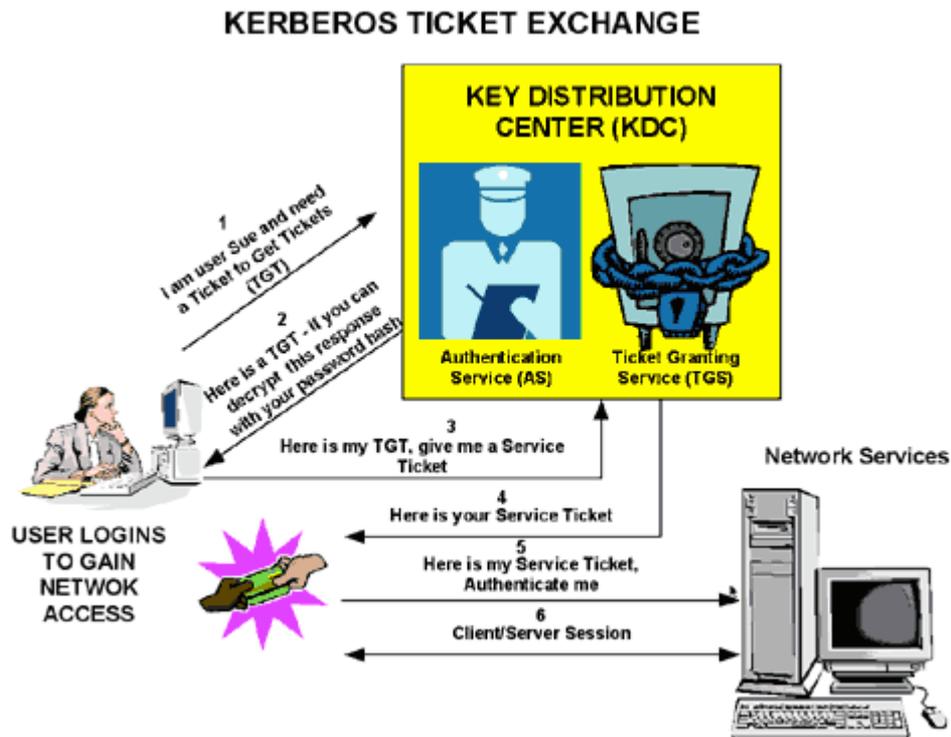


大数据安全技术

魅族大数据安全技术体系



魅族大数据安全技术体系架构 (图)



要点：

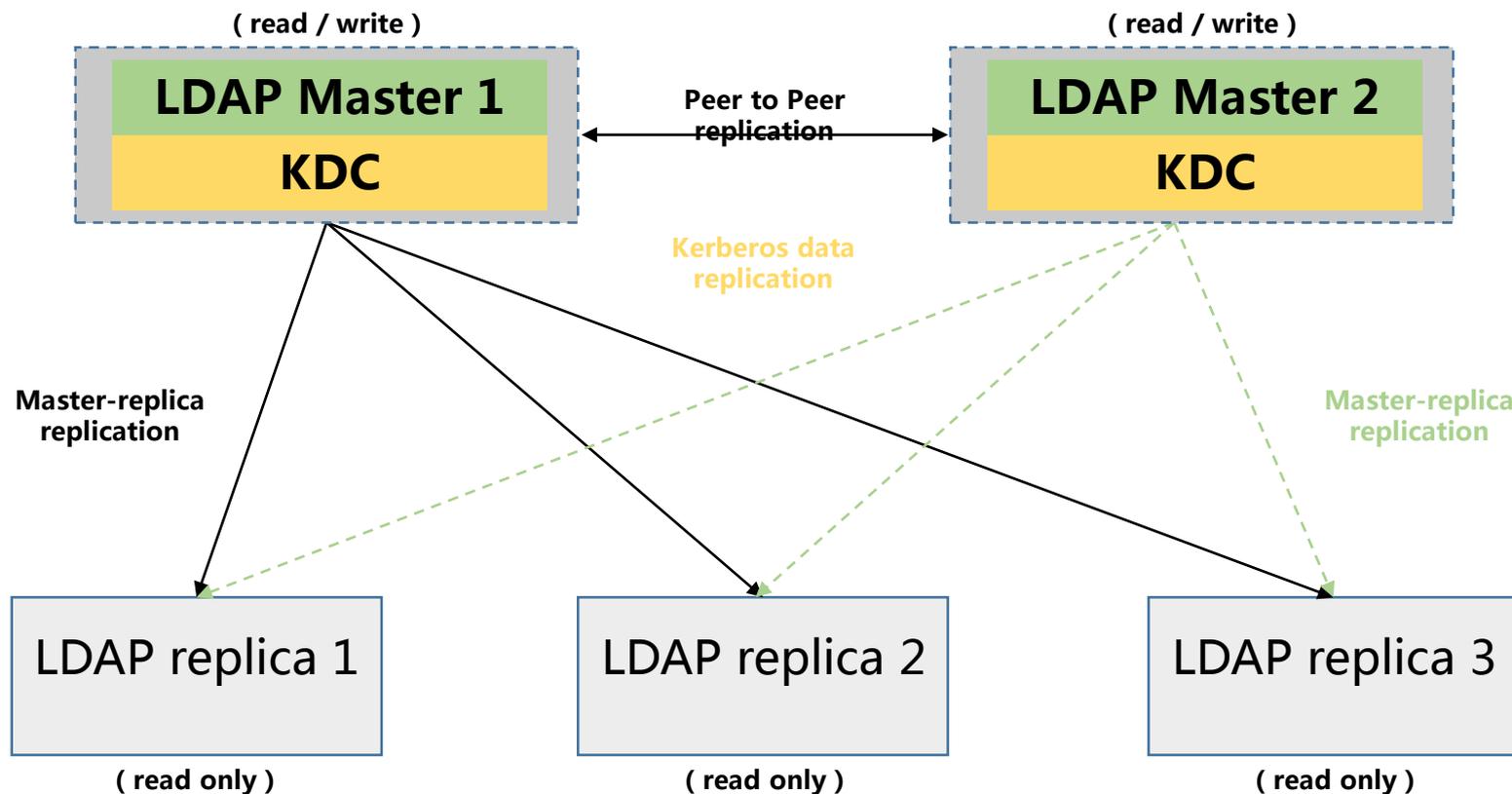
- 开源Hadoop生态原生唯一支持
- 服务器到服务器的认证
- Client到服务器的认证

