计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(1):1−9 [doi: 10.15888/j.cnki.csa.006169]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

Hadoop 大数据平台安全问题和解决方案的综述①

陈　丽[1], 黄　晋[2], 王　锐[3]

[1](广东交通职业技术学院 信息学院, 广州 510650)
[2](华南师范大学 计算机学院, 广州 510631)
[3](中国移动通信集团广东有限公司, 广州 510623)

摘　要: 大数据时代的到来, 更强的计算机和更成熟的大数据平台工具让企业从海量数据中挖掘数据价值成为了可能, 尤其是基于 Hadoop 的大数据平台, 甚至利用廉价的商业硬件处理 TB、PB 级别的数据. 在最初 Hadoop 大数据平台落地建设的过程中, 往往功能先行, 而忽略了安全的管控策略, 直到 2009 年 Yahoo 团队提出了基于 Kerberos 的身份验证方案, 才带动了 Hadoop 大数据平台安全管控工作的全面开展. 本文介绍了 Hadoop 大数据平台的基本历程, 描述了 2009 年之前 Hadoop 大数据平台存在的传统安全问题, 并尝试着将目前行业内 Hadoop 生态系统组件的安全性和每个组件的安全解决方案做一次系统的梳理, 希望为构建 Hadoop 大数据平台管控方案时提供参考意见, 以便合理利用先进的安全管控方案保护好企业、用户的隐私数据.

关键词: 大数据; Hadoop; 身份验证; 授权; 数据安全; 审计

引用格式: 陈丽,黄晋,王锐.Hadoop 大数据平台安全问题和解决方案的综述.计算机系统应用,2018,27(1):1–9. http://www.c-s-a.org.cn/1003-3254/6169.html

Overview on Security Issues and Solutions of Hadoop Big Data Platform

CHEN Li[1], HUANG Jin[2], WANG Rui[3]

[1](School of Information, Guangdong Communication Polytechnic, Guangzhou 510650, China)
[2](School of Computer, South China Normal University, Guangzhou 510631, China)
[3](China Mobile Group Guangdong Co. Ltd., Guangzhou 510623, China)

Abstract: With the arrival of the big data era, more powerful computers and more mature big data platform tools for enterprises from the massive data mining data value has become possible, especially based on Hadoop Big Data Platform, which can even handle TB, PB level of data with cheap commercial hardware. In the initial construction process of Hadoop Big Data Platform, the first step often starts with the building function, ignoring the security control strategy. The Yahoo team proposed Kerberos-based authentication scheme in 2009, which led to the Hadoop Big Data Platform security control work in full swing. This article introduces the history of the Hadoop Big Data Platform. Then, it describes the traditional security issues existing in Hadoop Big Data Platform before 2009. Finally, it tries to present the security of the Hadoop ecosystem components in the industry and the security solution for each component. We hope to provide reference for the construction of Hadoop Big Data Platform security, so people can reasonably use advanced security control program to protect the enterprise's and user's privacy data.

Key words: big data; Hadoop; authentication; authorization; data security; audit

所谓大数据, 狭义上可以定义为难以用现有的一般技术管理的大量数据的集合. 大数据难以管理的原因, 可以用 3V 来描述即 Volume(容量)、Variety(多样性)、Velocity(产生频率、更新频率)[1], 如图 1 所示.

① 基金项目: 广东省自然科学基金 (2016A030313437); 广东省重大科技专项 (2016B030305004)
收稿时间: 2017-04-08; 修改时间: 2017-05-04; 采用时间: 2017-05-16; csa 在线出版时间: 2017-11-14

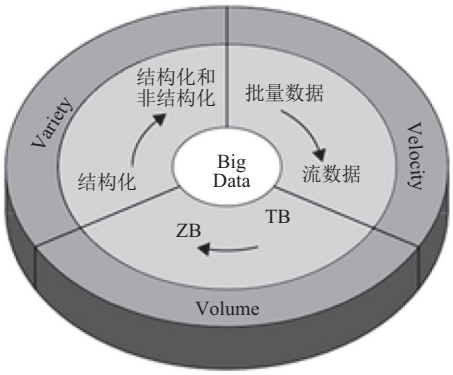

图 1 大数据的 3V 描述

从广义上来说, 大数据可以定义为包括因具备 3V 特征而难以进行管理的数据, 对这些数据进行存储、处理、分析的技术, 以及能够通过分析这些数据获得实用意义和观点的人才和组织的综合性概念[2].

对大量数据进行分析, 并从中获得有用观点这种做法, 过去就已经存在于一部分研究机构和大企业中. 现在的大数据和过去相比, 主要有 3 点区别[3]. 第一, 随着社交媒体和传感器网络等的发展, 在我们身边正产生出大量且多样的数据. 第二, 随着硬件和软件技术的发展, 数据的存储、处理成本大幅下降. 第三, 随着云计算的兴起, 大数据的存储、处理环境已经没有必要自行搭建.

