**产品安全验证报告**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 产品名称： | FusionInsight | |  |  | | 产品版本： | FusionInsight V100R002C30 | |  |  | | 报告编号： | SYBH(W) 016720150325 | |
| HW_POS_RGB_Vertical  华为技术有限公司内部网络安全实验室  地址：深圳市龙岗区坂田华为B1-1-01R  电话：+86 755 28780808 传真：+86 755 28786994  版权所有 侵权必究 |

|  |
| --- |
| 声明 |
| 1、如无报告拟制人和审批人的签字，报告将视为无效 |
| 2、如无证据证明评估结果不符合，则所有不符合项的判断均无效 |
| 3、本验证报告的结果只对被检测样品有效 |
| 4、未经实验室的书面批准不得部分/全部复制报告的内容 |

|  |  |
| --- | --- |
| **申请人:** | 华为技术有限公司 |
| **地址:** | 深圳市龙岗区坂田华为总部办公楼 |
| **产品名称:** |  |
| **版本:** | *请写上被测系统的最小版本* |
|  |  |
| **验证标准** | 网络安全和隐私保护 |
| **样品接收时间:** | YYYY-MM-DD |
| **验证开始时间:** | YYYY-MM-DD |
| **验证结束时间:** | YYYY-MM-DD |
| **验证人员：** | 姓名/工号、姓名/工号、姓名/工号 |
|  |  |
|  |  |
| **拟制人:** | YYYY-MM-DD 张三/00012345 工程师  日期 姓名 职位 签名 |
|  |  |
| **批准人:** | YYYY-MM-DD 韩少伟/64523 实验室经理  日期 姓名 职位 签名 |

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 描述 | 作者 |
| 2015-5-5 | V1.0 | 初稿 | 伍秋银/148893 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

[1 项目介绍 1](#_Toc419122195)

[1.1 目的 1](#_Toc419122196)

[1.2 验证对象 1](#_Toc419122197)

[1.3 评估验证环境描述 1](#_Toc419122198)

[1.3.1 产品典型应用组网 1](#_Toc419122199)

[1.3.1.1 物理组网 3](#_Toc419122200)

[1.3.1.2 逻辑组网 5](#_Toc419122201)

[1.3.2 验证组网 6](#_Toc419122202)

[1.3.3 安全评估工具 6](#_Toc419122203)

[2 产品安全性总体评价 7](#_Toc419122204)

[2.1 网络安全和隐私保护验证结果 7](#_Toc419122205)

[2.2 代码安全验证结果 7](#_Toc419122206)

[2.2.1 源码扫描结论 7](#_Toc419122207)

[2.2.2 代码健康度结论 8](#_Toc419122208)

[2.3 验证发现的安全问题统计 8](#_Toc419122209)

[3 安全验证内容 9](#_Toc419122210)

[3.1 网络安全和隐私保护验证 9](#_Toc419122211)

[3.1.1 系统分析及威胁分析 9](#_Toc419122212)

[3.1.1.1 关键组件安全威胁分析 9](#_Toc419122213)

[3.1.1.2 业务流程安全威胁分析 16](#_Toc419122214)

[3.1.1.3 开源漏洞分析 18](#_Toc419122215)

[3.1.2 验证内容及方法 20](#_Toc419122216)

[3.2 代码安全验证 21](#_Toc419122217)

[4 验证发现的安全问题描述 21](#_Toc419122218)

[4.1 安全问题概要描述 21](#_Toc419122219)

[4.2 安全问题详细描述 23](#_Toc419122220)

[4.2.1 访问通道控制 23](#_Toc419122221)

[4.2.1.1 8001端口未在通信矩阵中说明 23](#_Toc419122222)

[4.2.1.2 SNMPV3配置了鉴权及加密密钥模式时，客户端无需鉴权及加密密钥可对FI进行SNMPv3访问 24](#_Toc419122223)

[4.2.2 Web应用安全 26](#_Toc419122224)

[4.2.2.1 TGT过期前后，单点登出实现不一致，可能会因为登出不全而引起的安全风险 26](#_Toc419122225)

[4.2.2.2 业务组件界面如HBase\HDFS\Hue\Metadata退出后，管理组件Manager界面未失效，不能自动单点登出 27](#_Toc419122226)

[4.2.2.3 元数据管理界面没有单独logout功能 28](#_Toc419122227)

[4.2.2.4 权限为空的用户，可以访问HUE、HBase、HDFS所有组件界面 30](#_Toc419122228)

[4.2.2.5 角色的HBASE组件权限可以添加，不能删除，导致下发的权限无法回收 33](#_Toc419122229)

[4.2.2.6 用户解锁功能权限设计不合理，用户可以给自己解锁，有破解密码风险 33](#_Toc419122230)

[4.2.2.7 用户删除后，session未过期的业务界面可以继续访问 34](#_Toc419122231)

[4.2.3 敏感数据与加密保护 37](#_Toc419122232)

[4.2.3.1 后台加解密脚本AES256算法使用ECB加密模式 37](#_Toc419122233)

[4.2.4 隐私保护 38](#_Toc419122234)

[4.2.4.1 往HIVE加密表导入数据后，系统未自动删除原表或提示用户手工删除原表，存在从原表泄露用户数据的风险 38](#_Toc419122235)

[4.2.4.2 批量导入数据到hbase的加密表，实际数据未实现加密，存在泄露用户数据的风险 39](#_Toc419122236)

[4.2.4.3 HBASE用户数据文件HFile文件权限设置为674不合理 40](#_Toc419122237)

[4.2.5 系统管理和维护安全 40](#_Toc419122238)

[4.2.5.1 有权限的业务组件账号通过kinit认证后，本来没有权限的用户无需认证即可访问组件，存在越权访问风险 40](#_Toc419122239)

[4.2.6 其他问题 42](#_Toc419122240)

[4.2.6.1 FI存在本地不鉴权Rest接口，通过操作系统用户可以直接重置超户admin密码 42](#_Toc419122241)

[4.2.6.2 LDAP管理员用户输入多次错误密码，系统没有锁定用户 44](#_Toc419122242)

[4.2.6.3 日志文件权限过大750，建议设置为600，至少640 45](#_Toc419122243)

[4.2.6.4 环境搭建的配置规划工具有问题，在有物理业务网口的情况下，将属于业务面的DBServer 和Hue的浮动IP默认绑定到管理网口的子接口上，业务面、管理面没有物理隔离 46](#_Toc419122244)

[4.2.7 安全资料 48](#_Toc419122245)

[4.2.7.1 对于FI依赖的OS服务，请统一提供OS加固策略 48](#_Toc419122246)

[4.2.7.2 资料未提供业务组件管理员修改密码的方法 51](#_Toc419122247)

[4.2.7.3 Admin用户实际权限与资料不一致 52](#_Toc419122248)

[4.2.7.4 修改密码步骤中的密码策略资料描述不正确 53](#_Toc419122249)

[5 附录 53](#_Toc419122250)

[5.1 代码扫描结果 53](#_Toc419122251)

[5.1.1 Nmap扫描报告 53](#_Toc419122252)

[5.1.2 Codecc(Fortify)扫描报告 54](#_Toc419122253)

[5.1.3 Appscan扫描报告 54](#_Toc419122254)

[5.1.4 SecureCAT扫描报告 54](#_Toc419122255)

[5.2 版本配套表 54](#_Toc419122256)

# 项目介绍

## 目的

全球的法律环境和政治环境已经发生非常突出的变化，网络安全问题已上升为法律问题、政治问题，政治的博弈已转移到网络安全领域。网络安全已经成为我司业务拓展的短木板之一。为了避免网络安全引起的危机，避免网络安全成为业务扩展的瓶颈，网络安全实验室对公司大数据产品FusionInsight进行了此次安全验证。

## 验证对象

|  |  |
| --- | --- |
| 产品名称 | FusionInsight |
| 产品版本 | V100R002C30SPC300 |
| 版本所处开发阶段 | TR5－TR6 |

验证时间：2015-3-25 - 2015-4-30

验证地点：深圳市龙岗区坂田华为内部网络安全实验室B1-1-01R

验证人员：伍秋银/148893、林金堆/246948、林远龙/257195、韦建威/325821、郝晓斐/188919

产品线相关接口人：曾令桐/127865、崔旭涛/221399

## 评估验证环境描述

### 产品典型应用组网

华为FusionInsight2.3基于开源社区软件最新版本的Hadoop2.4针对可靠性、安全性、管理性等方面做企业级的功能增强，提供企业级大数据存储、查询、分析、数据挖掘的统一平台，帮助企业快速构建海量数据信息处理系统。通过对各类海量数据信息进行实时和非实时的分析和挖掘，帮助企业从海量数据信息中获取到真正的价值，及时洞察和决策新的机会与风险。

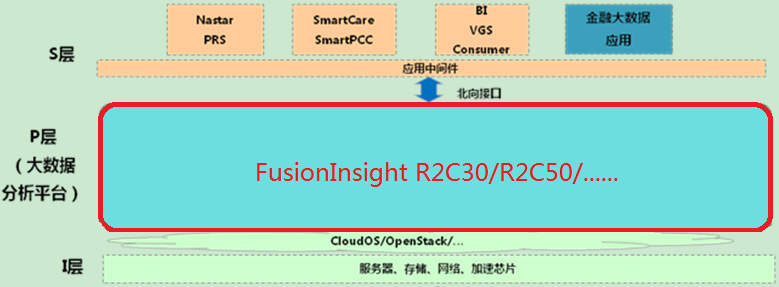
FusionInsight大数据两大特点：一是大，数据处理能力在TB甚至PB级以上，远超过传统数据库的处理能力；二是复杂的数据类型，可处理结构化、非结构化、半结构化的数据。

FusionInsight目前主要应用于应用于电信做历史话单查询、经营详单数据并发分析、经营分析、网优，应用于银行做历史交易明细实时查询业务、实时征信业务、小微贷业务预测，公安等。

我司FusionInsight2.3版本是第一个产品化的版本，FusionInsight在解决方案中的功能如下图示：

**R2C30**

FusionInsight与周边产品、解决方案的关系如下：

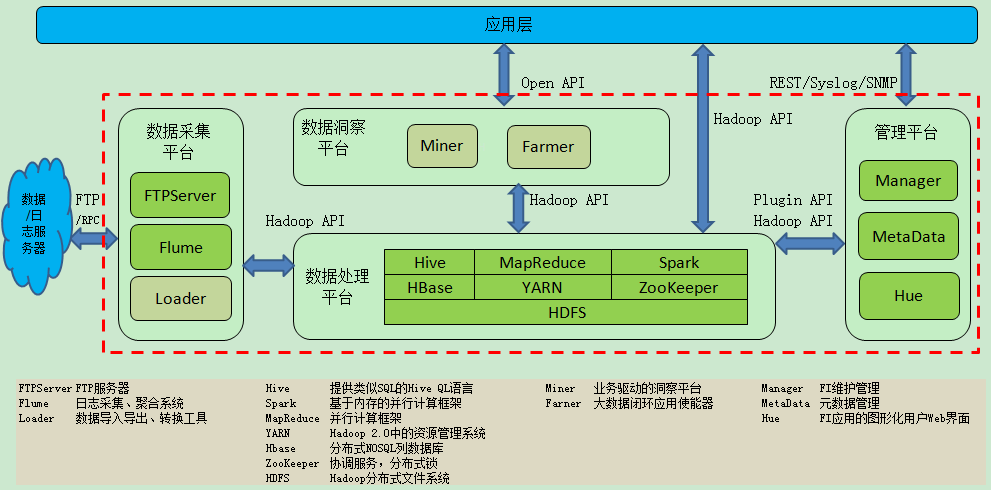


物理组网

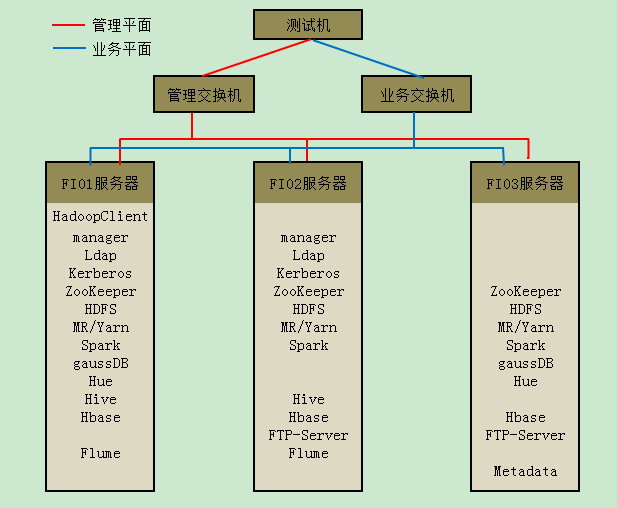
支持双平面隔离组网，集群中每个节点分别接入业务平面和管理平面。组网隔离时，双平面可以采用各自独立的端口配置，也可以采用VLAN的方式配置。节点数小于200的集群采用二层组网，集群内二层交换，采用独立的端口配置组网参见下图：



