Slider文档

# 1、Slider Client

slider.yarn.queue参数用于指定服务启动的队列，也可定定义优先级、资源限制和应用的其他值。默认是default

slider.yarn.queue.priority，配置队列的优先级，数字越小，优先级越高。

slider.cluster.directory.permissions，定义集群描述的目录文件的权限（类似于Linux目录）

slider.data.directory.permissions，slider 应用数据目录的权限

# 2、High Availabity

# 3、Security

Slider在Secure Clusters中运行，仍然有以下限制：

1. AM和components与Master认证使用的KeyTabs，提前分发到节点或者由Slider分发
2. Slider Node实例被限定在固定节点（a future Yarn feature）之前，对于集群中的所有节点都需要Keytabs，对于用户创建集群同样需要keytabs
3. 由于HBase及Accumula中的worker节点需要认证到masters。在同一服务器上的所有HBase node需要使用相同的principal，对于HBase Cluster具有相同的访问权限。
4. 每个用户目录在中都有一个Slider Cluster数据目录，集群中代表role实例的principals需要具有这些目录的读写权限。可以通过用户短名匹配，或者Slider创建目录，该目录具有组写权限，使用LDAP来标识user（app principals）为同一用户组的成员

## 3.1 安全需求：

### 3.1.1 前提

1. Slider部署应用时，HDFS不能启用Secure模式
2. Slider可以与Yarn secure模式共存
3. Slider启动Secure Applications
4. 使用Kerberos和ActiveDirectory来执行认证
5. Slider只允许用于通过用户命令行或者direct RPC来执行认证
6. 只有认证的用户才能访问Slider Web UI及Ambari REST API
7. 在~/.slider/clusters/$name/data下的Slider Database可以通过HBase写入

### 3.1.2 Short-lived Clusters

集群在Kerberos tokens规定的时间内保持secure

### 3.1.3 Long-lived clusters

Slider Application 实例和HBase实例一直保证功能及安全

### 3.1.4 Initial Non-requirements

集群操作的Secure audit trail

多认证用户可以访问Slider Cluster（Yarn admins可以停掉Slider app 实例）

Any way to revoke certificates/rights of running containers.

### 3.1.5 假设

Kerberos运行，HDFS和Yarn 运行在Kerberized

不一定安装LDAP

证书可以被pushed到worker 节点的本地系统（例如通过scp），访问证书要通过本地文件系统的访问权限

证书的存在时间和app instance不是相同的

应用和运行应用的用户具有相同的标识

同一用户的所有应用可以共享machine-specific kerberos标识

# 4、Design

用户有自己的Kerberos princial，使用kinit或者Kerberor，获取TGT

组件认证需要用户有集群中每个主机的principal（格式为username/hostname@REAL

M）。AM认证需要满足non-host based principal（username@REALM）。

AM需要不同的keytabs，包括AM login principal及service components（包括所有的service principal）。Keytabs需要手动的分布到所有节点（需要访问用户的读访问权限），用户可能会评估Slider keytab分发机制

当用户创建一个secure cluster，需要提供一个标准的HBase kerberos选项来标识使用的principal和keytab location。Slider Client和HDFS及Yarn通讯通过TGT来完成。通过client命令参数来指定，命令如下：

-D yarn.resourcemanager.principal=yarn/master@LOCAL

-D dfs.namenode.kerberos.principal=hdfs/master@LOCAL

Slient创建的HDFS集群数据目录，权限分别为rwx,r-x,---，这个可以作为集群选项配置。

### 4.1 Keytab distributed/access Options

为了保证安全性，Slider不采用认证机制中的delegation token，AM从KDC cluster中获取Keytab files。为了执行访问AM需要访问标识用户（发布application）的keytab file（例如HBase的安装获取HBase principal）。有两种方式来支持keytab访问and /or distribution。

1）Local Keytab file access:

App deployer可能选择pre-distribute的keytab files（在Yarn Cluster中NM需求）。在实例中，appConfig.json需要以下性质：

"components": {

"slider-appmaster": {

"jvm.heapsize": "256M",

"slider.am.keytab.local.path": "/etc/security/keytabs/hbase.headless.keytab",

“slider.keytab.principal.name” : “hbase" }}

slider.am.keytab.local.path提供keytab file的全路径，然后强制使用local lookup机制。文件中principal用slider.keytab.principal.name性质来指定。这种场景下，App deployer需要对集群有一个整体的把握。例如对于HBase的部署，HBase 的keytab已经被分布，而且hbase-site中进行指定。