大数据处理技术起源于 Google. Google 提出了一整套基于分布式并行集群方式的基础架构技术, 利用软件的能力来处理集群中经常发生的节点失效问题. Google 使用的大数据平台主要包括五个相互独立又紧密结合在一起的系统: 分布式资源管理系统 Borg[4], Google 文件系统 (GFS)[5], 针对 Google 应用程序的特点提出的 MapReduce 编程模式[6], 分布式的锁机制 Chubby[7]以及大规模分布式数据库 BigTable[8]. 而这些先进的大数据处理技术在 Doug Cutting 的牵头下开发了 Hadoop 开源软件, 支持在廉价商业硬件构建的大型集群上运行的应用程序, 这也是如今大数据技术和应用的飞速发展的关键推动力.

早期的 Hadoop, 包括 Hadoop v1 以及更早之前的版本, 主要由两个核心组件构成: HDFS 和 MapReduce. 其中 HDFS 是 Google GFS 的开源版本, MapReduce 计算框架实现了由 Google 工程师提出的 MapReduce 编程模型. 还有一些围绕在 Hadoop 周围的开源项目, 为完善大数据处理的全生命周期提供了必要的配套和补充. 这些软件常用的有 ZooKeeper、Hive、Pig、HBase、Storm、Kafka、Flume、Sqoop、Oozie、Mahout 等. 2012 年 5 月, Hadoop v2 的 alpha 版本发布, 其中最重要的变化是在 Hadoop 核心组件中增加了 YARN (Yet Another Resource Negotiator)[9]. YARN 的出现是为了把计算框架与资源管理彻底分离开, 解决 Hadoop v1 由此带来的扩展性差、单点故障和不能同时支持多种计算框架的问题.

Hadoop 是目前最为流行的大数据处理平台之一, 围绕 Hadoop 平台安全也已存在大量的研究工作, 但研究方向主要是对具体 Hadoop 平台的安全隐患研究和具体的 Hadoop 组件安全方案的优化实现, 缺少以 Hadoop 平台总体的安全问题和各个组件的解决方案为主题的综述型文章. 本文致力于填补这个研究方向上的空白. 本文首先介绍了 Hadoop 平台传统安全问题; 然后从身份验证、访问授权、数据加密和操作审计四个安全管控方向说明了 Hadoop 平台上述这些传统安全问题的解决方法, 并细化到具体组件, 包括: HDFS、YARN、HBase、Hive、Pig、Oozie、Zookeeper、Hue; 再次从工业界视角, 阐述了目前可投入实际生产环境中的大数据平台安全技术方案; 最后对全文进行总结并提出进一步研究方向.

1 Hadoop 平台传统安全问题

最初的 Hadoop 在开发时考虑的是功能优先, 因此没有过多的考虑安全问题, 没有安全管控方案, 没有用户/服务的身份认证, 也没有数据的隐私考虑, 而且集群中的任意用户均可以向集群提交作业任务[10]. 随着业务发展的需求, Hadoop 增加了审计和授权的机制 (主要是 HDFS 文件的访问权限和 ACL), 但因为依旧缺乏身份验证机制, 所以早期的安全方案很容易被恶意用户使用身份伪装的方式轻易绕过, 大数据平台的安全一直令人顾虑. 相对于庞大的 Hadoop 集群, 传统的安全管控方案愈发显得不足, 主要存在以下问题[11].

(1) 善意的用户偶尔也会犯错 (如: 误操作导致大量数据被删除);

(2) 任意用户、程序均可以通过 Hadoop 客户端或编程方式访问到 Hadoop 集群内的全部数据, 因为 HDFS 中用户身份可以随意申明而且无检查机制[12];

(3) 任意用户均可以向集群提交任务[13]、查看其他人的任务状态、修改任务优先级甚至强行杀死别人

正在运行的程序, 因为 MapReduce 任务没有身份验证和授权的概念[14].

```
[hack@edgeNode3 ~]$ HADOOP_USER_NAME=hdfs hadoop fs -rm -r /some/important/data
```

图 2 HDFS 中用户身份可随意申明

如今的大数据平台 Hadoop 如今已经不仅仅是 HDFS 加 MapReduce, 还包括了生态圈中众多的组件. 行业内的 Hadoop 大数据的平台一般不仅包括 Hadoop 核心组件: Hadoop Common、HDFS、YARN, 一般还包括与核心组件配套使用的主流组件: Zookeeper、HBase、Hive、Pig、Oozie、Hue 等. 各组件介绍如下.

(1) Hadoop Common: Hadoop 框架基础类库, 包含文件系统、RPC 协议和数据串行化库等, 提供基础支撑性的功能.

(2) HDFS: 分布式文件系统, 具有高度容错性的特点, 能提供高吞吐量的数据访问, 适合有超大数据集的应用程序.

(3) YARN: 集群资源调度器, 提供集群计算资源 (CPU、内存) 资源的集中管控和调度, 提供任务进度的集中管控, 支持多种分布式计算框架, 含 Spark、MapReduce、Tez 等, 可以有效提升集群机器资料利用率.

(4) Zookeeper: 利用 Paxos 算法解决消息传递一致性的分布式服务框架, 主要是用来解决分布式应用中经常遇到的一些数据管理问题, 如: 统一命名服务、状态同步服务、集群管理、分布式应用配置项的管理等; 分布式协调服务很难正确无误的实现, 它们很容易在竞争条件和死锁上犯错误, Zookeeper 的出现为上述场景提供了优秀的解决方案.