不足：

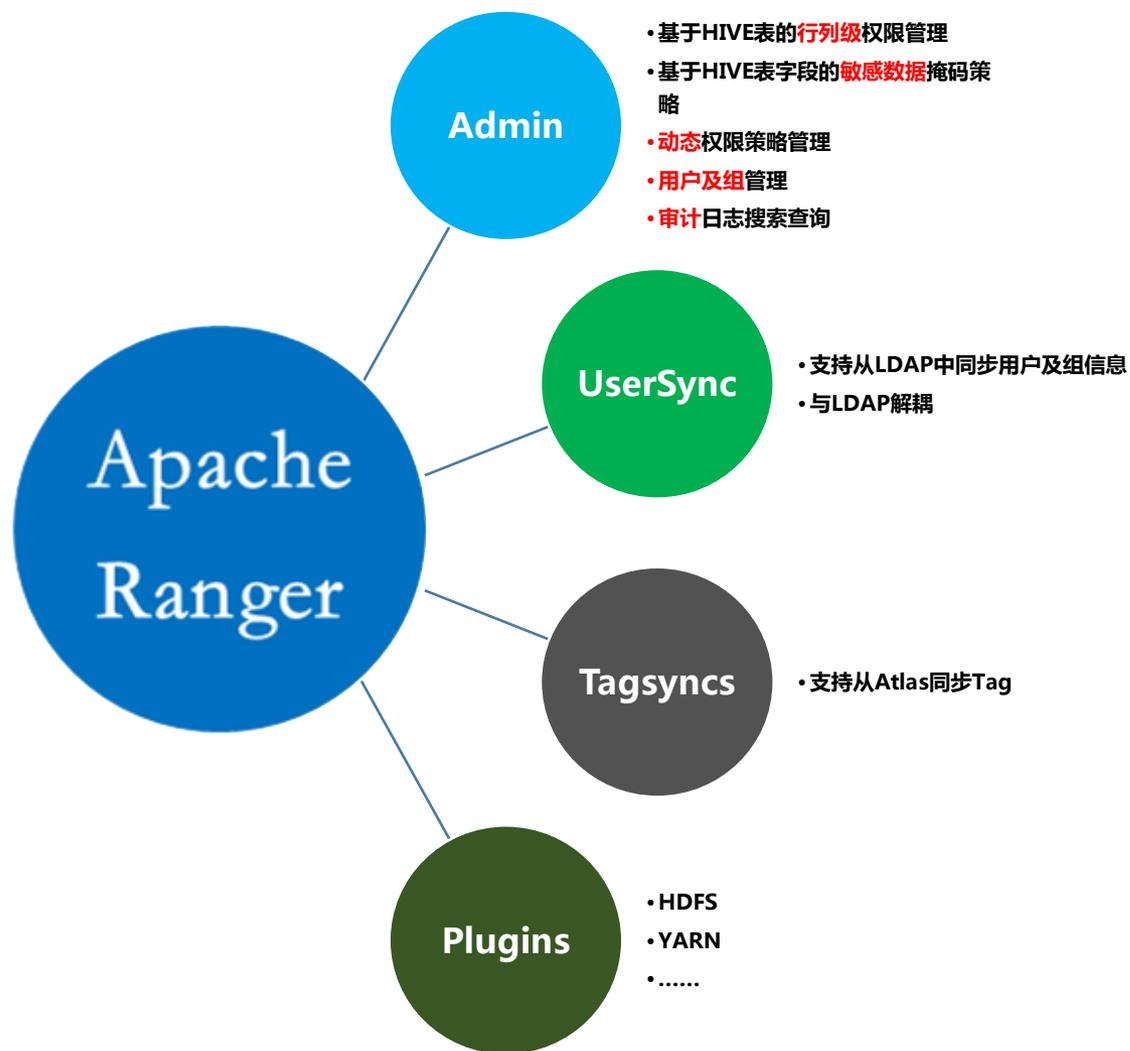
- 服务没有高可用
- 用户及组信息不能集中管理
- 缺乏JAVA API LIB