2）Slider keytab distribution

部署者也可以选择为AM及应用的HDFS目录上传keytab文件或者用Slider client install-keytab。Slider为AM及application containers下载keytab到本地目录。

"components": {

"slider-appmaster": {

"jvm.heapsize": "256M",

"slider.hdfs.keytab.dir": ".slider/keytabs/hbase",

"slider.am.login.keytab.name": "hbase.headless.keytab",

“slider.keytab.principal.name” : “hbase"}}

slider.hdfs.keytab.dir指向HDFS的目录（相对于用户的主目录），在该目录中Slider可以找到AM login需要的所有keytab文件及App service（例如hbase的headless keytab及hbase app components的service keytab）。如果没指定目录则默认使用.slider/keytab。slider.am.logion.keytab.name是keytab file的名字，在指定目录中可以获取，AM在该目录中查找login principal和认证。

如果采用slider-based distributed 机制，components的keytab files可以从container work目录的Keytabs子目录获取，子目录可以指定了$AGENT\_WORK\_ROOT/keytabs目录，例如：

"site.hbase-site.hbase.master.kerberos.principal": "hbase/\_HOST@EXAMPLE.COM",

"site.hbase-site.hbase.master.keytab.file": "${AGENT\_WORK\_ROOT}/keytabs/hbase.service.keytab",

上述两种方案，principal名字以下两种：

1）通过Slider CLI（kinit使用）来建立

2）slider.keytab.principal.name来指定

### 4.2 Slider Client Keytab的安装

使用Slider client来安装keytab files，命令格式如下：

slider install-keytab —keytab <path to keytab on local file system> —folder <name of HDFS folder to store keytab> [—overwrite]

该命令通过-keytab选项指定Keytab file存放的本地目录，-folder指定存放的HDFS目录，可以在/user/username/.slider/keytabs（如果指定文件夹名称，如HBASE，则存储在/user/username/.slider/keytabs）。这个命令用于将keytab files上次至HDFS，如果将AM和HBase服务上次值HBASE目录，则执行下面的命令两次：

slider install-keytab —keytab /my/local/keytabs/folder/hbase.headless.keytab —folder HBASE

slider install-keytab —keytab /my/local/keytabs/folder/hbase.service.keytab —folder HBASE

随后，hbase-site的配置性质如下：

"global": {

. . .

"site.hbase-site.hbase.master.kerberos.principal": "hbase/\_HOST@EXAMPLE.COM",

"site.hbase-site.hbase.master.keytab.file": "${AGENT\_WORK\_ROOT}/keytabs/hbase.service.keytab",

. . .

}

"components": {

"slider-appmaster": {

"jvm.heapsize": "256M",

"slider.hdfs.keytab.dir": ".slider/keytabs/HBASE",

"slider.am.login.keytab.name": "hbase.headless.keytab"

“slider.keytab.principal.name” : “hbase"

}

}

# 5. Slider Client和AM之间的通信

当AM部署在secure cluster中，自动会使用Kerberos-authorized RPC通道。Client访问AM必须获取token。运行过程中，Client可以通过--force选项强制停止Slider application实例。

### 5.1 启用Slider Client安全模式

通过设置Hadoop securty options，Slider采用Secure模式，slider-client.xml配置如下：

<property>

<name>hadoop.security.authorization</name>

<value>true</value>

</property>

<property>

<name>hadoop.security.authentication</name>

<value>kerberos</value>

</property>

或者通过下面的命令行进行配置：

-D hadoop.security.authorization=true -D hadoop.security.authentication=kerberos

### 5.2 为Slider Client JVM添加Kerberos binding properties

Java Kerberos library需要知道Kerberos controller和使用的Realm。如果在/etc/krb5.conf中配置后，自动启用。没有配置，则会提示java.lang.IllegalArgumentException

Can't get Kerberos real，Client失败。

realm和controller在java system properties中的java.security.krb5.realm和java.security.krb5.kdc来定义。也可以在Client configrution中进行定义JVM options。使用命令的格式如下：

-S java.security.krb5.realm=MINICLUSTER -S java.security.krb5.kdc=hadoop-kdc

### 5.3 Java Cryptography Package

访问secure cluster，可能看到以下信息：

No valid credentials provided (Mechanism level: Illegal key size)]

表示JRE没有扩展的Cryptography package