逻辑组网



### 验证组网



### 安全评估工具

|  |  |  |
| --- | --- | --- |
| **测试工具** | **用途** | **版本** |
| **端口和漏洞扫描工具** | | |
| Nessus | 系统和应用漏洞扫描工具 | V4.2.2 |
| map | 端口扫描工具 | 5.51 |
| **抓包工具** | | |
| WireShark | 抓包工具 | 1.4.1 |
| **代码开发工具** | | |
| Source Insight | 查看源码工具 | 3.0 |
| python | 脚本编写工具 | 2.5 |
| **其他工具** | | |
| ultraedit | 十六进制编辑工具 | 14.00a |
| Appscan | 业界领先的web安全扫描工具 |  |
| Codenomicon | 协议模糊测试软件 |  |
| Burpsuit | 攻击web 应用程序的集成平台 |  |
| Putty | Telnet、SSH、rlogin、纯TCP以及串行接口连接软件 |  |
| CsecCheck | 代码健康度扫描工具 | V1.0 |
| SecureCAT | 数据库扫描工具 |  |
| peach | 协议攻击工具 |  |
| Fortify | 静态代码扫描工具 | 4.0 |

# 产品安全性总体评价

## 网络安全和隐私保护验证结果

本版本网络安全和隐私保护验证，共发现21个问题。其中红线A1类红线问题0个，A2类红线问题0个，B类问题0个，红线观察项问题0个，非红线安全问题21个。其中权限管理、个人数据保护、WEB等方面问题较多。

## 代码安全验证结果

### 源码扫描结论

本次Codecc（Fortify+Coverity的结合）工具源码扫描策略主要关注FusionInsight产品中的自研代码部分。产品已经在之前通过Codecc扫描过源代码，扫描出多个“高”级别的告警，针对这些告警已进行一一分析，并对非误报问题已经做出修改，确认为误报问题进行屏蔽，并给出分析报告结果。目前产品已不存在高级别告警，遗留多个中低级别告警。



### 代码健康度结论

使用CsecCheck代码健康度扫描工具进行扫描，本次扫描结果作为原始数据，下个版本提供对比数据：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **维度** | **原始值** | **当前值** | **对比结果** | **对比结果评价标准** | |
| **不达标标准** | **达标标准** |
| 危险函数引用密度（个/Kloc） | 9.8 | 9.8 | 第一次送检 | 当前值>=原始值 | 当前值<原始值 |
| 源文件重复度 | 1.1% | 1.1% | 第一次送检 | 当前值>=原始值 | 当前值<原始值 |
| 代码逻辑行总行 | 863964 | 863964 | N/A | 仅度量，不提供评价标准 | |
| 代码文件总数 | 3913 | 3913 | N/A |
| 文件平均行数 | 220 | 220 | N/A |
| 废弃代码  （个/Kloc） | 0.7 | 0.7 | N/A |
| 代码注释率 | 25.3% | 25.3% | N/A |

## 验证发现的安全问题统计

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **A1类问题** | **A2类问题** | **B类问题** | **观察项** | **其他安全问题** | **总计** |
| 0 | 0 | 0 | 0 | 21 | 21 |

表2.4.1 按网络安全和隐私保护等级分类统计表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **致命问题** | **严重问题** | **一般问题** | **提示问题** | **总计** |
| 0 | 1 | 3 | 17 | 21 |

表2.4.2 按问题严重等级分类统计表

图2.4.1 按安全属性分类统计图

# 安全验证内容

## 网络安全和隐私保护验证

### 系统分析及威胁分析

关键组件安全威胁分析

##### 管理子系统威胁分析

Manager作为运维系统，Manager支持大规模集群的安装部署、监控、告警、用户管理、权限管理、审计、服务管理、健康检查、问题定位、升级和补丁等

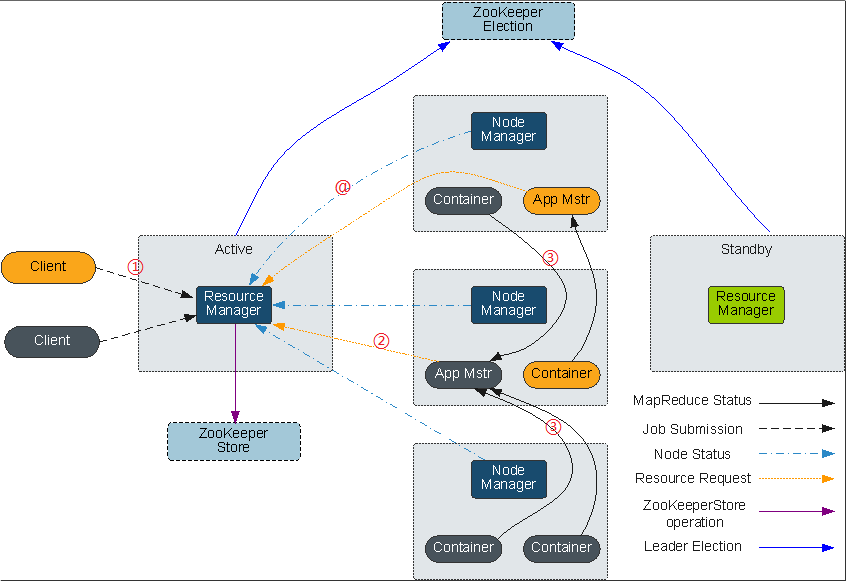
【识别威胁点】

* Web安全：认证、会话管理、权限管理、XSS、SQL注入、文件上传下载、日志审计
* 接口安全：REST API、Syslog、SNMP，SNMP可参考基线用例

结合系统分析的识别到的威胁点，使用思维导图对管理子系统Manager进行威胁分析结果如下：



##### 计算子系统威胁分析



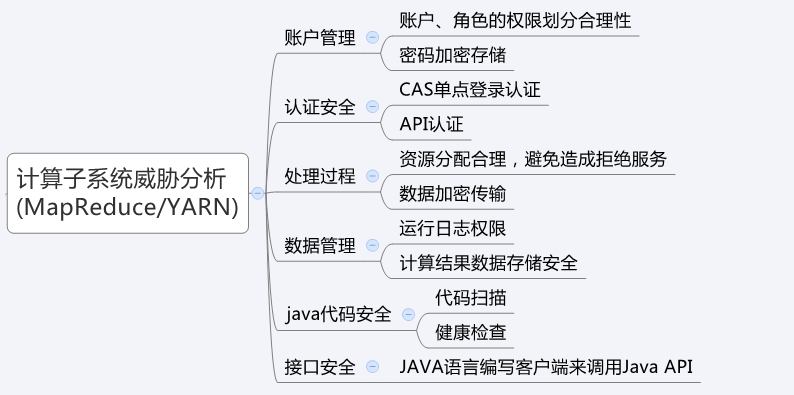
MapReduce/YARN工作流程：

1. 集群部署了YARN组件，会在每个节点部署一个NM，实时监控节点及应用程序的资源使用情况，并向RM汇报
2. Client向RM下发一个MR job
3. RM根据集群的资源使用情况，在集群中最空闲的节点上启动一个AM，AM向RM申请多个Container资源（Container数量=MAP任务数+REDUCE任务数，一个Container只能用于放置一个MAP任务或一个REDUCE任务，每个Container的资源是等同的）
4. 在Container启动不同的MAP及REDUCE进程来处理MR job，MR job完成后，上报AM，AM申请资源释放

【识别威胁点】

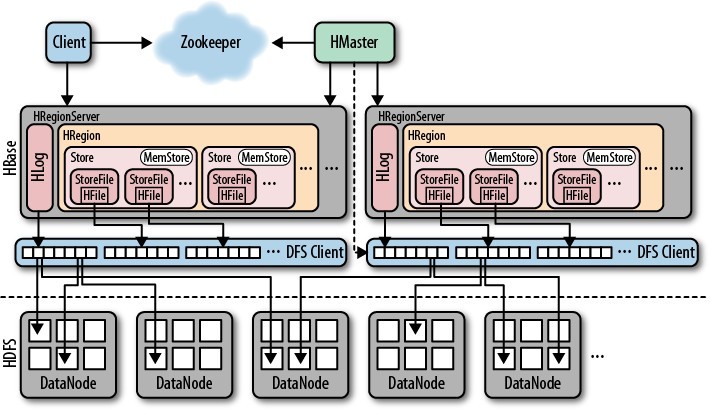
* 认证安全、处理过程数据传输安全、Dos攻击防护
* 接口安全：JAVA API

结合系统分析的识别到的威胁点，使用思维导图对管理子系统Manager进行威胁分析结果如下：



##### 存储子系统威胁分析

==================HBase==================



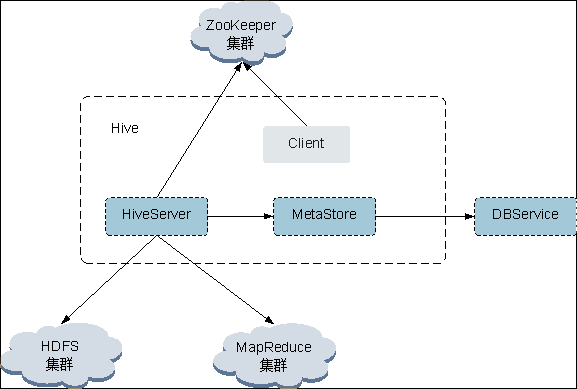
HBase集群由主备Master进程和多个RegionServer进程组成，其依赖的组件有ZK、HDFS：

* Client与Master进行管理类通信，与RegionServer进行数据操作类通信。
* HMaster负责HBase中RegionServer的管理，RegionServer的负载均衡，Region分布调整；Region分裂以及分裂后的Region分配；RegionServer失效后的Region迁移等。
* RegionServer负责提供表数据读写等服务，是HBase的数据处理和计算单元。RegionServer一般与HDFS集群的DataNode合并。实现数据的存储功能。
* ZooKeeper为HBase集群中各进程提供分布式协作服务。各RegionServer将自己的信息注册到Zookeeper中，Master据此感知各个RegionServer的健康状态。
* HDFS为HBase提供高可靠的文件存储服务，HBase的数据全部存储在HDFS中。

【识别威胁点】

* 认证安全
* 数据安全：元数据/数据访问权限、数据加密、数据读写安全、数据整合分割安全、组件审计日志
* 接口安全：Shell、Java API、Sqlline、JDBC API、REST API、Thrift API

==================Hive==================



Hive为单实例的服务进程，提供服务的原理是将HQL编译解析成相应的MapReduce或者HDFS任务。Hive由client、主备HiveServer进程和多个RegionServer进程组成，其依赖的组件有ZK、HDFS：

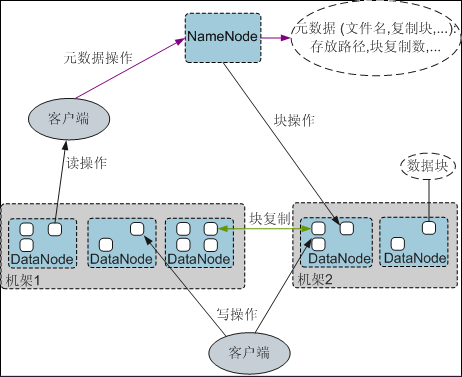
* HiveServer，HA模式下包含主用HiveServer和备用HiveServer，对外提供Hive数据库服务，将用户提交的HQL语句进行编译，解析成对应的MR任务或者HDFS操作，从而完成数据的提取、转换、分析。
* MetaStore，HA模式下包含主用MetaStore和备用MetaStore，提供Hive的元数据服务，负责Hive表的结构和属性信息读、写、维护和修改。
* ZooKeeper为HiveServer的HA机制提供仲裁。各HiveServer将自己的信息注册到Zookeeper中，为客户端访问主HiveServer提供依据
* HDFS集群，Hive表数据存储在HDFS集群中。
* MR集群提供分布式计算服务：Hive的大部分数据操作依赖MapReduce，HiveServer的主要功能是将HQL语句转换成MR任务，从而完成对海量数据的处理。

【识别威胁点】

* 认证安全
* 数据安全：元数据/数据访问权限、数据加密、数据读写安全、数据整合分割安全、组件审计日志
* 接口安全：JDBC API、Thrift API、Hive SQL

==================HDFS==================

在HDFS内部，一个文件其实分成一个或多个“数据块”，这些“数据块”存储在DataNode集合里，NameNode负责保管和管理所有的HDFS元数据(目录命名空间)。客户端连接到NameNode，执行文件系统的“命名空间”操作，例如打开、关闭、重命名文件和目录，同时决定“数据块”到具体DataNode节点的映射。DataNode在NameNode的指挥下进行“数据块”的创建、删除和复制。另外客户端连接到DataNode，执行读写用户数据操作。



【识别威胁点】

* 认证安全
* 数据安全：元数据/数据访问权限、数据读写安全、数据整合分割安全、组件审计日志
* 接口安全：Shell、Java API、C API、HTTP REST API