挑战：

- ◆ 运维管理（如keytab、ticket有效期）

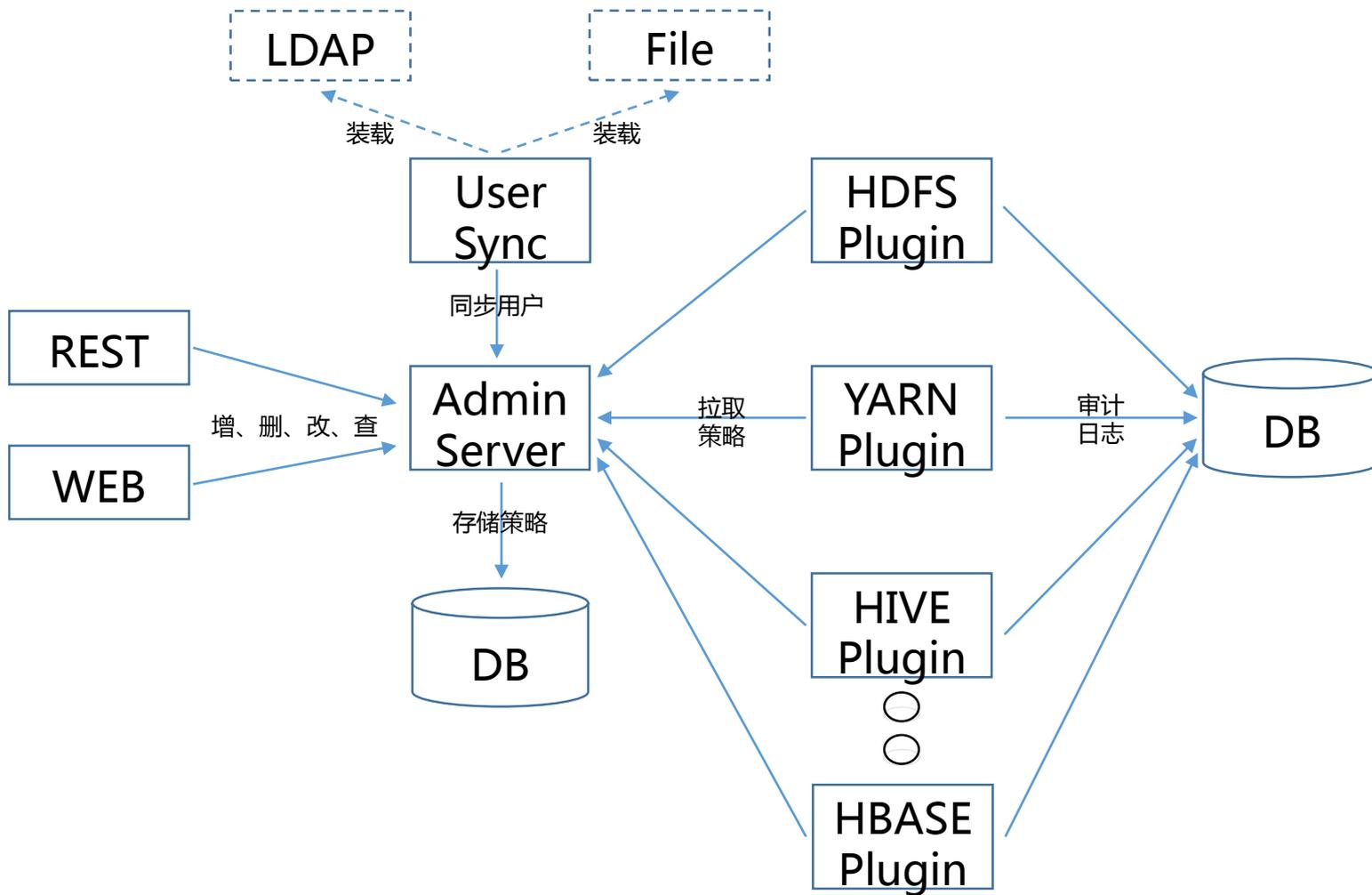


