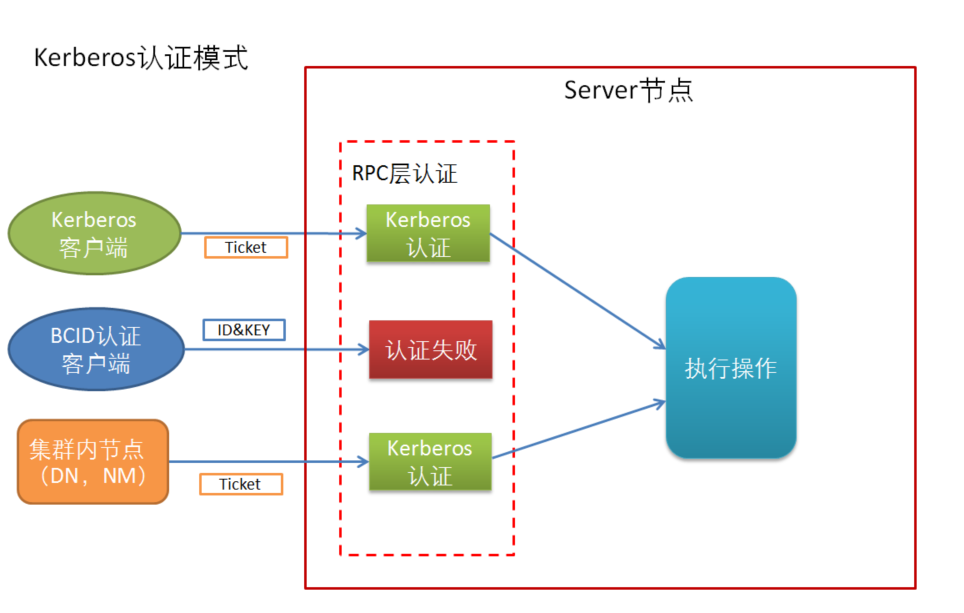
# BCID兼容Kerberos认证

## 背景

目前关于Hadoop的安全认证方案，社区以及基于社区版本的大数据产品主流使用kerberos进行认证。在我们苏研发布的BC-Hadoop版本中，安全认证使用的是苏研自主研发的BCID认证方案。BCID认证方案相比于Kerberos认证方案，具有部署运维使用更便利，性能影响更小的优势。但是当已有集群需要升级到BC-Hadoop版本，认证方式迁移到BCID认证时，需要考虑到已有应用基于Kerberos方式认证。因此BCID认证机制能够兼容Kerberos认证就非常有意义。