结合以上系统分析的识别到的威胁点，使用思维导图对管理子系统Manager进行威胁分析结果如下：



业务流程安全威胁分析

以Hive组件的HQL-load语句导入数据到HBase数据库为例，分析数据导入业务流程如下：



STRIDE O层接口及数据流图分析如下：



根据STRIDE分析方式，分析对外部实体、处理过程、数据存储、数据流的资产进行威胁分析：

外部实体：JAVA Client、shell Client、OM Client

处理过程：Hive、Hbase、HDFS、GaussDB、Mapreduce、OM、Kerberos

数据存储：LOG、DB、HDFS文件

数据流：Hive--gaussDB、HBase--HDFS、Client--Hive、Hive –HDFS等

开源漏洞分析

与产品确认，以下开源组件已知漏洞都已提供归避措施，目前未发现未修复的严重开源漏洞。

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞 | 描述 | 风险 | 方案 |
| <http://www.2cto.com/Article/201302/189431.html> | Hive任意命令/代码执行漏洞+渗透实例 | hue的主页和Hive查询页面有跨站点点脚本攻击风险，即XSS攻击 | 增加了适当的html编码检测 |
| [https://review.cloudera.org/r/4577/diff/#](https://review.cloudera.org/r/4577/diff/) | HUE-2321 [filebrowser] Add support for hdfs umask | 用户通过Hue创建的文件和文件夹都是默认的755权限，权限过大。可能导致A用户的敏感信息暴露给同组的B用户。 | 在hue设置默认创建的hdfs文件或文件夹权限，并把该权限的值传给hdfs，控制hue调用hdfs时的权限。 hue设置的默认值掩码为 07 |
| <https://issues.cloudera.org/browse/HUE-2394> | Fix Cross-site request forgery (CSRF) vulnerabilities | hue有CSRF攻击风险 | 利用Django中内置的django.middleware.csrf.CsrfViewMiddleware中间件 和 CSRF token 对所有视图添加CSRF认证 |
| <http://www.2cto.com/Article/201302/189431.html> | Hive任意命令/代码执行漏洞+渗透实例 | 通过在在Hive的transform中嵌入恶意脚本，实现攻击的目的 | 禁止该功能 |
| CVE-2014-5352 | Kerberos allows remote authenticated users to cause a denial of service | 该漏洞会导致在认证达到一定负荷场景下，引起KDC服务的拒绝处理，导致KDC无法正常工作 | 该漏洞已经按照开源社区的修补方法进行修复 |
| CVE-2014-9421 | Kerberos allows remote authenticated users to cause a denial of service | 该漏洞在畸形报文数据发送到KDC的时候，会引起KDC服务异常，导致KDC无法正常工作 | 该漏洞已经按照开源社区的修补方法进行修复 |
| CVE-2014-9422 | Kerberos allows remote authenticated users to bypass a kadmin/\* authorization check | 该漏洞在客户端使用kadmin/\*用户进行登陆认证时，会引起越权访问 | 该漏洞已经按照开源社区的修补方法进行修复 |
| CVE-2014-4345 | Kerberos allows remote authenticated users to cause a denial of service | 该漏洞在客户端发送的报文中包含cpw -keepold命令时会引起KDC的拒绝服务 | 该漏洞已经按照开源社区的修补方法进行修复 |

### 验证内容及方法

FI作为第一次送检，本来是需要E2E全面覆盖测试，但由于FI组件太多，当前版本重点测试关键组件Manager、MapReduce/YARN、HBase、HDFS、Hive及典型业务全流程。其他组件只做基线红线排查；

产品敏感特性重点验证CAS单点登录、统一权限控制、数据存储与加密；

Web测试重点参考Web规范、并重点排查XSS及SQL注入；

协议攻击重点验证SNMP，使用peach进行；

基线用例覆盖了web基线用例、SNMP基线用例；

工具扫描覆盖DB扫描、端口扫描、代码扫描；

对自研的代码review，针对关键模块omm、aos、acs抽样人工走读；

|  |  |  |
| --- | --- | --- |
| 分类 | 内容 | 方法 |
| 基础设施防护 | guassDB数据库 | SecureCAT评估、数据库安全加固检查 |
| OS加固 | 产品不交付OS，重点关注FI依赖的OS服务的安全加固 |
| LDAP | 人工检查用户管理、权限管理 |
| 业务功能安全性 | 关键组件Manager、MapReduce/YARN、HBase、HDFS、Hive | 人工检查，检查项参考前面的威胁分析 |
| 典型业务 | 人工检查，检查项参考前面的威胁分析 |
| 单点登录 | 人工检查，检查项参考前面的威胁分析 |
| 统一权限控制 | 人工检查，检查项参考前面的威胁分析 |
| 系统整体 | 红线安全维度分类 | 红线分解后的通用检查项目进行检查 |
| WEB | Web规范、web基线用例、XSS及SQL注入渗透测试 | 人工检查，检查项参考前面的威胁分析 |
| 接口 | REST | 人工走读代码，排查是否存在可利用的无需认证端口 |
| SNMP | 参考SNMP基线用例，并使用peach进行协议攻击测试 |
| 代码 | 代码规范性 | Coverity、Fortify、CsecCheck检查 |

## 代码安全验证

按照编程规范人工Review：对FI自研代码(主要是omm、aos、acs代码)的关键代码进行代码走读，通过API调用关系分析业务流，重点关注XSS、SQL注入，越权问题。

# 验证发现的安全问题描述

## 安全问题概要描述

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **问题类别** | **问题描述** | **问题严重等级** | **定级依据** | **问题单号** | **问题状态** |
|
| 1 | 访问通道控制 | SNMPV3配置了鉴权及加密密钥模式时，客户端无需鉴权及加密密钥可对FI进行SNMPv3访问 | 严重 | CVSS 7.5 |  | open |
| 2 | Web应用安全 | 组件界面如HBASE\HDFS\HUE退出后，MANAGER界面未失效，不能自动单点登出 | 提示 |  |  | open |
| 3 | TGT过期前后，单点登出实现不一致，可能会因为登出不全而引起的安全风险 | 提示 |  |  | open |
| 4 | 元数据管理界面没有单独logout功能 | 提示 |  | DTS2015031800101 | open |
| 5 | 权限为空的用户，可以访问HUE、HBase、HDFS所有组件界面 | 一般 | CVSS 4.0 | DTS2015040904342 | open |
| 6 | 角色的HBASE组件权限可以添加，不能删除，导致下发的权限无法回收 | 提示 |  | DTS2015042905524 | open |
| 7 | 用户解锁功能权限设计不合理，用户可以给自己解锁，有破解密码风险 | 提示 |  | [DTS2015042103256](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042103256) | open |
| 8 | 用户删除后，session未过期的业务界面可以继续访问 | 提示 |  | DTS2015031905212 | open |
| 9 | 敏感数据与加密保护 | 后台加解密脚本AES256算法使用ECB加密模式 | 提示 |  | DTS2015032801342 | open |
| 10 | 隐私保护 | 往HIVE加密表导入数据后，系统未自动删除原表或提示用户手工删除原表，存在从原表泄露用户数据的风险 | 提示 |  | [DTS2015042908044](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042908044) | open |
| 11 | 批量导入数据到hbase的加密表，实际数据未实现加密，存在泄露用户数据的风险 | 提示 |  | DTS2015042402328 | open |
| 12 | HBASE用户数据文件HFile文件权限设置为674不合理 | 提示 |  |  | open |
| 13 | 系统管理和维护安全 | 有权限的业务组件账号通过kinit认证后，本来没有权限的用户无需认证即可访问组件，存在越权访问风险 | 一般 | CVSS 6.0 |  | open |
| 14 | 其他问题 | FI存在本地不鉴权Rest接口，通过操作系统用户可以直接重置超户admin密码 | 一般 | CVSS 6.8 |  | open |
| 15 | LDAP管理员用户输入多次错误密码，系统没有锁定用户 | 提示 |  |  | open |
| 16 | 日志文件权限过大750，建议设置为600，至少640 | 提示 |  |  | open |
| 17 | 环境搭建的配置规划工具有问题，在有物理业务网口的情况下，将属于业务面的DBServer 和Hue的浮动IP默认绑定到管理网口的子接口上，业务面、管理面没有物理隔离 | 提示 |  | DTS2015041005049 | open |
| 18 | 安全资料 | 对于FI依赖的OS服务，请统一提供OS加固策略 | 提示 |  | DTS2015040904438 | open |
| 19 | 资料未提供业务组件管理员修改密码的方法 | 提示 |  | [DTS2015042102727](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042102727) | open |
| 20 | Admin用户实际权限与资料不一致 | 提示 |  | [DTS2015042102877](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042102877) | open |
| 21 | 修改密码步骤中的密码策略资料描述不正确 | 提示 |  | DTS2015040904533 | open |

## 安全问题详细描述

### 访问通道控制

SNMPV3配置了鉴权及加密密钥模式时，客户端无需鉴权及加密密钥可对FI进行SNMPv3访问

【问题严重等级】

严重问题，非红线安全问题，定级依据是CVSS基础分为 7.5（AV:N/AC:L/Au:N/C:P/I:P/A:P），CVSS基础分评分说明如下：

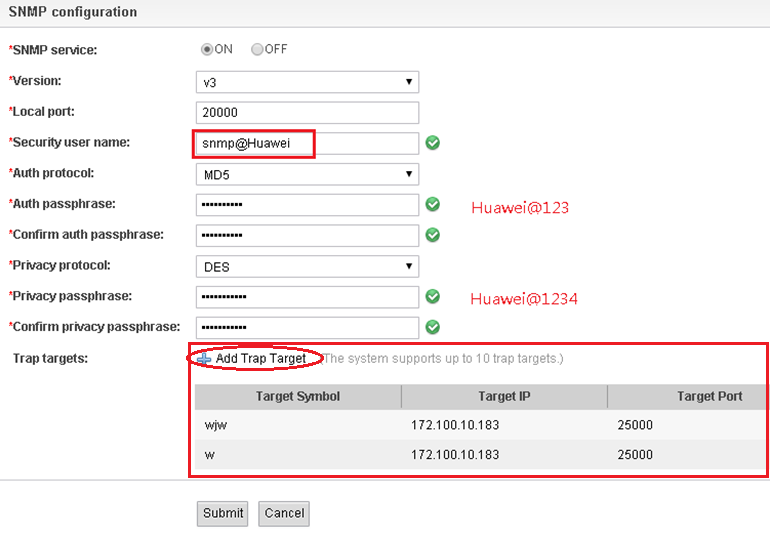
|  |  |  |
| --- | --- | --- |
| 维度 | 评分情况 | 评分说明 |
| Access Vector | N | 远程SNMP访问 |
| Access Complexity | L | 只需要打开SNMP V3服务 |
| Authentication | N | 无需鉴权及加密密钥 |
| Confidentiality Impact | P | 可获取告警信息、Trap服务器列表 |
| Integrity Impact | P | 可清除告警状态，增删Trap服务器，修改原来的trap配置列表 |
| Availability Impact | P | 可清除告警状态，删除Trap服务器，使上层网管无法获取告警 |

【问题现象】

SNMPV3支持3个安全级别的模式：noAuthNoPriv指无需认证且无需加密， AuthNoPriv指需要认证但无需加密，AuthPriv指需要认证且需要加密，是最安全的一种模式。

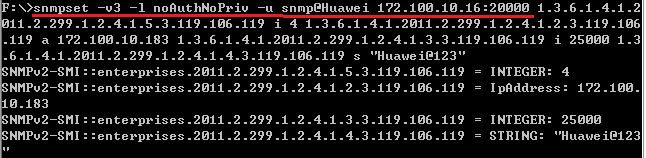
FI的SNMP V3接口主要是用于做告警消息的上报，此接口的安全模式设计的原意是只支持AuthPriv：

1. FI系统SNMPV3配置了认证/加密算法类型、密钥后，可以在界面添加告警上报的服务器信息，如下图所示：

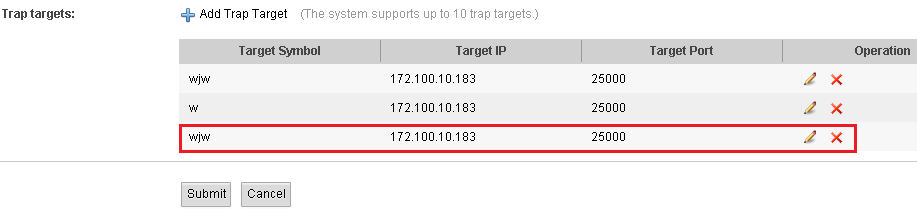


1. 还使用Net-SNMP工具执行命令，增加一条Trap服务器记录
2. 但使用Net-SNMP工具执行命令时，指定模式使用noAuthNoPriv，只需输入v3用户名，不输入认证/加密的算法类型、密钥，命令执行成功：

snmpset -v3 -l noAuthNoPriv -u snmp@Huawei 172.100.10.16:20000 1.3.6.1.4.1.2011.2.299.1.2.4.1.5.3.119.106.119 i 4 1.3.6.1.4.1.2011.2.299.1.2.4.1.2.3.119.106.119 a 172.100.10.183 1.3.6.1.4.1.2011.2.299.1.2.4.1.3.3.119.106.119 i 25000 1.3.6.1.4.1.2011.2.299.1.2.4.1.4.3.119.106.119 s "Huawei@123"



1. FI界面查看，使用工具成功增加了一条Trap服务器记录。



【注】此时，如果改为authPriv模式，使用正确密钥可正常访问，使用错误密钥无法访问。

存在风险：

1. SNMPv3场景，无需认证/加密密钥，可获取告警信息、Trap服务器列表信息；136960
2. SNMPv3场景，无需认证/加密密钥，可清除（恢复）告警状态，使告警被忽略；
3. SNMPv3场景，无需认证/加密密钥，可删除Trap服务器，使上层网管无法获取告警。