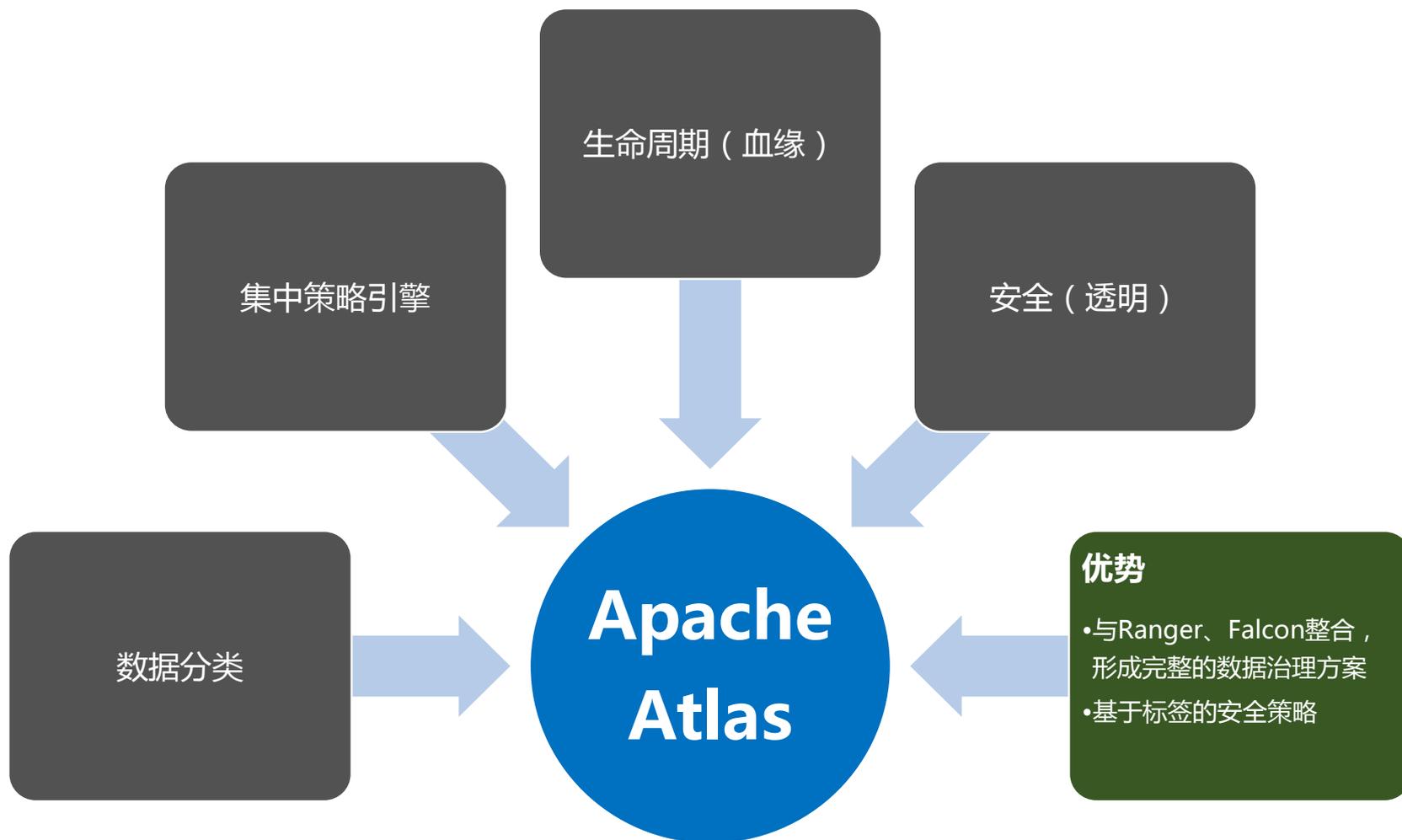
引入LDAP重点解决服务的高可用，同时兼顾性能，便利了用户及组信息的注册与管理。



