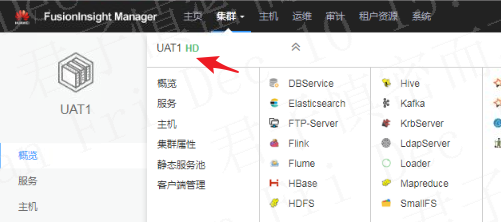
FI客户端安装

具体操作请参考华为官方文档：“软件安装” -> “初始配置” -> “配置客户端” -> “安装客户端” 具体说明进行操作。

1. 下载客户端







下载完成会自动保存在主管理节点“/tmp/FusionInsight-Client”，主节点在主机中查看如下：



1. 创建用户<root权限>（用户已存在无需执行此步骤）
2. 添加用户

useradd bdap

1. 增加密码

passwd bdap

1. 查看用户是否正常

id bdap

1. 新建目录修改权限

mkdir /home/app/bdap/ficlient

mkdir /home/app/bdap/clientsoft

chown bdap:bdap app

chmod -R 777 app

1. 拷贝客户端软件<root权限>

|  |
| --- |
| scp -r [root@10.6.92.50:/tmp/FusionInsight-Client/FusionInsight\_Cluster\_1\_Services\_Client.tar /home/app/bdap/](mailto:root@10.6.92.50:/tmp/FusionInsight-Client/FusionInsight_Cluster_1_Services_Client.tar%20/home/app/bdap/)  chown bdap:bdap FusionInsight\_Cluster\_1\_Services\_Client.tar |

1. 解压缩文件<bdap用户,所有解压后文件赋予755权限>,校验、解压文件

|  |
| --- |
| cd /home/app/bdap/  tar -xvf FusionInsight\_Cluster\_1\_Services\_Client.tar -C /home/app/bdap/clientsoft  解压后文件如下：    执行**sha256sum**命令校验解压得到的文件，检查回显信息与sha256文件里面的内容是否一致，例如：  **sha256sum -c FusionInsight\_Cluster\_1\_Services\_ClientConfig.tar.sha256**  FusionInsight\_Cluster\_1\_Services\_Client.tar: OK  --解压上述文件  tar -xvf FusionInsight\_Cluster\_1\_Services\_ClientConfig.tar  内容如下： |

1. 配置客户端网络：客户端是集群节点<如果客户端安装主机不是集群节点，请参考华为官方说明>

查看hosts文件



测试连通性，ping ip完成。

1. 安装客户端

|  |
| --- |
| cd /home/app/bdap/clientsoft/FusionInsight\_Cluster\_1\_Services\_ClientConfig/  --安装  ./install.sh /opt/ficlient<该目录必须为空>  结果：Components client installation is complete.  卸载，更新或者单独安装某个组件，需要单独安装，使用单独的目录，具体请看华为官方说明。 |

1. 检查客户端是否安装成功

|  |
| --- |
| 1. 执行 cd /home/app/bdap/ficlient 2. 执行 source bigdata\_env命令配置客户端环境变量 3. 执行以下命令，设置 kinit 认证，输入客户端用户登录密码；   kinit rcp  Password for admin@HADOOP.COM: #输入rcp用户登录密码（与登录集群的用户密码一致）这里使用flink权限的人机用户rcp.   1. Klist命令查询并确认权限内容。 |

1. 在~/.bash\_profile中添加

|  |
| --- |
| PATH=$PATH:$HOME/bin  source /home/app/bdap/hadoopclient/bigdata\_env  kinit kt /home/app/bdap/user.keytab hds  注意此目录:/home/app/bdap/user.keytab放置的为hds的认证文件 |

加载环境变量

source ~/.bash\_profile

1. 修改客户端的flink-conf.yml文件

|  |
| --- |
| security.kerberos.login.principal: rcp  security.kerberos.login.keytab: config/rcp.keytab |

1. 生成token

|  |
| --- |
| 1.用户调用FusionInsight提供的“generate\_keystore.sh”脚本工具生成“Security Cookie”、“flink.keystore”和“flink.truststore”。  说明：  generate\_keystore.sh脚本在Flink客户端的bin目录下，执行命令“sh generate\_keystore.sh <password>”即可，<password>由用户自定义输入。  •若<password>中包含特殊字符"$"，应使用如下方式，以防止被转义，“sh generate\_keystore.sh ‘Huawei$123’”  •密码不允许包含“#”。  执行脚本后，在Flink客户端的conf目录下生成flink.keystore、flink.truststore文件，并且在客户端配置文件“flink-conf.yaml”中将以下配置项进行了默认赋值。  •将配置项“security.ssl.key-password”、“security.ssl.keystore-password”和“security.ssl.truststore-password”设置为<password>  •将配置项“security.ssl.keystore”设置为“flink.keystore”文件所在绝对路径。(目前：为工作目录下的config/ flink.keystore)  •将配置项“security.ssl.truststore”设置为“flink.truststore”文件所在的绝对路径。  •将配置项“security.cookie”设置为一串密码，该密码是“generate\_keystore.sh”脚本自动生成的一串随机规则密码。  2.打开“Security Cookie”开关，配置“security.enable: true”，查看“security cookie”是否已配置成功，例如：security.cookie: ae70acc9-9795-4c48-ad35-8b5adc8071744f605d1d-2726-432e-88ae-dd39bfec40a9 |

1. 下载rcp的认证文件并解压的配置目录config/
2. 使用flink run 及启动某个应用测试环境