【解决方案建议】

【问题单号及状态】

【产品反馈】

### Web应用安全

TGT过期前后，单点登出实现不一致，可能会因为登出不全而引起的安全风险

【问题严重等级】

提示，非红线安全问题

【问题现象】

FI系统的业务组件HBase\HDFS\Hue\Metadata多个web界面与管理组件Manager的web界面之间，已实现单点登录。

20分钟TGT过期前，Manager退出，业务组件HBase\HDFS\Hue\Metadata都可以自动退出；

20分钟TGT过期后，单点登出失效，Manager退出，业务组件HBase\HDFS\Hue\Metadata不能自动登出。

如果用户不了解实现机制，无法判断单点登出的有效场景，可能会因为登出不全而引起的安全风险。

【解决方案建议】

【问题单号及状态】

【产品反馈】

业务组件界面如HBase\HDFS\Hue\Metadata退出后，管理组件Manager界面未失效，不能自动单点登出

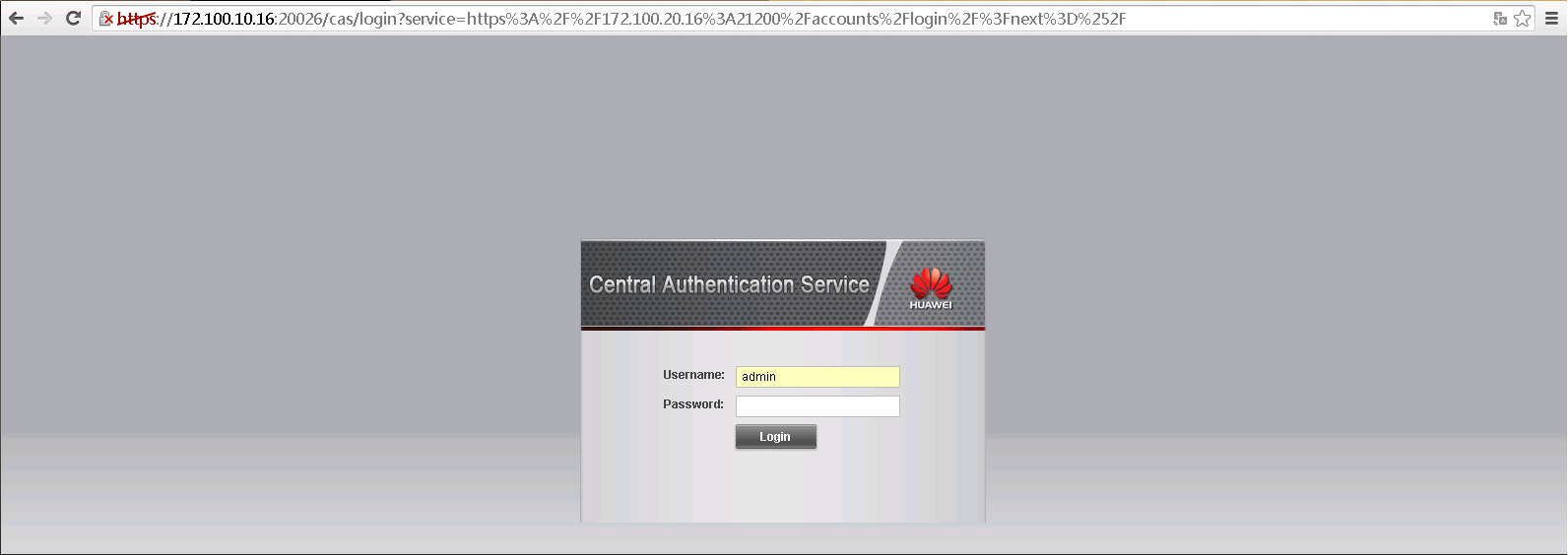
【问题严重等级】

提示，非红线安全问题

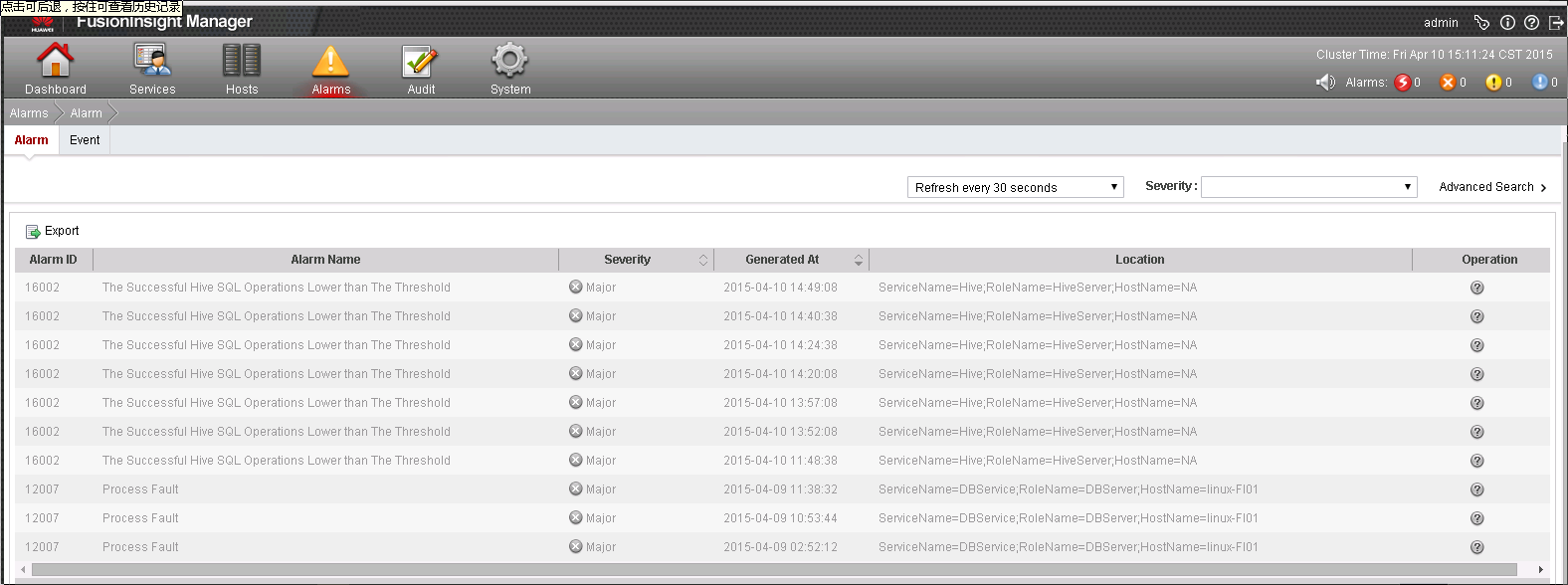
【问题现象】

业务组件界面如HBase\HDFS\Hue退出后，管理组件Manager界面未失效，不能自动单点登出

1. 业务组件HBase的web界面已退出



1. 管理组件Manager的web界面未失效，可以继续操作



【解决方案建议】

【问题单号及状态】

【产品反馈】

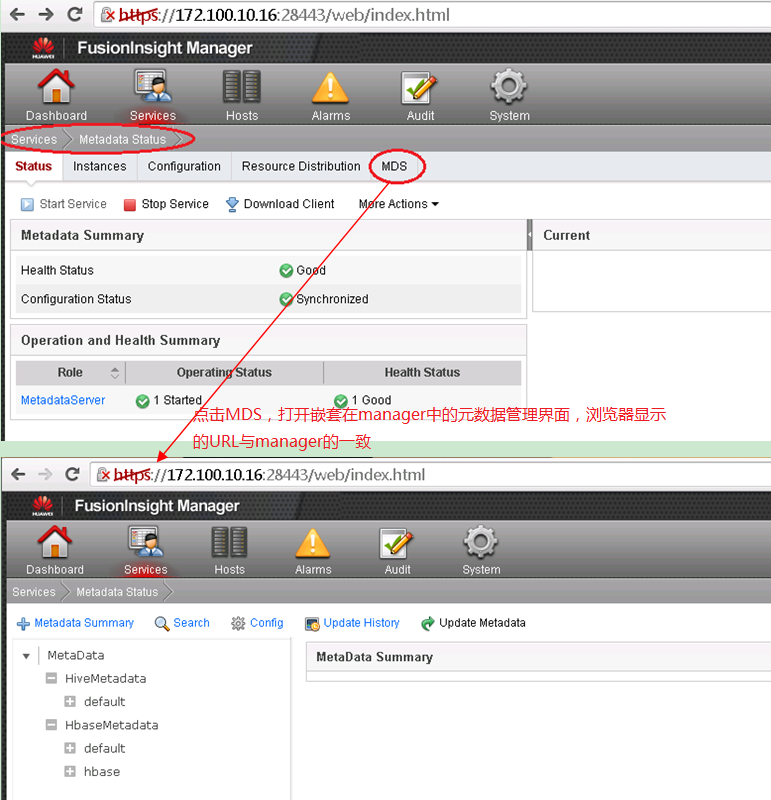
元数据管理界面没有单独logout功能

【问题严重等级】

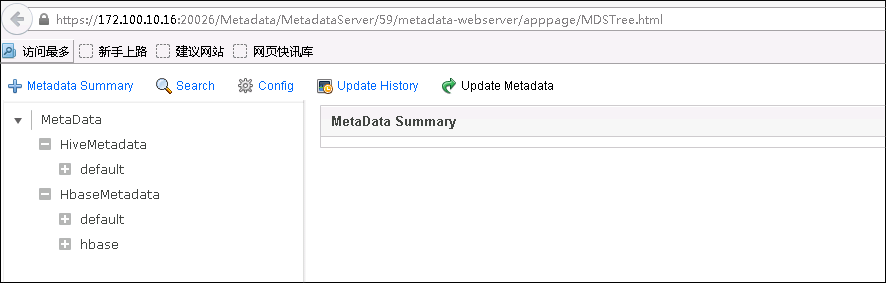
提示，非红线安全问题

【问题现象】

元数据管理界面嵌在manager中，但Web容器使用单独的，所以manager退出，元数据没有自动退出。元数据没有提供单独的logout按钮。



也可以在新页签输入元数据管理界面的url直接登录，同样没有提供单独的logout按钮。



浏览器关闭后，前台不活动，后台session 20分钟超时退出，目前没有立即销毁后台session手段。

用户登录元数据页面后，删除用户，有同样的问题。

【解决方案建议】

【问题单号及状态】

DTS2015031800101

【产品反馈】

权限为空的用户，可以访问HUE、HBase、HDFS所有组件界面

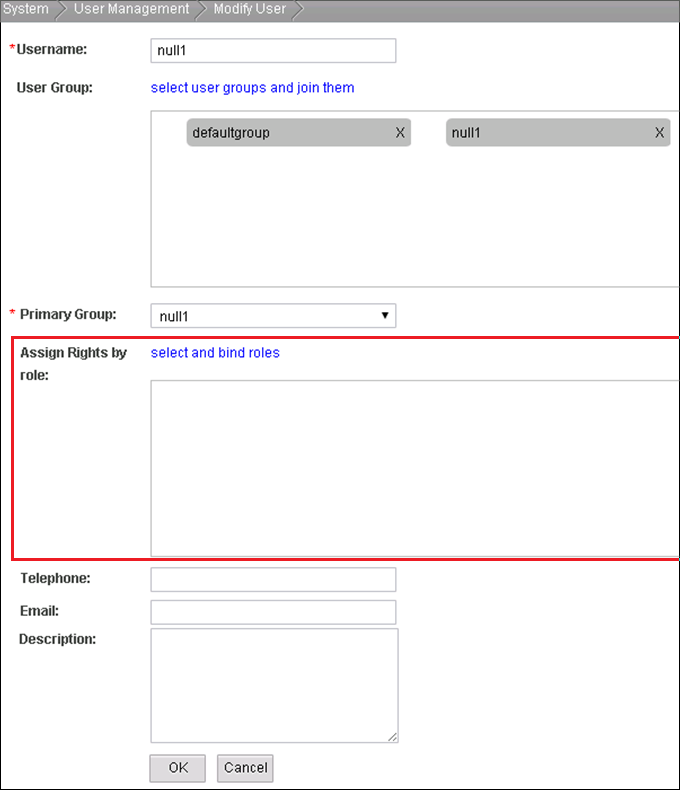
【问题严重等级】

一般问题，非红线安全问题，定级依据是CVSS基础分为 4.0（AV:N/AC:L/Au:S/C:P/I:N/A:N），CVSS基础分评分说明如下：

|  |  |  |
| --- | --- | --- |
| 维度 | 评分情况 | 评分说明 |
| Access Vector | N | 通过WEB访问 |
| Access Complexity | L | 无任何权限用户都可以查看 |
| Authentication | S | 需要通过一次登录认证 |
| Confidentiality Impact | P | 可以查看用户创建的表名、列名，可以查看XX4以上的HDFS文件并可下载 |
| Integrity Impact | N | 不能增删改数据 |
| Availability Impact | N | 不能对业务组件造成损坏，不影响业务组件正常运行 |