(5) HBase: 分布式的、面向列的开源数据库, 适合于结构化和非结构化数据存储, 依托 HDFS, 具备高可靠性、高性能、可伸缩, 能在大量数据中进行实时查询.

(6) Hive: 面向数据实时性要求低的海量数据查询, 基于 SQL, 结合自定义的复杂组合查询函数实现目标业务搜索, 依托 HDFS, 数据可靠安全, 但不支持删除、更新、中间插入.

(7) Pig: 使用专属分析语言 (Pig Latin) 的大数据分析工具, 支持并行化处理, 适合数据准备阶段对大量快速到达的数据进行 ETL 处理, 并能对大规模数据集进行迭代处理.

(8) Oozie: 分布式任务调度系统, 使用 DAG(有向无环图 Direct Acyclic Graph) 来定义工作流程以及每一个环节具体的操作动作.

(9) Hue: 可快速开发和调试 Hadoop 生态系统各种应用的一个基于浏览器的图形化用户接口, 支持 HDFS 文件浏览、HBase 数据查看和修改、Hive 元数据查看、Spark 任务开发调试、MapReduce 任务进度追踪、Zookeeper 浏览和编辑、Oozie 任务的开发和监控等众多功能.

随着 Hadoop 大数据平台应用的广泛性和重要性日渐提高, 安全问题又被众多组织机构提上议程, 然而 Hadoop 大数据平台的安全确实相当复杂的问题, 因为涉及的组件非常之多、技术非常之复杂, 以及数据量、计算规模都非常大之, Hadoop 大数据平台需要的是一个能满足众多组件且能横向扩展的安全管控方案.

终于在 2009 年, Yahoo 在 Hadoop 安全管控上提出了系统而全面的解决思路, 作出了实质性的贡献; 2013 年, Intel 牵头启动了开源项目“Project Rhino”, 致力于为 Hadoop 生态组件安全和数据安全提供增强能力的保证. 通过 Hadoop 社区众多贡献者的共同努力, 目前已经提供了一套可以解决上述问题的基本解决方案, 主要是通过引入 Kerberos, 配置防火墙、基础的 HDFS 权限和 ACLs 实现. Kerberos 其实并不是建设 Hadoop 集群必备, 而是更贴近操作系统层面的一套身份验证系统, 且其搭建以及与 Hadoop 服务整合的配置工作还是非常复杂的, 因而在易用性方面一直没有能够获得比较好的效果, 这也使得该 Hadoop 的安全管控方案在行业内实践依旧很少.

缺少有效身份验证的安全解决方案 (Kerberos) 而只剩下防火墙、HDFS 权限和 ACLs 的管控方案是不足以提供安全保证的, 恶意用户只要可以穿透防火墙, 就可以使用身份伪装的方式任意读取集群中的数据, 这些安全隐患包括但不限于以下 9 条.

(1) 未授权的用户可以通过 RPC 或 HTTP 访问 HDFS 上的文件, 并可以在集群内执行任意代码.

(2) 未授权的用户可以直接使用相应的流式数据传输协议直接对 DataNode 中的文件块进行读写操作.

(3) 未授权的用户可以私下为自己授权从而可以向集群的任意队列提交任务、修改其他用户任务的优先级, 甚至删除其他用户的任务.

(4) 未授权的用户可以通过 HTTP shuffle protocol

直接访问一个 Map 任务的中间输出结果.

(5) 一个任务可以通过操作系统的接口访问其他正在运行的任务, 或直接方案运行任务所在节点 (一般是一台 DataNode) 的本地磁盘数据.

(6) 未授权用户可以截获其他用户客户端和 DataNode 通信的数据包.

(7) 一个程序或节点可以伪装成 Hadoop 集群内部的服务, 如: NameNode、DataNode 等.

(8) 恶意用户可以使用其他用户身份向 Oozie 提交任务.

(9) 由于 DataNode 自身无文件概念 (只有数据块的概念), 恶意用户可以无视集群的 HDFS 文件权限和 ACLs 而直接读取 DataNode 中的任意数据块.

综上所述, 传统的 Hadoop 平台建设优先考虑的是功能和性能, 对于安全问题没有重点考虑, 这给恶意用户留下了利用安全漏洞的隐患, 对于善意用户也留下了错误操作影响超预期的隐患. 虽然 Hadoop 行业领先企业、开源社区都提出了一些安全管控的方案, 但实际上工业界普及率仍然很低, 安全问题依旧需要引起重视.

2 Hadoop 平台安全问题解决方法

Hadoop 是一个分布式系统, 它允许我们存储大量的数据, 以及还可以并行处理数据. 因为支持多租户服务, 不可避免的会存储用户相关的敏感数据, 如个人身份信息或财务数据. 对于企业用户而言, 其 Hadoop 大数据平台存储的海量数据往往也包含了用户相关的敏感数据, 这些数据仅可以对有权限的真实用户可见, 因此需要强大的认证和授权.