大数据安全技术

精细化权限控制





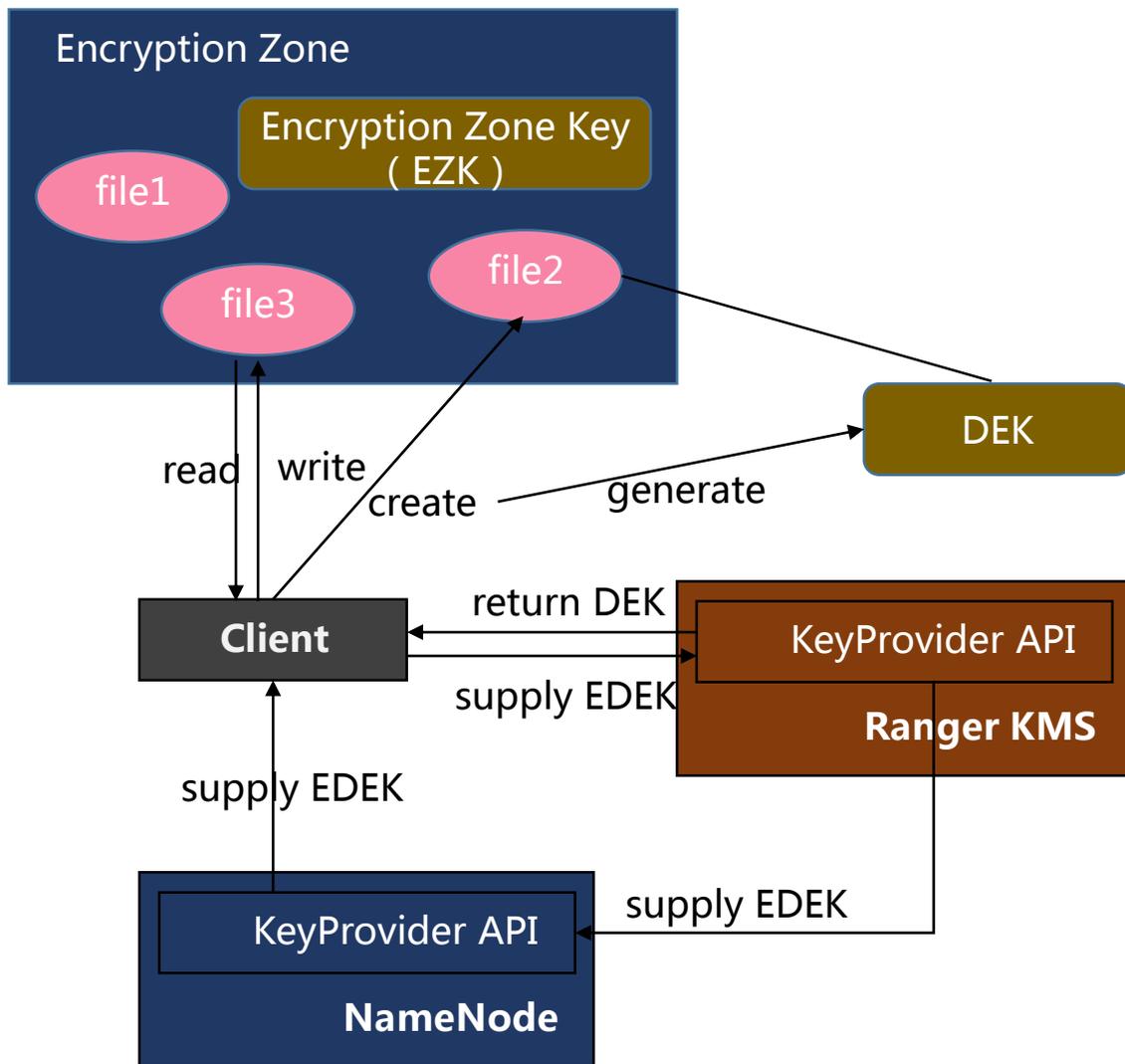
HDFS Encryption (端到端数据加、解密)

- **加密Key**
- **HDFS加密Zone**
 - 加密Zone与创建加密Zone指定的Key相关联
 - 加密Zone内的每个文件仅有唯一加密Key (DEK)
 - HDFS无法访问DEK。DN只能看到一串加密字节。HDFS将“加密数据加密密钥” (EDEK) 作为文件元数据存储>NameNode
 - Client访问KMS解密EDEK，得到DEK去读/写数据

Ranger KMS (开源密钥管理服务)

- **密钥管理**：提供对存储的加密Zone Key的 (增、删、改、查)
- **访问控制策略**：控制权限以生成或管理加密Zone Key，创建EDEK存储在HDFS
- **审计**：提供Ranger KMS访问事件的完整审计跟踪

大数据安全技术



数据加密与密钥管理

官方示例：

以普通用户的身份创建一个加密key

```
hadoop key create myKey
```

以超级用户的身份创建一个空目录,并使之成为加密空间

```
hadoop fs -mkdir /zone  
hdfs crypto -createZone -  
keyName myKey -path /zone
```

修改此目录权限为普通用户的

```
hadoop fs -chown  
myuser:myuser /zone
```

以普通用户的身份进行put上传文件和cat查看文件操作

```
hadoop fs -put helloWorld  
/zone hadoop fs -cat  
/zone/helloWorld
```

大数据安全技术

监控管理

Apache Eagle核心能力：

- 监控Hadoop中的数据访问流量
- 检测非法入侵和违反安全规则的行为
- 检测并防止敏感数据丢失和访问
- 实现基于策略的实时检测和预警
- 实现基于用户行为模式的异常数据行为检测