【问题现象】

1. 创建一个用户null1，此用户未分配任何角色，即没有任何权限

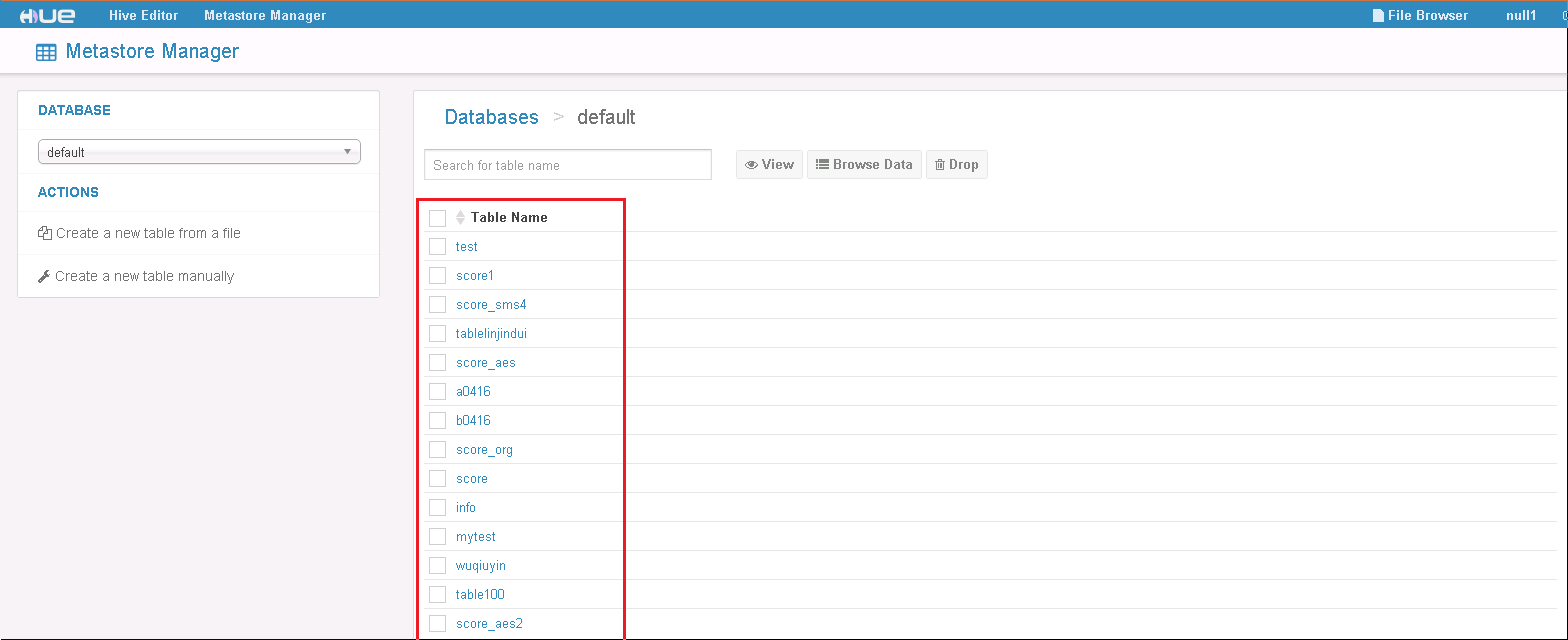


1. Null1用户可以访问所有业务组件的WEB界面，如下：

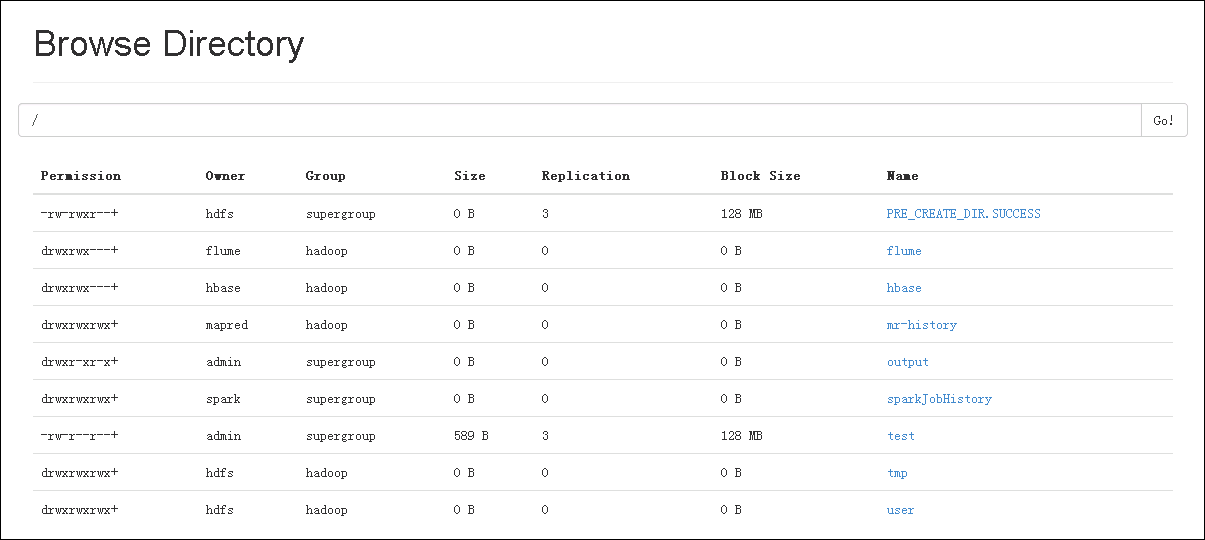
访问HBASE界面，查看到所有HBASE表名、列族名：



访问HUE界面，查看到所有HIVE表名：



访问HDFS界面，查看HDFS文件目录，并可下载权限为XX4以上的文件：



【解决方案建议】

控制无权限用户的访问权限

【问题单号及状态】

DTS2015040904342

【产品反馈】

角色的HBASE组件权限可以添加，不能删除，导致下发的权限无法回收

【问题严重等级】

提示，非红线安全问题

【问题现象】

添加一个角色，具有HBASE组件所有表的读/写权限，添加成功后，去某个表的选读/写权限失败，导致下发的权限无法回收

【解决方案建议】

【问题单号及状态】

DTS2015042905524

【产品反馈】

修改角色的时候不能将hbase权限设置为空，是当前的功能约束，如果要删除角色的hbase的权限可以通过删除角色实现。计划TR6前解决.

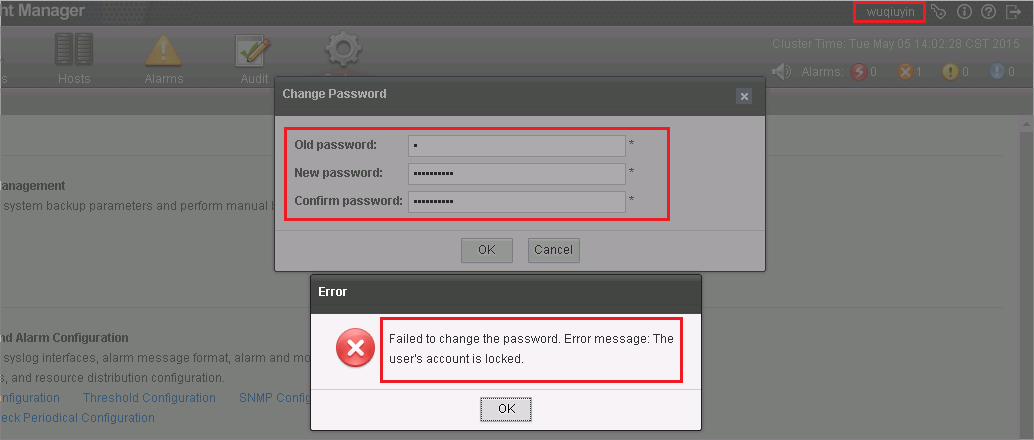
用户解锁功能权限设计不合理，用户可以给自己解锁，有破解密码风险

【问题严重等级】

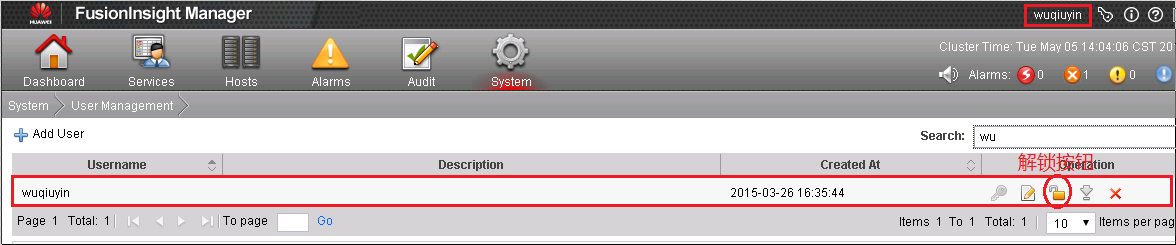
提示，非红线安全问题

【问题现象】

1. 用户登录后，修改密码输入旧密码三次错误后，用户被锁定，不能进行修改密码操作



1. 用户被锁定后，还可继续正常使用potal，用户可以给自己解锁，解锁后继续尝试旧密码，有破解密码风险



【解决方案建议】

【问题单号及状态】

[DTS2015042103256](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042103256)

【产品反馈】

用户删除后，session未过期的业务界面可以继续访问

【问题严重等级】

提示，非红线安全问题

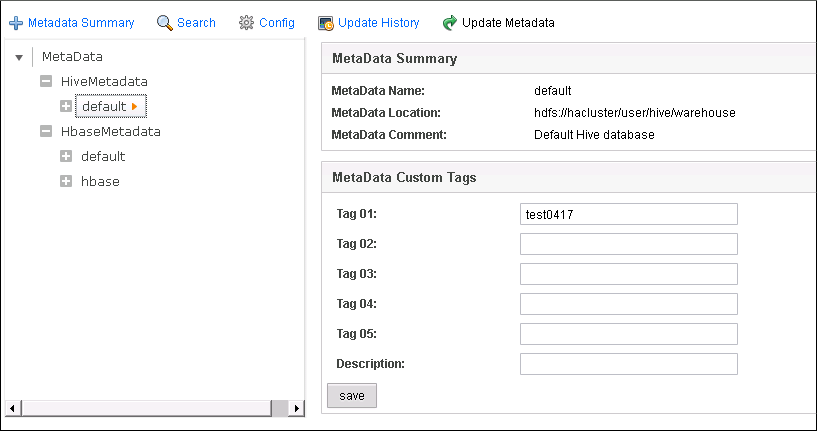
【问题现象】

用户删除后，session未过期的业务界面可以继续访问，20分钟session过期后或24小时TGT过期后访问失效。可访问的范围如下：

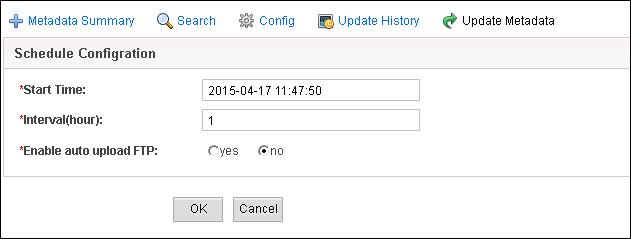
1. 目前FI的实现，对于权限的删除，是实时的；但对于权限的更改，不能实时更新，要3-5分钟才生效。同样的，对于用户删除后3-5分钟以内，用户可以继续保持原来所有的权限访问系统
2. 用户删除后3-5分钟以后，用户权限范围会收窄，