Hadoop 生态系统由各种组件组成, 需要保护所有其他 Hadoop 生态系统组件. 这些 Hadoop 组件一般都会被最终用户直接访问或被 Hadoop 核心组件内部 (HDFS 和 Map-Reduce) 访问. 2009 年, Yahoo 团队发表论文[15]选择使用 Kerberos 做为 Hadoop 平台的身份验证方案, 为 Hadoop 大数据平台的安全管控方案提供了坚实的基础, 从此 Hadoop 生态系统的安全管控突飞猛进. 我们尝试着将每个生态系统组件的安全性和每个组件的安全解决方案做一次系统的梳理, 每个组件都有自己的安全挑战, 需要采取特定的方案并根据需求进行正确配置才可以确保安全.

Hadoop 大数据平台安全问题主要在两方面有体现: 第一, 对内部 Hadoop 大数据平台需要支持多租户安全, 确保用户的身份是可信的且具备细粒度的访问权限控制, 保证操作不能相互影响, 数据是安全隔离的; 第二, 对外部 Hadoop 大数据平台需要支持禁止匿名用户访问, 禁止恶意窃取用户信息, 确保用户的操作都是被审计的, 有据可查, 保证用户数据是被加密的, 避免泄露数据导致信息被窃取.

针对上述 Hadoop 大数据平台安全的两大方面的问题, 解决时需要针对其全部组件, 并从身份验证、访问授权、数据加密和操作审计[16,17]四个方向给出解决方案.

2.1 身份验证

身份验证指验证访问系统的用户标识. Hadoop 提供 Kerberos 作为主身份验证. 最初, SASL/GSSAPI 用于实现 Kerberos, 并通过 RPC 连接相互验证用户, 应用程序和 Hadoop 服务. Hadoop 还支持 HTTP Web 控制台的“Pluggable”身份验证, 意味着 Web 应用程序和 Web 控制台的实现者可以为 HTTP 连接实现自己的身份验证机制, 这包括但不限于 HTTP SPNEGO 身份验证.

Hadoop 组件支持 SASL 框架, RPC 层可以根据需要选择 SASL Digest-MD5 认证或 SASL GSSAPI/Kerberos 认证[18], 详细如下.

(1) HDFS: NameNode 和 DataNode 之间的通信通过 RPC 连接, 并在它们之间执行相互 Kerberos 认证[19].

(2) YARN: 支持 Kerberos 身份验证, SASL Digest-MD5 身份验证以及 RPC 连接上的委派令牌身份验证.

(3) HBase: 支持通过 RPC, HTTP 的 SASL Kerberos 客户端安全认证.

(4) Hive: 支持 Kerberos 和 LDAP 认证, 也支持通过 Apache Knox 的认证.

(5) Pig: 使用用户票据将作业提交到 Hadoop, 因此, 不需要任何额外的 Kerberos 安全认证, 但在启动 Pig 之前, 用户应该使用 KDC 进行身份验证并获取有效的 Kerberos 票据.

(6) Oozie: 可以为 Web 客户端提供 Kerberos HTTP 简单和受保护的 GSSAPI 协商机制 (SPNEGO) 身份验证, 当客户端应用程序想要向远程服务器进行身份验证, 但不能确定要使用的身份验证协议时, 将使用 SPNEGO 协议.

(7) Zookeeper: 在 RPC 连接上支持 SASL Kerberos

身份验证.

(8) Hue: 提供 SPENGO 身份验证, LDAP 身份验证, 现在还支持 SAML SSO 身份验证.

Hadoop 认证涉及多个数据流: Kerberos RPC 认证机制用于用户认证、应用程序和 Hadoop 服务, HTTP SPNEGO 认证用于 Web 控制台, 以及使用委托令牌. 委托令牌是用户和 NameNode 之间用于认证用户的双方认证协议, 它比 Kerberos 使用的三方协议更加简单而且运行效率更高, Oozie、HDFS、MapReduce 均支持委托令牌.

2.2 访问授权

授权是为用户或系统指定访问控制权限的过程. Hadoop 中, 访问控制是遵循 UNIX 权限模型的、基于文件的权限模型来实现的, 具体如下.

(1) HDFS: NameNode 基于用户、用户组的文件权限对 HDFS 中文件进行访问控制.

(2) YARN: 为作业队列提供 ACL, 定义哪些用户或组可以将作业提交到队列以及哪些用户或组可以更改队列属性.

(3) HBase: 提供对表和列族的用户授权, 使用协处理器来实现用户授权. 协处理器就像 HBase 中的数据库触发器, 它们在前后拦截了对表的任何请求, 目前 HBase 还支撑对单元级别超细粒度访问控制.

(4) Hive: 可以依赖 HDFS 的文件权限进行控制, 也可以使用类似于 SQL 的方式实现对数据库、数据表甚至字段级别超细粒度的访问控制.

(5) Pig: 使用 ACL 为作业队列提供授权.

(6) Oozie: 提交的任务的权限依赖 YARN 定义的任务队列提交的权限控制.

(7) Zookeeper: 提供使用节点 ACL 的授权.

(8) Hue: 通过文件系统权限提供访问控制; 它还提供作业队列的 ACL.