Apache Eagle主要优势：

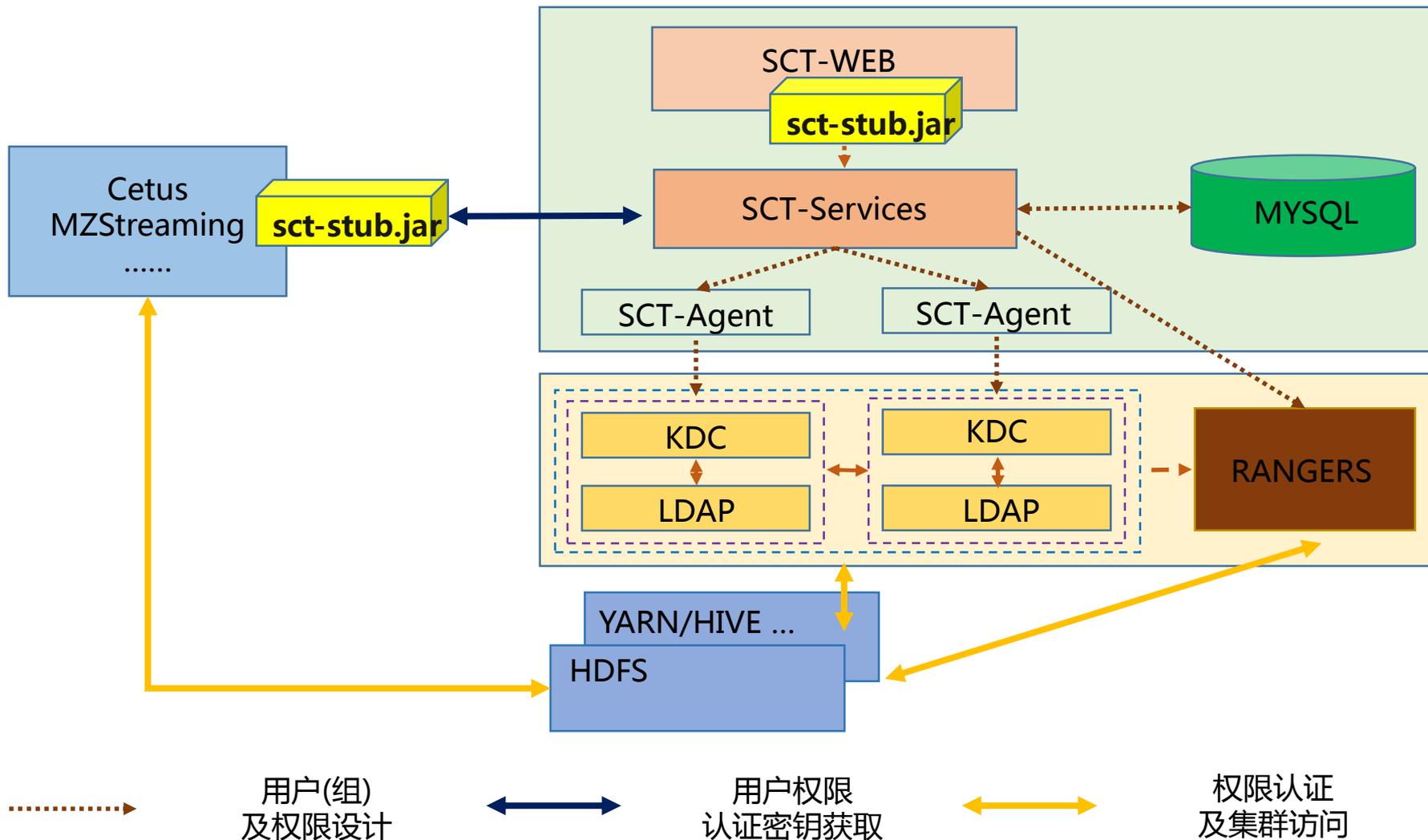
- 实时
- 易扩展
- 使用成熟的Hadoop生态技术
- 一套现成可用的告警策略规则引擎
- 机器学习算法

Apache Eagle框架概览：



魅族大数据安全管理系统

通用权限系统产品架构设计



魅族大数据安全管理系统

通用权限系统产品展示

通用权限管理平台 帮助中心

产品: 流平台

安全管理 **安全用户管理** 安全组管理 客户端管理

通用权限

权限申请

权限配置

安全管理

请输入用户名

新增用户

每页显示 15 条记录

用户名	ssCode	LDAP-DN	创建时间	操作
[redacted]	sct	uid=h[redacted]guang.ou=Pe...	2017-10-11	<input type="button" value="删除"/>
[redacted]	sct	uid=z[redacted].ou=People.d...	2017-10-11	<input type="button" value="删除"/>

通用权限管理平台 帮助中心

产品: 流平台

安全管理 安全用户管理 **安全组管理** 客户端管理

通用权限

权限申请

权限配置

安全管理

新增安全组

1、用户（组）管理

3、资源与权限策略管理（不展示）

每页显示 15 条记录

组名	LDAP-DN	成员	操作
accumulo	cn=accumulo,ou=Group,...	yu[redacted]in	<input type="button" value="添加成员"/>
airflow	cn=airflow,ou=Group,dc...	无	<input type="button" value="添加成员"/>