* 可以继续访问元数据管理界面，并且可以下发配置：

可设定或清除标签配置



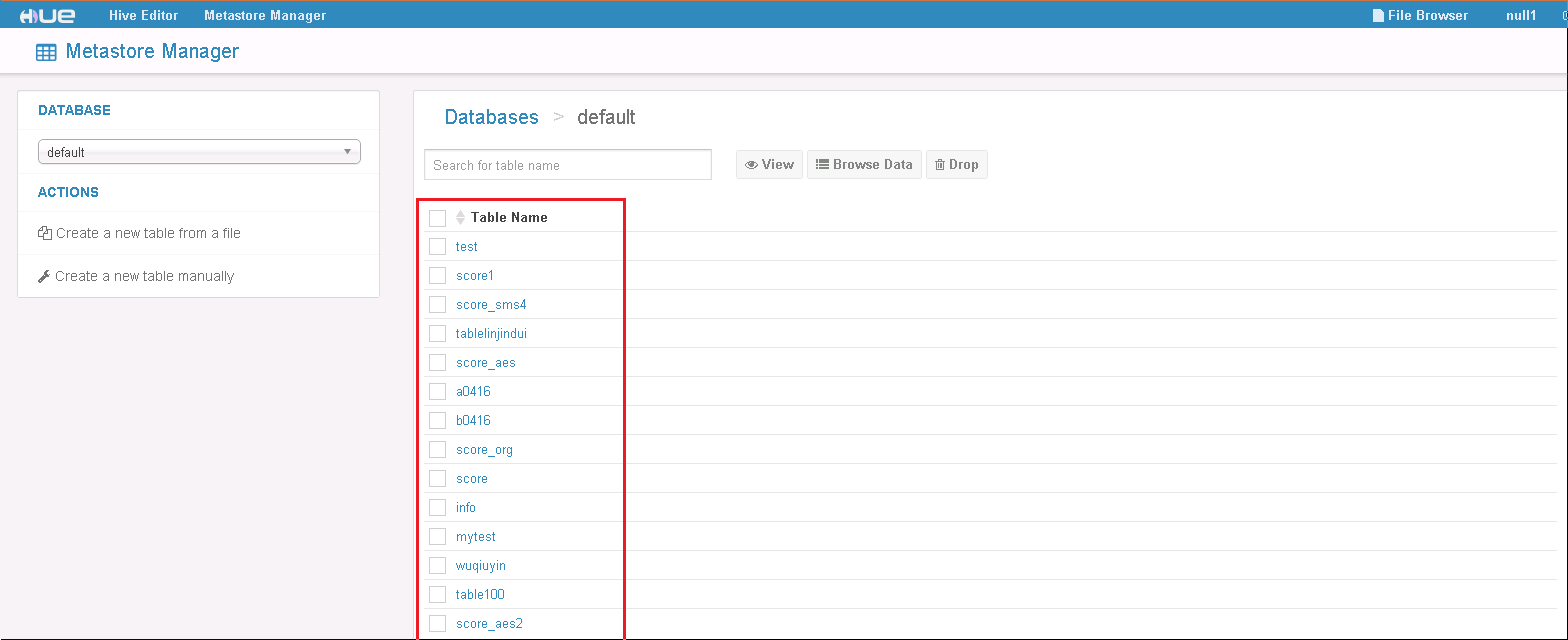
可下发定时采集元数据任务



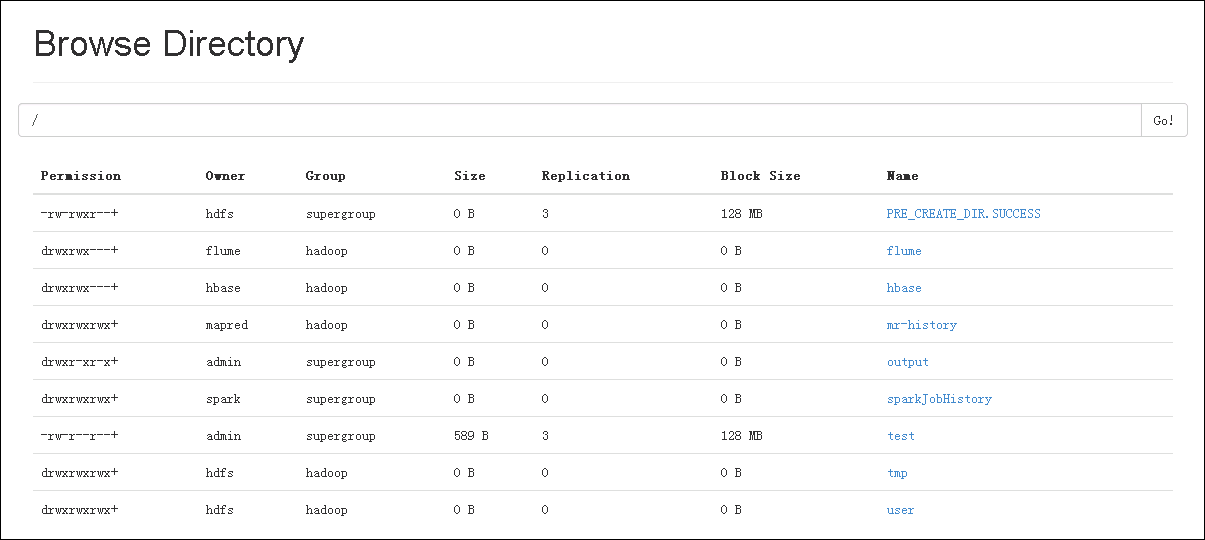
* 可以继续访问HBASE界面，查看到所有HBASE表名、列族名：



* 可以继续访问HUE界面，查看到所有HIVE表名：



* 可以继续访问HDFS界面，查看HDFS文件目录，并可下载权限为XX4以上的文件：



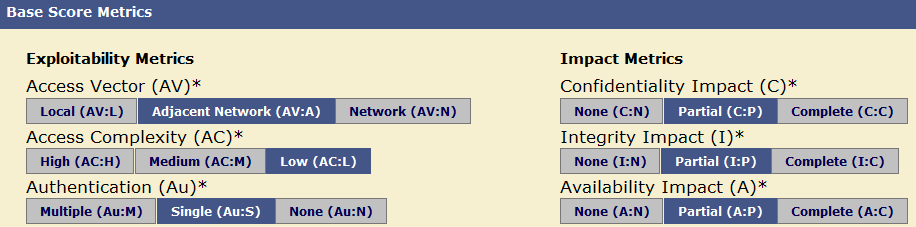
【解决方案建议】

【问题单号及状态】

DTS2015031905212

【产品反馈】

参考CVSS评分5.4分：



### 敏感数据与加密保护

后台加解密脚本AES256算法使用ECB加密模式

【问题严重等级】

提示，非红线安全问题

《密码算法应用规范 V1.0.docx》

规则：使用分组密码算法时，应优先选择CBC模式

ECB模式对于同样的明文块会生成相同的密文块，不能提供严格的数据保密性，不能抵抗替换攻击，攻击者可以调换加密块的顺序而不被发现。因此，**应禁止使用ECB模式**。

【问题现象】

密码算法应用规范中的要求AES算法要使用CBC模式，FI后台加解密脚本AES256算法使用ECB加密模。

【解决方案建议】

【问题单号及状态】

DTS2015032801342

【产品反馈】

### 隐私保护

往HIVE加密表导入数据后，系统未自动删除原表或提示用户手工删除原表，存在从原表泄露用户数据的风险

【问题严重等级】

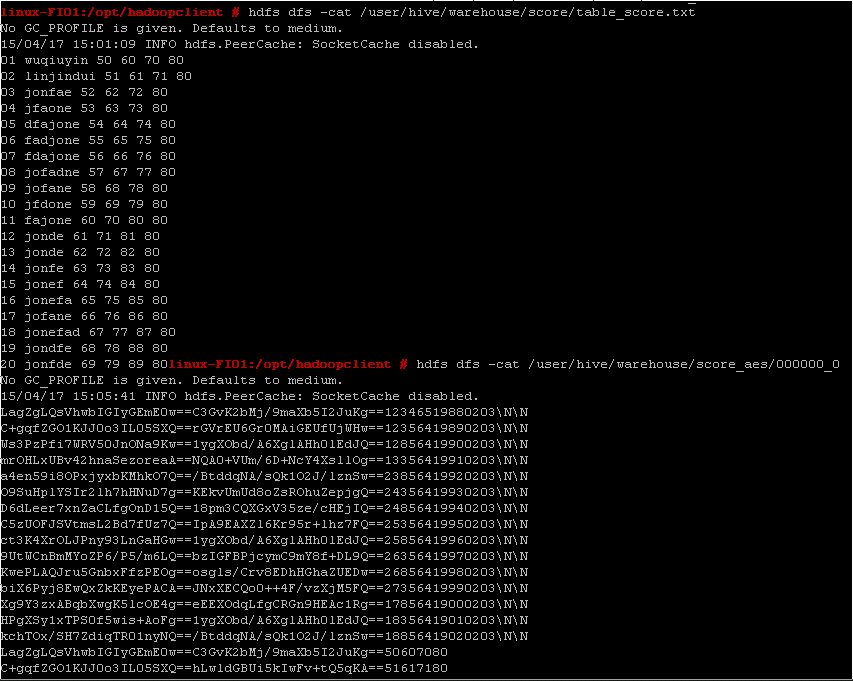
提示，非红线安全问题

【问题现象】

insert语句向HIVE加密表score\_aes导入数据后，系统未自动删除原表或提示用户手工删除原表，存在从原表泄露用户数据的风险



从后台HDFS可以看到原表score还是明文存储，加密表score\_aes已加密存储



【解决方案建议】

自动删除原数据或提醒用户删除，避免敏感的用户数据泄露

【问题单号及状态】

[DTS2015042908044](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042908044)

【产品反馈】

批量导入数据到hbase的加密表，实际数据未实现加密，存在泄露用户数据的风险

【问题严重等级】

提示，非红线安全问题

【问题现象】

为了保护用户的敏感数据，FI支持AES、SMS4两种加密算法对用户数据进行加密。目前验证批量导入数据到hbase的加密表时，发现数据文件Hfile实际未实现加密：

hdfs dfs -cat /hbase/data/default/test\_SMS4/6309c52f36310e6c3e1f32cccc46ebf1/f1/a33fc86bb2774ba38badbbc6329a35b9\_SeqId\_2\_



【解决方案建议】

【问题单号及状态】

DTS2015042402328

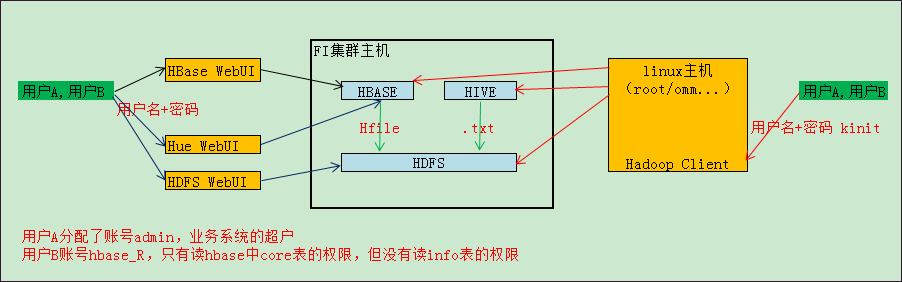
【产品反馈】

HBASE用户数据文件HFile文件权限设置为674不合理

【问题严重等级】

提示，非红线安全问题

【问题现象】



用户A通过HBase接口创建的表info，生成的HFile文件的权限为674；用户B通过HBase接口不能访问表info，但可以通过HDFS接口访问HFile文件来越权读取数据，HFile文件权限建议控制在600/700：

1. 一般情况，本用户的权限大于同组用户的权限
2. 本用户以外的其他用户权限没必要开放，请作权限最小化控制

linux-FI01:/opt/hadoopclient # hdfs dfs -ls /hbase/data/default/info/86611bf131c66af8877a4b434eebd75d/name

-rw-rwxr--+ 3 hbase hadoop 5313 2015-04-09 20:25 /hbase/data/default/info/86611bf131c66af8877a4b434eebd75d/name/3be789b114354129964b937f358009c9

-rw-rwxr--+ 3 hbase hadoop 37 2015-04-09 19:25 /hbase/data/default/info/86611bf131c66af8877a4b434eebd75d/.regioninfo

其中HIVE组件也是存在类似的问题。

【解决方案建议】

【问题单号及状态】

【产品反馈】

### 系统管理和维护安全

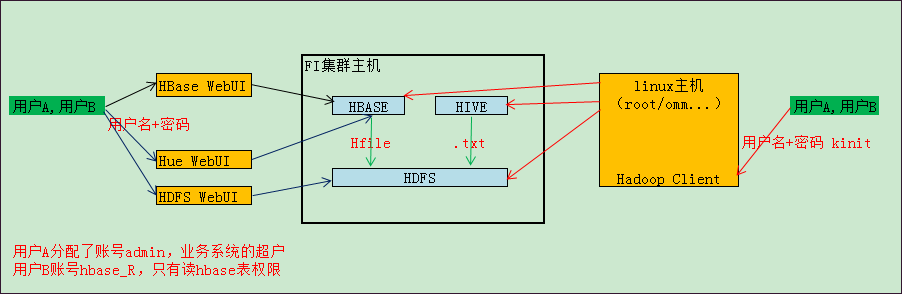
有权限的业务组件账号通过kinit认证后，本来没有权限的用户无需认证即可访问组件，存在越权访问风险

【问题严重等级】

一般问题，非红线安全问题，定级依据是CVSS基础分为 6.0（AV:L/AC:H/Au:S/C:C/I:CA:C），CVSS基础分评分说明如下：

|  |  |  |
| --- | --- | --- |
| 维度 | 评分情况 | 评分说明 |
| Access Vector | L | 本地ssh访问 |
| Access Complexity | H | admin权限的业务组件账号通过kinit认证后，攻击者才可利用 |
| Authentication | S | 需要通过一次OS登录认证 |
| Confidentiality Impact | C | 可以查看所有业务数据，导致用户数据泄露 |
| Integrity Impact | C | 可以增删改所有业务数据，破坏用户数据完整性 |
| Availability Impact | C | 可以导入大量用户数据，导致HDFS存储资源耗尽 |