尽管 Hadoop 可以设置为通过用户和组权限和访问控制列表 (ACL) 执行访问控制, 但这可能不足以满足每个企业的需要, 因为各个组件均有自己的一套管控体系导致管控入口分散, 各个组件管控的具体操作方式也各异, 导致运维实施操作时复杂度高. 因此一般的会采用一些集成的解决方案, 将访问授权以集中的、可视化的方式封装起来[20], 降低运维操作的复杂度, 提升效率, 这些解决方案包括: Apache Ranger、Cloudera Sentry 等.

2.3 数据加密

加密确保用户信息的机密性和隐私性, 并且保护 Hadoop 中的敏感数据[21]. Hadoop 是在不同的机器上运行的分布式系统, 这意味着数据在网络上定期传输是不可避免的, 而且对于数据挖掘的需求会要求这些数据持续不断地写入到集群. 数据写入或读出集群时, 称之为运动的数据, 数据保存在集群内部时, 称之为静止的数据, 全面的数据加密方案需要同时兼顾运动的数据加密和静止的数据加密[22], 常见的数据加密保护策略包括以下两条.

(1) 运动的数据加密保护策略: 在数据传输到 Hadoop 系统和从 Hadoop 系统读出数据时, 可以使用简单认证和安全层 (SASL) 认证框架用于在 Hadoop 生态系统中加密运动中的数据. SASL 安全性保证客户端和服务器之间交换的数据, 并确保数据不会被“中间人”读取. SASL 支持各种身份验证机制, 例如 DIGEST-MD5, CRAM-MD5 等.

(2) 静止的数据加密保护策略: 静止的数据可以通过两种方案加密, 方案一: 在数据存储到 HDFS 之前, 首先对整个数据文件进行加密, 然后再将加密后的文件写入 HDFS 中. 在这种方法中, 每个 DataNode 中的数据块不能被单独解密, 只有全部 DataNode 中全部的数据块被读取出来后, 才可以进行解密; 方案二: 在 HDFS 层面对每一个数据块进行加密, 这个操作对于文件写入方是无感知的, 是 HDFS 底层静默进行加密处理的.

Hadoop 组件对于数据加密的支持如下.

(1) HDFS: 支持各种通道的加密功能, 如 RPC, HTTP 和数据传输协议等, 可支持对运动的数据进行加密保护; Hadoop 也支持对于静止数据的加密保护, 可以通过 Hadoop 加密编解码器框架和加密编解码器实现.

(2) YARN: 不存储数据, 因此不涉及数据加密.

(3) HBase: 支持使用基于 SASL 框架的 RPC 操作提供对运动的数据进行加密; 目前暂不提供对静止数据加密的解决方案, 但可以通过定制加密技术或第三方工具来实现.

(4) Hive: 目前官方暂不提数据加密解决方案的数据, 但可以通过定制加密技术或第三方工具来实现.

(5) Pig: 支持使用 SASL 对运动的数据进行加密; 目前暂不提供对静止数据加密的解决方案, 但可以通

过定制加密技术或第三方工具来实现.

(6) Oozie: 支持使用 SSL/TLS 对运动的数据进行加密; 目前暂不提供对静止数据加密的解决方案, 但可以通过定制加密技术或第三方工具来实现.

(7) Zookeeper: 目前官方暂不提数据加密解决方案的数据, 但可以通过定制加密技术或第三方工具来实现.

(8) Hue: 支持使用 HTTPS 对运动的数据进行加密, 目前暂不提供对静止数据加密的解决方案, 但可以通过定制加密技术或第三方工具来实现.

2.4 操作审计

Hadoop 集群托管敏感信息, 此信息的安全对于企业具有成功的安全大数据使用至关重要[23]. 即便做了比较完善的安全管控, 但仍然存在未经授权的访问或特权用户的不适当访问而发生安全漏洞的可能性. 因此为了满足安全合规性要求, 我们需要定期审计整个 Hadoop 生态系统, 并部署或实施一个执行日志监视的系统[24], 详细如下.

(1) HDFS: 提供对用户访问 HDFS 执行操作行为的审计支持.

(2) YARN: 提供对用户任务提交、资源用量和资源队列操作等行为的审计支持.

(3) HBase: 提供对用户访问 HBase 执行操作行为的审计支持.

(4) Hive: 通过 Metastore 提供对用户访问 Hive 执行操作行为的审计支持.

(5) Pig: 目前官方暂不提审计的功能, 但可以通过定制加开发或第三方工具来实现.

(6) Oozie: 通过 Oozie 日志文件提供对用户执行的分布式任务调度信息的审计支持.

(7) Zookeeper: 目前官方暂不提审计的功能, 但可以通过定制开发或第三方工具来实现.

(8) Hue: 通过 Hue 日志文件提供对用户使用 Hue 执行操作行为的审计支持.

对于官方不提供内置审计日志记录的 Hadoop 组件, 行业内一般通过自定义开发日志记录并结合日志采集工具, 例如: Flume、Scribe 和 LogStash 等开源工具, 实现审计日志数据接入到大数据平台中, 然后依托于按需采集的日志, 搭建适合企业内部的日志管理系统, 用以支持集中式日志记录和审核[25].