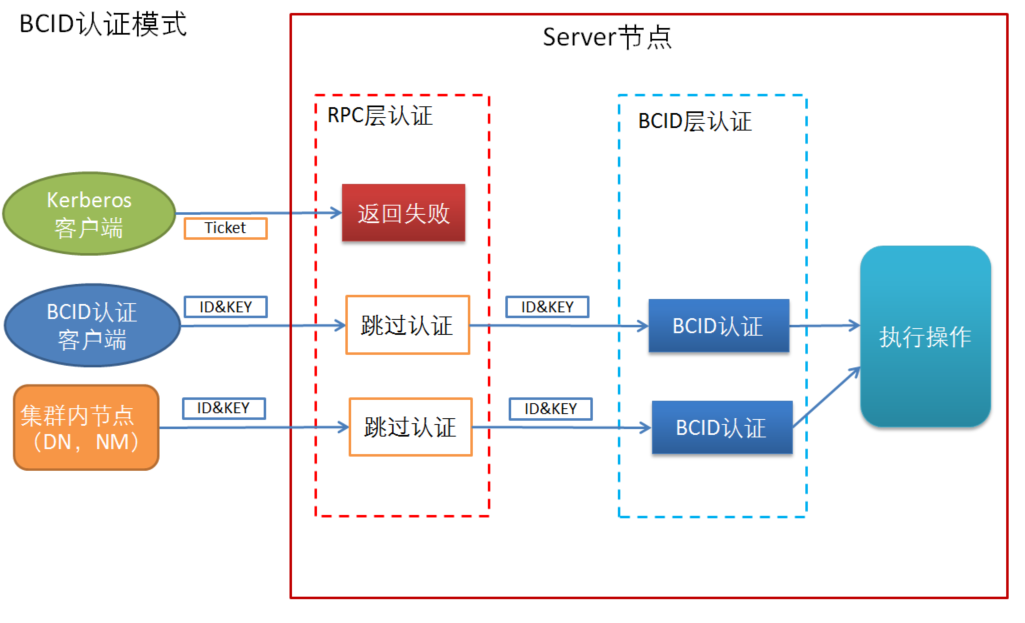
## Compatible模式认证原理

先BCID认证机制和Kerberos认证机制，如下图所示



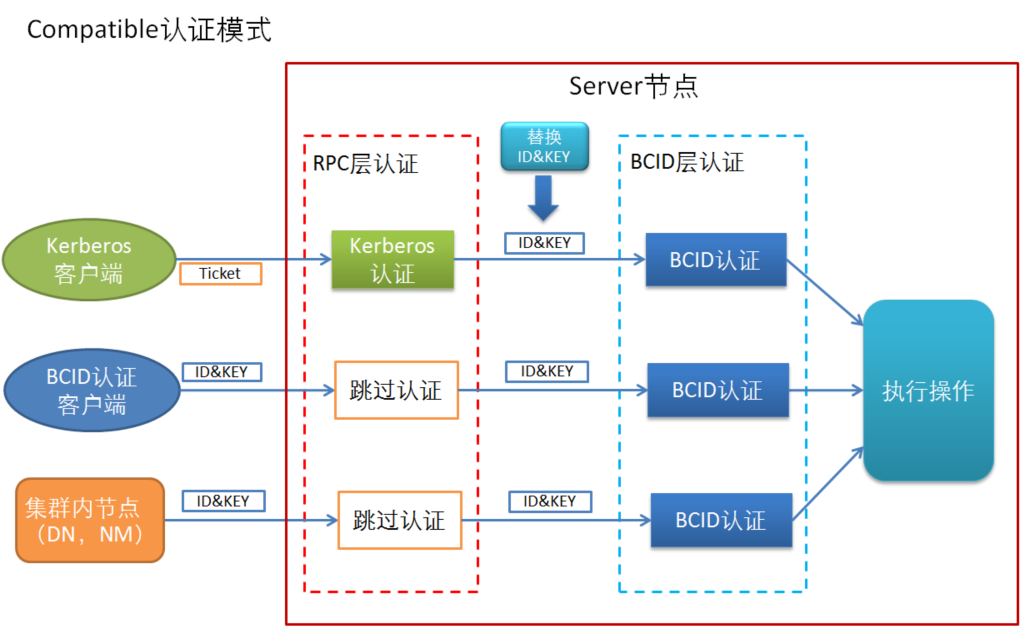
Kerberos认证模式中，认证逻辑实际在请求的RPC层进行的。kerberos客户端向服务端发起请求时会在请求中带上ticket（或者token）信息，Server端会对ticket进行认证。当非kerberos客户端或者kerberos客户端请求中ticket信息不合法时，RPC层认证就会失败从而拒绝访问。

对于集群内节点（Datanode、NodeManager），节点自身也需要部署kerberos客户端。集群内节点于Master发生通信时，同样走kerberos认证逻辑。



在BCID认证模式中，服务端认证实际上是在RPC层认证之后，再增加了一层BCID认证。但是在RPC层会对客户端请求的认证模式进行校验，只接受认证方式为SIMPLE的客户端请求。因此配置为Kerberos的客户端请求，会在RPC层校验中就返回失败。使用BCID认证的客户端，会在请求中带上accessId和securityKey，请求会直接跳过RPC层的认证，然后在BCID层认证中对ID/Key进行校验，通过认证后才能继续访问，否则返回失败。

集群内的节点（Datanode、NodeManager），本身也需要进行BCID的认证。和普通BCID客户端的区别是，集群内节点统一配置一组admin的ID/KEY，以表示集群内用户。



Compatible模式中服务端可以同时支持kerberos认证客户端的请求与BCID认证客户端的请求：

1. Server节点在RPC层认证同时支持KERBEROS方式和SIMPLE方式（BCID认证使用）两种方式。
2. Server节点自身采用Kerberos认证，从而kerberos客户端在与Server通信时可以拿到Server的kerberos用户信息。
3. Kerberos客户端传入ticket后，在RPC层进行认证，通过认证之后，会将其UGI对象中认证方式改成Compatible模式，然后使用Server节点上的系统AccessId和SecurityKey填充到UGI对象中，随后再该对象进行BCID层验证。由于此时UGI对象中的id&key是系统id&key，所以BCID认证结果会返回原先kerberos的用户名。最终使用kerberos中的用户进行访问。
4. 对于BCID认证客户端，请求传入id&key信息，在RPC层认证直接通过，随后进行BCID认证，逻辑与BCID认证模式相同。
5. 对于集群内节点，需要配置系统id&key，在请求时传入。RPC层认证也是直接通过，随后BCID层在进行认证。

## Compatible模式部署

部署Compatible模式集群，大体上就是需要同时部署kerberos认证和BCID认证。具体步骤如下：

1. 部署kerberos认证环境，包括：
   1. 安装并配置KDC
   2. 在Master（NN、RM）节点安装kerberos客户端
   3. 为Master节点的每个角色创建Principal**和**keytab
   4. Master节点上配置kerberos认证相关参数

具体步骤参考：<http://223.105.0.132:8090/pages/viewpage.action?pageId=24254317>

需要注意的是，Compatible模式中只需要对Master配置kerberos，而不用配置每个slave节点，同样无需通过jsvc特权模式启动datanode。Kerberos相关参数中需要剔除datanode和nodemanager相关参数包括：

|  |
| --- |
| dfs.datanode.kerberos.principal |
| dfs.datanode.keytab.file |
| yarn.nodemanager.principal |
| yarn.nodemanager.keytab |

1. 部署BCID认证：

具体参考：<http://223.105.0.132:8090/pages/viewpage.action?pageId=21262989>

1. 集群中所有节点配置认证模式参数为compatible：

在core-site.xml中设置参数**hadoop.security.authentication=compatible**。（该参数在kerberos认证模式中配置值为kerberos，在BCID认证模式下，配置值为simple）