【问题现象】



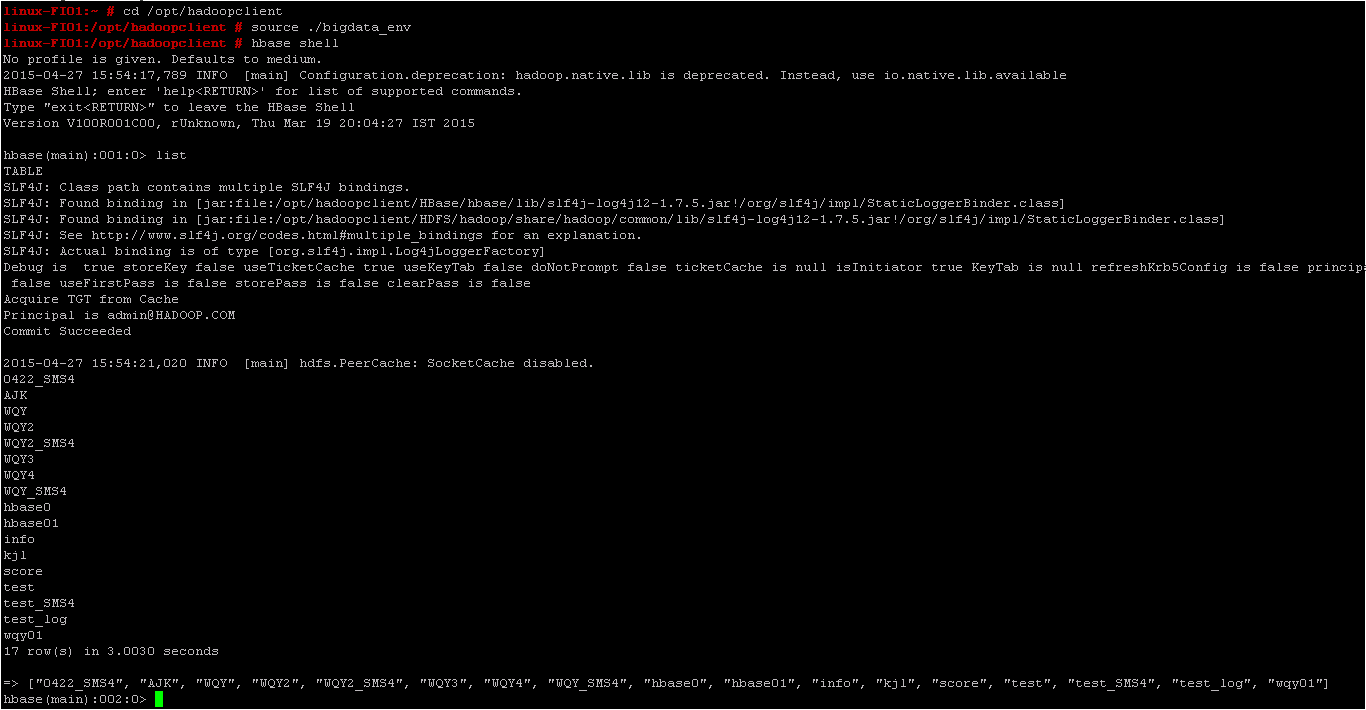
用户访问业务组件有两种接入方式，一是通过业务组件的webUI接入，一是通过安装在linux/windows主机上的hadoop client接入，其中hadoop client接入存在越权访问风险：

1. 用户A，登录linux主机FI01的OS，使用业务组件的超户账号admin通过kinit认证成功后，即可通过FI01的hadoop client接入组件



1. 用户B，管理员给B分配了一个只有读hbase表权限的账号hbase\_R，用户B与A共用一个hadoop client，B登录主机FI01的OS，无需kinit认证，即可通过FI01的hadoop client接入组件，拥有超户账号admin权限，存在越权风险。

PS：如果给B单独分配一台安装hadoop client的主机FI02去接入组件，需要重新kinit认证



【解决方案建议】

【问题单号及状态】

【产品反馈】

### 其他问题

FI存在本地不鉴权Rest接口，通过操作系统用户可以直接重置超户admin密码

【问题严重等级】

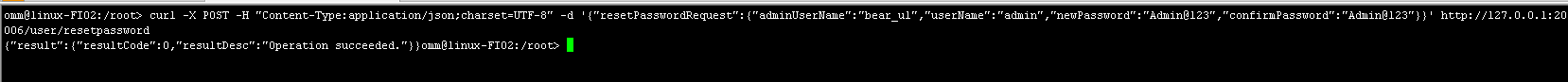
一般问题，非红线安全问题，定级依据是CVSS基础分为 6.8（AV:L/AC:L/Au:S/C:C/I:C/A:C），CVSS基础分评分说明如下：

|  |  |  |
| --- | --- | --- |
| 维度 | 评分情况 | 评分说明 |
| Access Vector | L | 本地ssh访问 |
| Access Complexity | L | 无需鉴权连接20006端口，直接发REST消息 |
| Authentication | S | 需要通过一次OS用户认证 |
| Confidentiality Impact | C | 获得系统超户admin权限后，可以查看所有管理文件和业务数据，可以重置任何用户的密码，导致所有系统文件泄露 |
| Integrity Impact | C | 可以增删改任何管理文件和业务数据 |
| Availability Impact | C | 可以删除集群等，使集群瘫痪 |

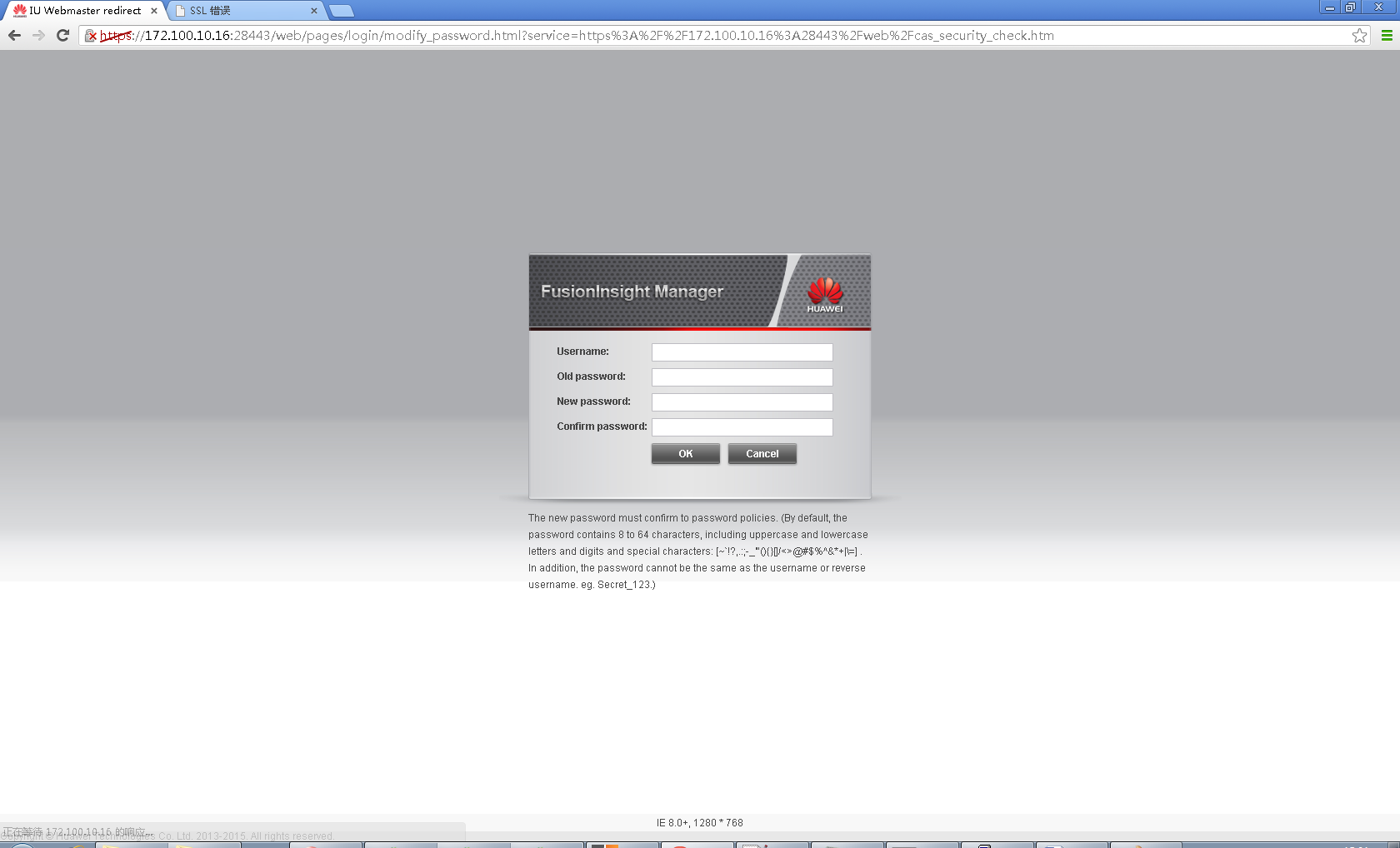
【问题现象】

1. 通过代码分析发现，FI系统中存在一个ACS模块，提供账户管理功能，包括增/删/改/查用户、修改/重置用户密码、解锁用户、用户组管理、密码策略管理等，其端口20006绑定在127.0.0.1，出Rest接口，且不需要鉴权；
2. 通过操作系统omm用户执行curl命令发送重置admin用户密码命令，执行成功：

curl -X POST -H "Content-Type:application/json;charset=UTF-8" -d '{"resetPasswordRequest":{"adminUserName":"bear\_u","userName":"admin","newPassword":"Admin@123","confirmPassword":"Admin@123"}}' http://127.0.0.1:20006/user/resetpassword



1. 通过重置后的密码登录成功，出现修改密码界面(用户重置密码后第一次登录要求修改密码)



1. 系统中有另外一个模块AOS，提供角色管理功能，存在ACS模块一样的问题

【解决方案建议】

本地Rest接口也要鉴权，防止操作系统用户直接破坏web用户

【问题单号及状态】

【产品反馈】

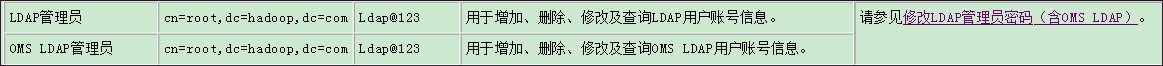
LDAP管理员用户输入多次错误密码，系统没有锁定用户

【问题严重等级】

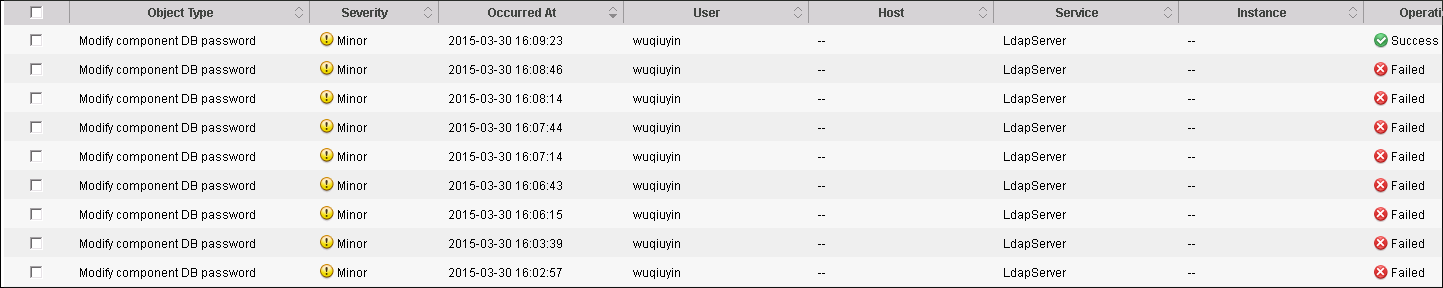
提示，非红线安全问题

【问题现象】

1.修改LDAP管理员密码时，多次（9次）输入错误的旧密码，没有锁定用户，第10次输入正确的密码可以修改密码成功



2.审计日志记录了9次出错未锁定：



【解决方案建议】

当前的消减措施要有公司能力中心评审后，才能关闭问题

【问题单号及状态】

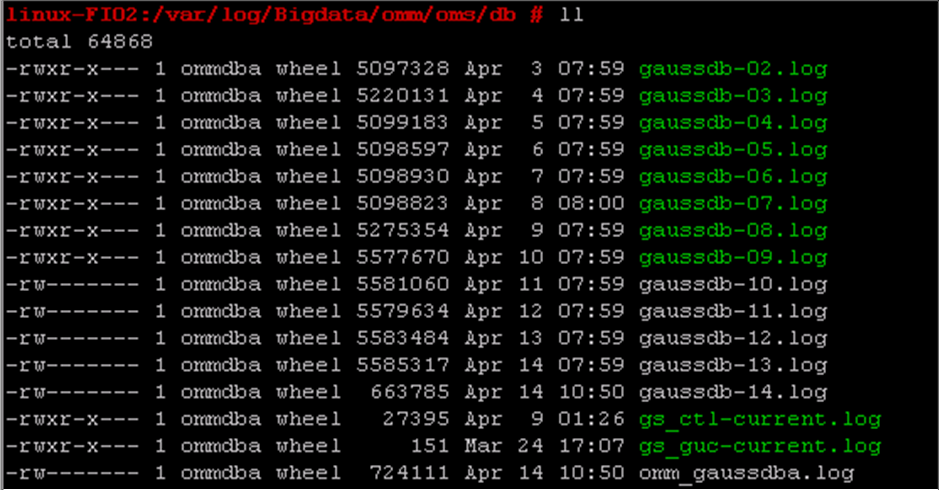
【产品反馈】

日志文件权限过大750，建议设置为600

【问题严重等级】

提示，非红线安全问题

【问题现象】

日志文件权限过大750，建议设置为600

【解决方案建议】

【问题单号及状态】

【产品反馈】

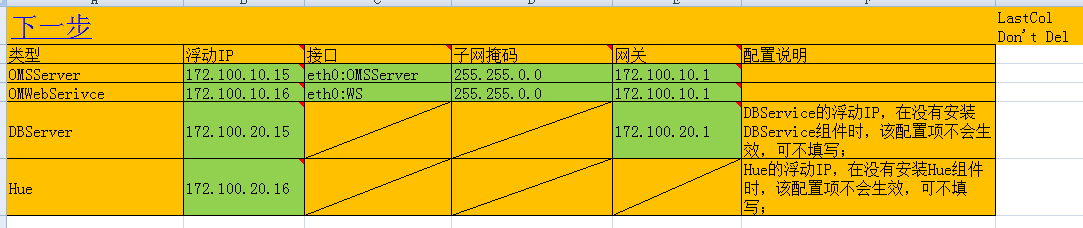
环境搭建的配置规划工具有问题，在有物理业务网口的情况下，将属于业务面的DBServer 和Hue的浮动IP默认绑定到管理网口的子接口上，业务面、管理面没有物理隔离