综上所述, Hadoop 安全问题目前在身份验证、访问授权、数据加密和操作审计四个主要方向上均有可用解决方案或待实现的解决思路, 对于大数据平台用户应该合理分析自己的应用场景来明确安全保障等级, 对于平台使用到的组件不应该存在安全短板, 具体的: 在多租户场景下, 用户的身份验证和访问授权是至关重要的; 在数据敏感场景下, 数据传输中的动态加密和数据存储时的静态加密均需考虑; 在有问题追责体系或用量计量需求时, 操作审计是必需具备的安全管控能力, 但在实际生产环境中实践显示操作审计对于性能有一定的影响, 且审计日志体量较大, 需要做好评估和优化设计.

3 Hadoop 平台安全技术方案

大数据平台的开源社区在致力于开发更高性能、更稳定的大数据组件的同时, 也致力于解决平台安全这个重要问题, 随着发行版 Hadoop 的日趋成熟, 目前行业领先的 Cloudera 和 Hortonworks 等 Hadoop 发行厂商也支持开源社区并输出了一些比较成熟而先进的组件产品和技术方案.

这些 Hadoop 平台安全技术方案正致力于覆盖更全面的 Hadoop 平台组件, 均从大数据平台安全管控的身份验证、访问授权、数据加密和操作审计这四个方向对应设计出了安全管控产品, 具备安全能力保障和安全能力易用两大特性. 具体的, 这些技术方案可分如下几类.

(1) Hadoop 平台安全技术管控核心: 集中化的安全管控.

(2) Hadoop 平台安全技术对平台应用方更友好的封装: 集群边界安全管控.

(3) Hadoop 平台安全技术对平台运维方更友好的封装: 自动化安全管控.

3.1 集中化安全管控

早期没有集中化安全管控工具时, Hadoop 大数据平台的安全管理问题对于运维团队相当不友好.

(1) 管控入口零散: 不同的技术组件具备不同的管控指令和语法, 管控工作繁琐且效率低.

(2) 缺少可视化界面: 全部的技术组件仅支持命令行式的配置、查询操作方式, 管控工作复杂且出错概率高.

```
[hdfsOp@adminNode ~]$ hdfs dfs -setfacl /hdfs/path/to/file ... ...
[hbaseOp@adminNode ~]$ grant user <permissions> table ... ...
[hiveOp@adminNode ~]$ GRANT <priv_type> ON <table_name> TO USER <username>
```

图 3 传统大数据平台安全管控方式

通过集中化安全管控组件, 可以大幅度降低大数据平台安全管控的复杂度和工作量.

3.1.1 Apache Sentry

Apache Sentry 是 Cloudera 公司发布的一个 Hadoop 开源组件, 它提供了细粒度级、基于角色的授权以及多租户的管理模式. 该项目于 2016 年 3 月孵化成果, 目前属于 Apache 顶级项目之一.

Apache Sentry 目前是 Cloudera 发行版 Hadoop (CDH) 使用的集中化安全管控组件. 其定位为集中化提供 Hadoop 大数据平台的组件权限管控, 设计目标为:

(1) 为授权用户对于数据和元数据的访问需求提供细粒度的、基于角色的控制 (RBAC, role-based access control);

(2) 企业级别的大数据安全管控标准;

(3) 提供统一的权限策略管控方式;

(4) 插件化和高度模块化.

截止到版本 v.1.7.0 已经支持的组件包括: HDFS、Hive、其他 (Solr、Kafka、Impla).

Apache Sentry 架构设计上支持高可用, 单点故障不影响正常服务.

但是目前 Apache Sentry 支持的 Hadoop 相关组件数量仍然不多, 不支持基于属性标签的权限控制方案, 不支持 Hadoop 相关组件的操作行为审计.

3.1.2 Apache Ranger

Apache Ranger 是 Hortonworks 发布的一个 Hadoop 开源组件, 它解决了 Hadoop 平台各个服务安全管理各自为政的现状, 打造了一个集中统一的管理界面, 为所有服务提供权限管理、日志审计等.

Apache Ranger 目前是 Hortonworks 发行版 Hadoop (HDP) 使用的集中化安全管控组件. 其定位为集中化提供 Hadoop 大数据平台的组件权限管控并为相关组件提供审计能力, 设计目标为:

(1) 通过 Web UI 或 REST APIs 的方式提供集中化的安全管控能力;

(2) 集中式的管理工具提供细粒度的操作和使用行为管控;

(3) 对于 Hadoop 相关技术组件提供标准化的授权管理方案;

(4) 增强支持不同的权限管控方案, 如: 基于角色的管控和基于属性标签 (Tag) 的管控;

(5) 支持 Hadoop 相关技术组件的用户操作和维护行为的集中审计.

截止到版本 0.7.0 已经支持的组件包括: YARN、HDFS、Hive、HBase、其他 (Solr、Kafka、Knox、Storm、NiFi).

Apache Ranger 目前支持的组件较为丰富, 且提供了统一的审计能力.

但是目前 Apache Ranger 的高可用能力暂不完善, 单点故障时虽然不影响 Hadoop 相关组件的权限判断和用户使用, 但此时是无法提供访问权限变更的服务的.

3.2 集群边界安全管控

大数据平台的安全解决方案虽然可以显著提升集群的安全性, 但对于运维团队来说面向多租户场景的运维存在一定的复杂性和工作量, 对于开发团队来说, 基于 Kerberos 的身份验证也存在着一些编程开发的门槛. 因此集群边界安全管控方案被提出, 对于运维团队仅须关注集群内部, 无需将部署细节对外公布, 对于开发团队来说, 通过边界网管集中式访问各种 Hadoop 相关服务, 大幅度简化了开发的复杂性.

