# 第九章 构建hadoop集群

**内存**

与早期的MapReduce基于槽的模型相比，YARN以更加精细化的方式管理内存。YARN不会为可同时在tasktracker 上执行map和reduce槽的最大数量设置一个最大值。他允许应用程序为任务请求任何规模的内存量（内存量需要在一个预定范围之内）。在YARN模型中，节点管理器从一个内存池中分配内存，这意味着可同时运行任务的数量依赖于内存需求总量，而非槽数量。

基于槽的模型可能导致集群未被充分利用，原因是map槽和reduce槽之间的比率在整个集群内是固定的，然而在不同的时段，作业对map和reduce槽的需求也会变化。

一个YARN守护进程运行一个或者多个RPC和HTTP服务。

## 9.6 安全性

从安全角度分析，Hadoop缺乏一个安全的认证机制，以确保正在操作集群的用户是所声称的安全用户。

雅虎公司在2009年遇到这个难题，组织解决这个问题，他们提出了kerberos（一个成熟的开源网络认证协议）实现用户认证。Kerberos的职责在于鉴定登录账号是不是他所声称的用户。

自从0.20.20x版本之后，hadoop就支持Kerberos认证。

### 9.6.1 Kerberos和hadoop

使用kerberos时，一个客户端要经过三个步骤才可以获得服务：

1. 认证 客户端向认证服务发送一个报文，并获得一个含时间戳的票据授予票据（TGT）
2. 授权 客户端使用TGT向票据授予服务器（TGS）请求一个服务票据
3. 服务请求 客户端向服务器出示服务票据，以证明自己的合法性。

在hadoop应用中，服务器可以是namenode或jobtracker。

授权和服务请求都是非用户级别的，客户端会代替用户来执行这些步骤，但是 认证步骤是用户调用 kinit 命令来执行的。该过程会提示用户输入密码。

这并不意味着每次运行一个作业都要输入密码，TGT是具有一定的有效期的，更通用的方法是采用自动认证。

为了在hadoop中使用Kreberos，用户需要安装一个KDC（hadoop并不自带一个KDC）

将core-site.xml中的 hadoop.security.authentication 属性项设置为kerberos ，启动kerberos认证。该属性的默认值是simple，表示采用传统的向后兼容的方式。

还需要将同一文件中 hadoop.security.authorization 属性项设置为 true，以启动服务级别的授权。Hadoop-policy.xml文件中的访问控制列表（ACL）决定哪些用户和组能够访问哪些hadoop服务。在默认情况下，各个服务的ACL都被设置为\* ,表示所有用户都能够访问这个服务。

$ kinit #KDC认证

$ klist #查看票据的过期时间

$ kdestory #销毁票据

### 9.6.2 委托令牌

在分布式系统中，客户端和服务器之间频繁交互，且每次交互都需认证。如果在一个高负载集群上采用三步骤Kerberos 票据交换协议来认证每次交互，则对KDC造成很大的压力。因此hadoop使用委托令牌来支持后续的认证。

委托令牌由服务器创建（namenode），可以视为客户端和服务器之间一个共享的一个密文。

当客户端通过RPC访问namenode时，客户端并没有委托令牌，因此使用Kerberos进行认证，之后namenode取得一个委托令牌，在后续的RPC调用下，客户端出示委托令牌就行，namnode能识别真伪。

客户端需要使用一种特殊的委托令牌来执行HDFS块操作，称为“块访问令牌

当客户端向namenode发出元数据请求时，namenode创建相应的块访问令牌并发送到客户端。客户端使用块访问令牌向datanode认证自己的访问权限。由于namenode和datanode分享创建块访问令牌时的密钥（通过心跳信息传送）。

可以通过将 dfs.block.access.token.enable 的值设置为true来启动块访问令牌特性。

默认hdfs会自动获取委任令牌。

### 9.6.3 其他安全性改进

这本书讲的版本有点老，书上写的安全性改进可能又被改进了

## 9.7 利用基准评测程序测试Hadoop集群

为了获得最佳的评测结果，在集群入役之前进行评测是最合适的。

实践表明，硬盘驱动器故障时新系统最常见的硬件故障，通过运行含有高强度IO操作的基准评测程序，就能在上线前对集群做“烤机”测试。

### 9.7.1 Hadoop基准评测程序

Hadoop自带若干基准评测程序，安装开销小，运行方便。