【红线等级】

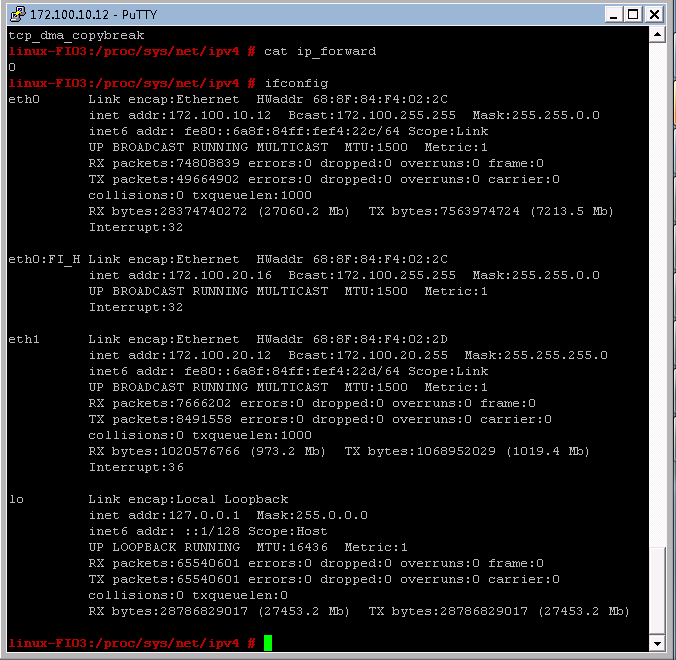
提示，非红线安全问题

【问题现象】









【解决方案建议】

【问题单号及状态】

DTS2015041005049

【产品反馈】

### 安全资料

对于FI依赖的OS服务，请统一提供OS加固策略

【问题严重等级】

提示，非红线安全问题

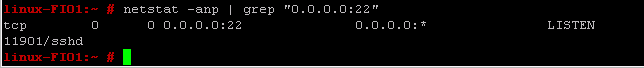
【问题现象】

1. 问题一：22端口同时在管理面和业务面放通，导致可以通过业务面IP连接后台OS系统。请提供统一的OS加固策略说明其依赖的22端口绑定到管理平面的具体IP。

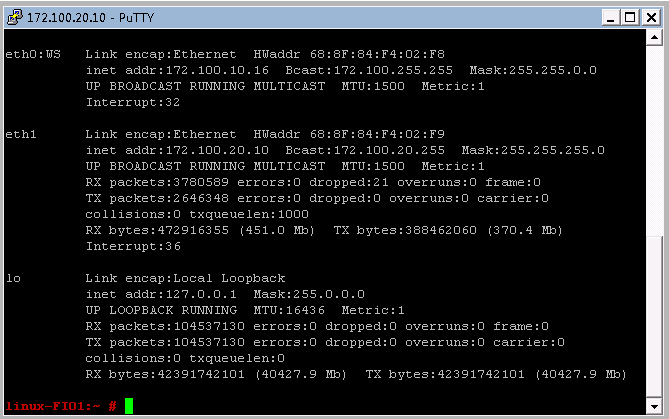
172.100.20.10是业务IP



后台操作系统中端口22是通配监听



ssh 172.100.20.10可以登录后台OS系统，正常应该只能ssh 172.100.10.10登录后台OS系统



1. 问题三： FI产品创建的操作系统用户omm、ommdba，没有防暴力破解

FI产品创建的操作系统用户omm、ommdba，多次输入密码错误不锁定，没有防暴力破解，也没有密码复杂度等密码策略。



1. 问题三：FI使用的OpenSSL 0.9.8j-fips 07 Jan 2009版本存在业界已知漏洞，请提供统一的OS加固策略说明其风险

OpenSSL版本如下：

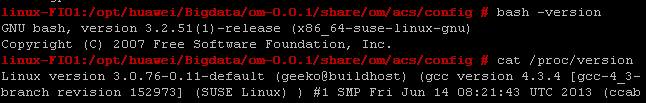


Openssl漏洞列表如下：

|  |  |  |
| --- | --- | --- |
| 漏洞CVE编号 | 漏洞名称 | 受影响的版本 |
| CVE-2014-0224 | SSL/TLS Man-in-the-Middle Vulnerability | Server：1.0.1 和1.0.2-beta1  Client：所有版本 |
| CVE-2014-0221 | DTLS Recursion Flaw Vulnerability | 所有版本 |
| CVE-2014-0195 | DTLS Invalid Fragment Vulnerability | 所有版本 |
| CVE-2014-0198 | SSL\_MODE\_RELEASE\_BUFFERS NULL Pointer Dereference Vulnerability | 1.0.0 和1.0.1 |
| CVE-2012-2110 | Denial of Service Vulnerability | 0.9.8；1.0.0 和1.0.1 |
| CVE-2014-3470 | Anonymous ECDH Denial of Service Vulnerability | 0.9.8；1.0.0 和1.0.1 |
| CVE-2014-0076 | ECDSA NONCE Side-Channel Recovery Attack Vulnerability | 0.9.8；1.0.0 和1.0.1 |
|  |  |  |
|  |  |  |

1. 问题四：FI配套的Linux系统suse11.3版本的bash版本存在业界已知漏洞，请提供统一的OS加固策略说明其风险

当前系统使用bash版本是3.2.51（1）已发布存在如下CVE-2014-6271、CVE-2014-7169、CVE-2014-7186和CVE-2014-7187等4个漏洞，需要在系统加固指导书上增加该安全修复建议



【解决方案建议】

在CPI资料中将涉及到OS服务的章节，增加OS加固说明

【问题单号及状态】

DTS2015040904438

【产品反馈】

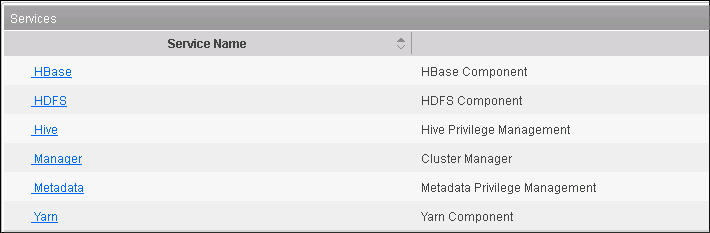
资料未提供业务组件管理员修改密码的方法

【问题严重等级】

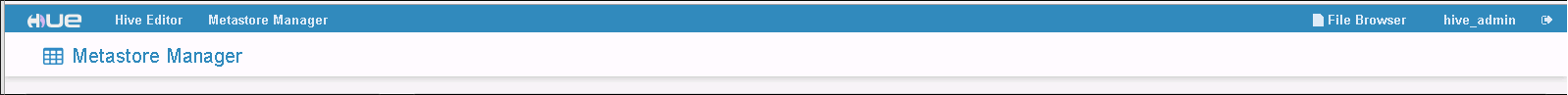
提示，非红线安全问题

【问题现象】

1. 在MANAGER上创建的业务组件权限（hbase,hdfs,hive,metadata,yarn）的人机账户



1. 使用此账户登录业务组件界面，用户在界面上不能修改自己的密码



【解决方案建议】

【问题单号及状态】

[DTS2015042102727](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042102727)

【产品反馈】

Admin用户实际权限与资料不一致

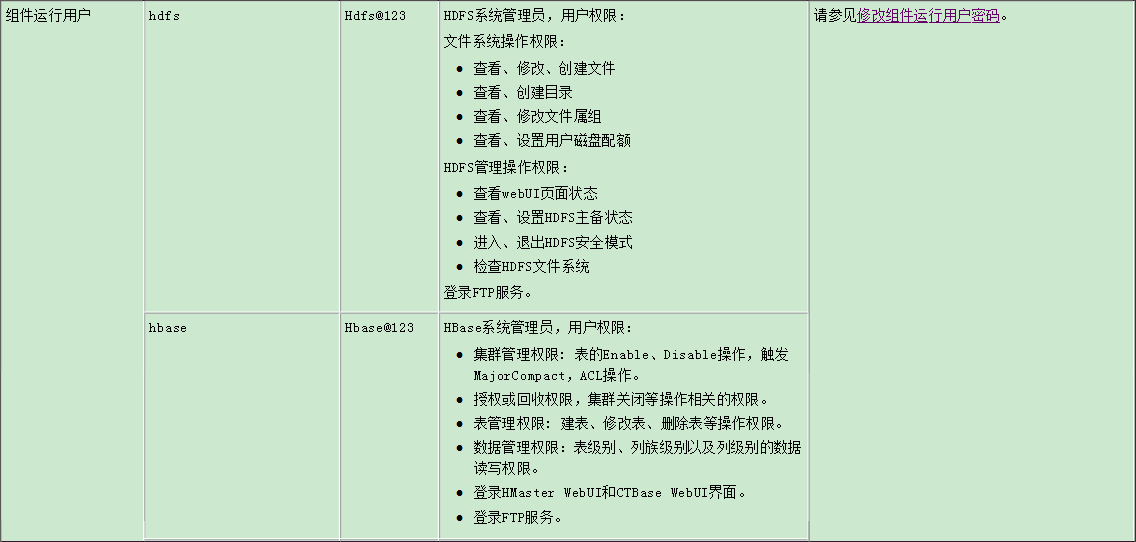
【问题严重等级】

提示，非红线安全问题

【问题现象】

CPI资源里对Admin用户定义为FusionInsight Manager系统管理员用户，但实际上不仅仅是Manager系统管理员用户，其还具备所有组件的业务访问权限，如创建表、增删业务数据等。





【解决方案建议】

建议系统管理员和业务管理员权限分离

【问题单号及状态】

[DTS2015042102877](http://dts.huawei.com/net/dts/DTS/DTSWorkFlowPage.aspx?No=DTS2015042102877)

【产品反馈】

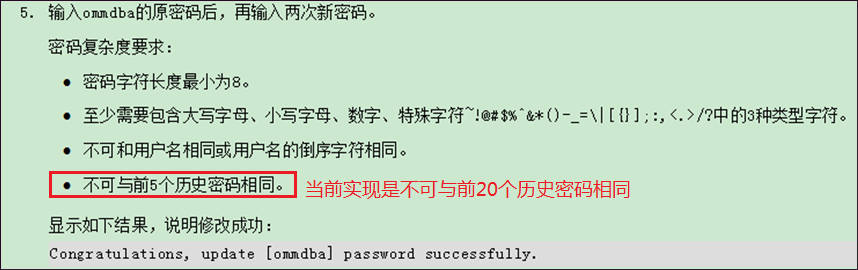
修改密码步骤中的密码策略资料描述不正确

【问题严重等级】

提示，非红线安全问题

【问题现象】

1. 修改OMS数据库管理员密码中的密码策略描述不正确，“不可与前5个历史密码相同”，请修改为“不可与前20个历史密码相同”
2. 修改OMS数据库数据访问用户密码有同样的问题



【解决方案建议】

【问题单号及状态】

DTS2015040904533

【产品反馈】

# 附录

## 代码扫描结果

### Nmap扫描报告

通过端口扫描工具nmap对FC做TCP和UDP端口扫描（UDP当初使用命令检查，正在补充工具检查报告，待扫描完添加进来），对比产品通信矩阵文档，扫描结果同产品通信矩阵文档，符合公司红线安全要求。



### Codecc(Fortify)扫描报告

通过源代码安全扫描工具Codecc对产品源代码做扫描，扫描结果如下。把垃圾代码及工具误报的屏蔽后，所有通过。



### Appscan扫描报告

通过Web漏洞扫描工具Appscan对FI的Web系统进行扫描，报告存在2个中风险级别问题，经过验证属于工具误报，实际不存在工具报告中的风险，符合公司红线安全要求。



### SecureCAT扫描报告

使用安全配置评估工具SecureCAT对FI的高斯数据库进行评估，不存在“高”风险的漏洞，评估结果89分，符合公司红线安全要求。



## 版本配套表

| 软件类型 | 软件版本 |
| --- | --- |
| GaussDB | V100R003C10SPC083 |
| DataSight | BasePlatform\_V100R001C00SPC500 |
| Hadoop | 2.4.1 |
| Zookeeper | 3.4.6 |
| HBase | 0.98.3 |
| Hive | 0.13.1 |
| Spark | 1.1 |
| Sqoop | 1.99.3 |
| Flume | 1.4.0 |
| Hue | 3.6.0 |
| Kerberos | 1.10.1 |
| Ladp | OS自带 |
| Tomcat | 7.0.57 |
| JDK | 1.7.0\_72 |

开源组件配套表：

结束