3.2.1 Apache Knox

Apache Knox 是一个开源的 Hadoop Gateway, 其目的是为了简化和标准化发布和实现安全的 Hadoop 集群, 对于 Kerberos 化的集群, 他可以对使用者屏蔽与复杂的 Kerberos 交互, 只需要专注于通过集中式的 REST APIs 访问 Hadoop 相关的服务.

具体的, Apache Knox 支持用户身份验证、单点登录、服务级别的授权控制和审计功能, 配合合理配置的网络安全策略和 Kerberos 化的 Hadoop 集群, Apache Knox 可以提供企业级别的 REST API Gateway 服务.

(1) 可与企业现有的用户身份管理方案快速集成;

(2) 保护集群的部署细节, 对终端用户无需保留集群的主机、端口号等信息, 减少安全隐患;

(3) 简化开发团队需要与交互的服务数量, 无需和众多 Hadoop 相关组件直接交互, 仅需要与 Apach Knox 交互即可.

截止到版本 0.12.0 已经支持的组件包括:

(1) 服务: Ambari、HDFS、HBase、HCatalog、Oozie、Hive、YARN、Storm;

(2) Web UI: NameNode UI、JobHistory UI、Oozie UI、HBase UI、YARN UI、Spark UI、Ambari UI、Ranger Admin Console.

Apache Knox 还处于快速的发展过程中, Hortonworks 发行版 Hadoop (HDP) 已经对其提供了较为完善的支持, 可以支持一键安装, 其余 Hadoop 发行版使用时仍需自行做相关适配工作.

3.3 自动化安全管控

3.3.1 Apache Ambari

Apache Ambari 是一个用于创建、管理、监视 Hadoop 集群的开源工具, 它是一个让 Hadoop 以及相关的大数据软件更容易使用的一个工具; Ambari 对于大数据平台的安全支持良好, 提供了一键式、可视化的 Kerberos 化 Hadoop 集群的功能.

截止到版本 2.5.0, 对于安全管控方面, Apache Ambari 提供了以下功能.

(1) 可视化、自动化的 Kerberos 化 Hadoop 集群操作;

(2) Apache Ranger 一键安装和配置;

(3) Apache Knox 一键安装和配置.

Apache Ambari 主要由 Hortonworks, IBM, Pivotal, Infosys 等公司的支持开发, 得益于开源社区的力量, 其发展速度相当之快, 目前是相当成熟的 Hadoop 集群管控工具.

目前主要存在的问题是界面友好性较弱, 在自动化部署配置时错误日志显示不精确 (不便于定位到问题根本原因), 出现问题后缺少自动回滚能力 (停留在配置中间状态需要人工修复).

3.3.2 Cloudera Manager

Cloudera Manager 是一个定位与 Apache Ambari 一致的产品, 是 Cloudera 公司开发的用于支持其自有发行版 Hadoop (CDH) 的管理工具, 其开发投产时间要早于 Apache Ambari 约 3 年, 因此在产品的完善程度、用户界面友好程度较为领先.

截止到版本 5.10.1, 对于安全管控方面, Cloudera Manager 提供了以下功能.

(1) 可视化、自动化的 Kerberos 化 Hadoop 集群操作;

(2) Apache Sentry 一键安装和配置.

Cloudera Manager 为 Cloudera 公司闭源开发的产品, 仅支持与其发行版 Hadoop 配套使用, 由于没有采用开源路线, 对于缺陷、新功能、修改意见等均无法像 Apache Ambari 那样得到快速响应, 使用时需要为 License 付费且不支持二次开发.

目前主要存在的问题是缺少集群边界安全管控的支持.

综上所述, 目前工业界和开源社区已经具备基本可用的 Hadoop 安全技术方案, 可以实现基本的安全管控能力. 在构建安全的大数据平台时, 建议选择集中化安全管控工具和自动化安全管控工具来实现安全管控, 对于希望降低大数据平台用户使用门槛和运维管理维护工作量的需求, 可以考虑引入集群边界安全管控工具. 但总体而言, 目前的安全技术方案在开箱即用能力、稳定性和易用性上并不完善, 一般需要投入一定的定制化开发、适配工作, 并在平台的运营管理流程需要针对性做好规范, 避免平台运维者和使用者之间因分工模糊、流程紊乱而产生冲突和问题.

4 结语

在大数据时代, 大数据平台需要处理海量的数据、承载多租户应用, 集群安全、数据安全成为需要重点关注的问题. 随着 Hadoop 在行业内越来越多被采纳、被广泛用于生产环境, 可用于实战环境中的安全解决方案是每一个企业、团队需要综合考虑和实践. 本文描述传统 Hadoop 大数据平台的安全隐患, 基本涵盖了解决这些隐患采用的技术方法, 以及目前可用的成熟技术方案. 我们认为之后的研究方向可侧重以下 4 个方面.

(1) Hadoop 平台安全问题: 持续跟进 Hadoop 生态圈各个技术组件, 关注生产实践中新发现的安全问题、隐患.