通用权限管理平台 帮助中心

产品: 流平台

安全管理 安全用户管理 安全组管理 **客户端管理**

通用权限

权限申请

权限配置

安全管理

新增客户端

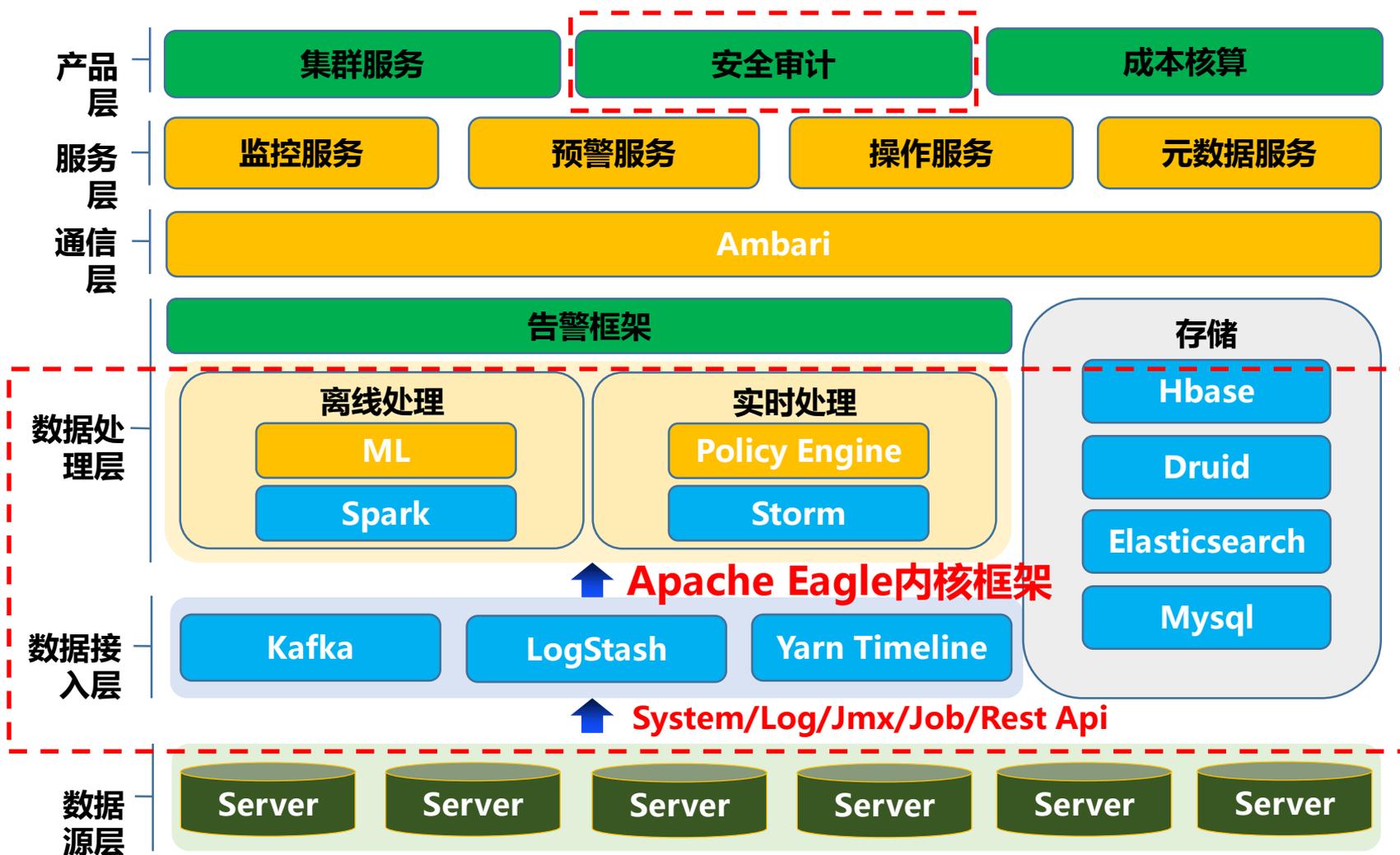
每页显示 15 条记录

2、客户端IP与平台应用类型管理

客户端 ID	client-ip	秘钥	类型	产品名称	备案时间	操作
94552688	1[redacted]127.0.0.1...	0b24673a819a5f88bf81...	业务接入类客户端	集成开发平台	2017-10-11	<input type="button" value="复制秘钥"/> <input type="button" value="添加 IP"/>
-1672042388	127.0.0.1	5fd43ac9abf17be7fb314...	业务接入类客户端	流平台	2017-10-11	<input type="button" value="复制秘钥"/> <input type="button" value="添加 IP"/>
110397	1[redacted],0.0.0.1...	d33215f1e77c5e3ba2dd...	业务接入类客户端	ouc	2017-10-18	<input type="button" value="复制秘钥"/> <input type="button" value="添加 IP"/>