(2) Hadoop 平台安全问题解决方法: 持续跟进安全管控的四个主要方向和可能的新方向, 对于 Hadoop 生态圈各个技术组件的安全问题的解决方法补充和更新, 并关注新安全问题的解决方法.

(3) Hadoop 平台安全问题技术方案: 持续跟进工业界和开源社区, 关注对于 Hadoop 平台安全问题的技术方案能力更新和可能出现的新技术方案.

(4) Hadoop 平台安全管控最佳实践: 根据技术方案的成熟度和行业应用的实战经验, 待到技术方案足

够解决基本的安全问题时, 给出 Hadoop 平台安全管控最佳实践, 对于不同的安全管理等级需求, 给出针对性的落地方案指导和最佳实践建议.

参考文献

1 Laney D. 3D data management: Controlling data volume, velocity and variety. META Group Research Note, 2001, (6): 70.

2 Terzi DS, Terzi R, Sagiroglu S. A survey on security and privacy issues in big data. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). London, UK. 2015. 14–16.

3 Hashem IAT, Yaqoob I, Anuar NB, *et al*. The rise of "big data" on cloud computing: Review and open research issues. Information Systems, 2015, (47): 98 –115. [doi: 10.1016/j.is.2014.07.006]

4 Verma A, Pedrosa L, Korupolu M, *et al*. Large-scale cluster management at Google with Borg. Proceedings of the Tenth European Conference on Computer Systems. Bordeaux, France. 2015. 18.

5 Ghemawat S, Gobioff H, Leung ST. The Google file system. ACM SIGOPS Operating Systems Review, 2003, 37(5): 29–43. [doi: 10.1145/1165389]

6 Dean J, Ghemawat S. MapReduce: A flexible data processing tool. Communications of the ACM, 2010, 53(1): 72 –77. [doi: 10.1145/1629175]

7 Burrows M. The Chubby lock service for loosely-coupled distributed systems. Proceedings of the 7th Symposium on Operating Systems Design and Implementation. Berkeley, CA, USA. 2006. 335–350.

8 Chang F, Dean J, Ghemawat S, *et al*. Bigtable: A distributed storage system for structured data. ACM Transactions on Computer Systems (TOCS), 2008, 26(2): 4.

9 Vavilapalli VK, Murthy AC, Douglas C, *et al*. Apache Hadoop YARN: Yet another resource negotiator. Proceedings of the 4th Annual Symposium on Cloud Computing. New York, NY, USA. 2013. 5.

10 Big Data Working Group. Expanded top ten big data security and privacy challenges. 2013.

11 Adluru P, Datla SS, Zhang XW. Hadoop eco system for big data security and privacy. 2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY, USA. 2015. 1–6.

12 Somu N, Gangaa A, Sriram VSS. Authentication service in Hadoop using one time pad. Indian Journal of Science & Technology, 2014, 7(S4): 56–62.

13 Bardi M, Zhou XW, Li S, *et al*. Big Data security and privacy: A review. China Communications, 2014, 11(14): 135–145. [doi: 10.1109/CC.2014.7085614]

14 Fernandez EB. Security in data intensive computing systems. Furht B, Escalante A. Handbook of Data Intensive Computing. New York: Springer, 2011: 447–466.

15 O 'Malley O, Zhang K, Radia S, *et al*. Hadoop security design. Sunnyvale, CA, USA: Yahoo Inc., 2009.

16 Hortonworks. Securing your hadoop infrasturcture with apach knox. http://hortonworks.com/hadoop-tutorial/securing-hadoop-infrastructure-apache-knox, 2014.

17 Shukla V. Hadoop security: Today and tomorrow. https://hortonworks.com/blog/hadoop-security-today-and-tomorrow/. [2013-12-09].

18 Zhang XF. Secure your Hadoop cluster with apache sentry. Cloudera. [2014-04-07].

19 Saraladevi B, Pazhaniraja N, Paul P V, *et al*. Big Data and Hadoop-a study in security perspective. Procedia Computer Science, 2015, (50): 596 –601. [doi: 10.1016/j.procs.2015.04.091]

20 Hortonworks. Comprehensive and coordinated security for enterprise hadoop. http://hortonworks.com/labs/security. [2014-05-15].

21 Tene O, Polonetsky J. Big Data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property Volume, 2013, 11(5): 240–273.

22 Cheng HB, Rong CM, Hwang K, *et al*. Secure Big Data storage and sharing scheme for cloud tenants. China Communications, 2015, 12(6): 106–115. [doi: 10.1109/CC.2015.7122469]

23 Marchal S, Jiang XY, State R, *et al*. A Big Data architecture for large scale security monitoring. 2014 IEEE International Congress on Big Data (BigData Congress). Anchorage, AK, USA. 2014. 56–63.

24 Lan L, Jun L. Some special issues of network security monitoring on Big Data environments. Proceedings of the 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing (DASC). Washington, DC, USA. 2013. 10–15.

25 Gupta A, Verma A, Kalra P, *et al*. Big Data: A security compliance model. Proceedings of the 2014 Conference on IT in Business, Industry and Government (CSIBIG). Indore, India. 2014. 1–5.