魅族大数据安全管理系统

安全审计系统产品架构设计



MEIZU 首页 集群服务 集群安全 系统管理

策略管理 告警查询 元数据 数据分类 管理

1 选择流 2 定义告警策略 3 配置警告通知

匹配规则：隐藏 / 展开

> user

> timestamp

> command

▼ sensitivityType

== PHONE_NUMBER add

==

隐藏

contains

regex

1、添加Hive敏感表字段访问预警策略

2、实时搜集Hive行为日志并处理，触发告警

上一步 下一步

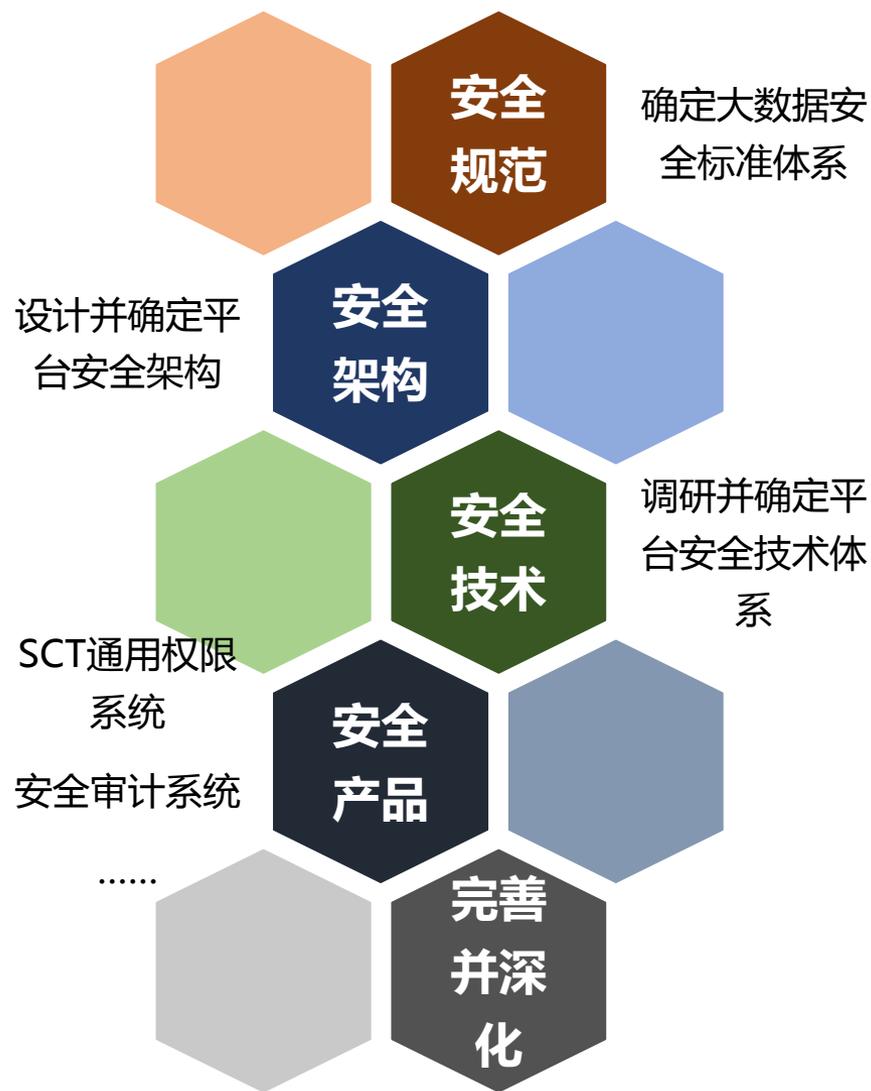
MEIZU 首页 集群服务 集群安全 系统管理

策略管理 告警查询 元数据 数据分类 管理

DAM / HIVE

ID	告警时间	消息时间	应用名称	策略名称	用户	源	描述
1	2017-11-02 08:30:17	2017-11-02 08:30:17	hiveQueryLog	queryPhoneNumber	hive	hiveAccessLogStream	The Policy "queryPhoneNumber" has been detected with the below information: timestamp="1512313017" sensitivityType="PHONE_NUMBER" resource="/xademo/customer_details/phone_number" command="SELECT" user="hive"
2	2017-11-02 07:09:00	2017-11-02 07:09:00	hiveQueryLog	queryPhoneNumber	hive	hiveAccessLogStream	The Policy "queryPhoneNumber" has been detected with the below information: timestamp="1512298540" sensitivityType="PHONE_NUMBER" resource="/xademo/customer_details/phone_number" command="SELECT" user="hive"

总结与展望



THANKS

