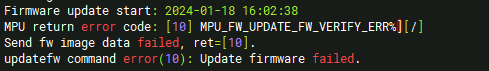
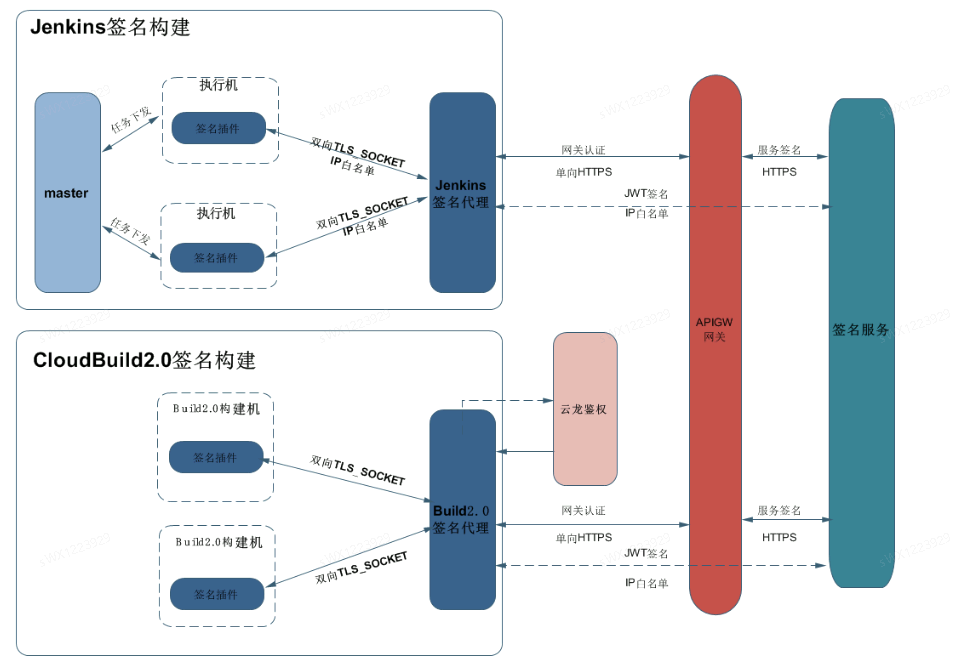
# 问题阐述

新的DPU卡会对固件进行一个签名验证，重新编译的固件不具备签名会被拒绝更新：



流水线方式需要在黄区进行，因此需要手动签名

# 签名构建结构



关键部件：

* 签名服务：执行签名
* **签名代理**：接收签名请求并转发给签名服务
* **签名插件**：触发签名任务的工具

环境要求：

1. 构建环境
   1. **jenkins**，推荐2.222.4以上版本；（暂时尝试这种构建方式，可能需要web接入访问，需要安装web和jenkins环境）
   2. *cloudbuild2.0，可能是创建虚拟环境专用于构建，不确定是否拥有权限*
2. 签名插件：Linux机器、JDK1.8 （选择41的服务器，需要安装JDK）

签名插件、签名代理V5.1.X以上版本

# 签名客户端搭建步骤

## 步骤总结

根据聊天记录判断签名客户端指的是签名代理**10.243.226.158**可能已经配置完成

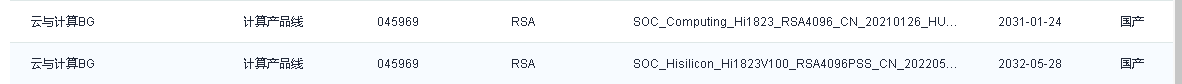
因此1-4可以跳过（是吗？）

在本地（41服务器）执行5-6：

1. 安装JDK1.8和Jenkins
2. 获取并安装Jenkins的Master插件（[5.1.1 Master插件安装](#_cetefkxnd3it)）
3. 配置自动安装脚本，获取Jenkins的slave插件并安装，（[5.1.2 脚本安装slave插件](#_wa28z6zg6r42)）
   1. 对应的签名代理**10.243.226.158**的ssl通信根无法获得
      1. 根据[5.1.2 脚本安装slave插件](#_wa28z6zg6r42)，需要签名代理安装脚本的**目录**或者执行脚本之后生成的ssl通信根文件：**root.jks、root.crt、root.properties**
4. 在Jenkins中创建workspace，在workspace中添加signconf\_jenkins.xml文件，根据xml的配置将要签名的文件放在执行的相对路径中，构建Jenkins项目（[6.2 Jenkins构建，签名任务配置](#_mpnuq45fuf3a)）

不确定之处：

* 签名代理是否已经配置好？
  + 推测：使用给的ip 10.243.226.158可以在签名平台（https.//signcenter.clouddragon.huawei.com/Signcenter/）搜索到已经开通的签名权限，并且能够查询到对应需要在jenkin.xml中需要的alias和productlineid值，这两个值和已有的“signconf\_jenkins.xml”中的值对应，因此判断签名代理是现成的，根据聊天记录推测当时他们在已有的签名代理客户端中加入了我们需要的签名证书



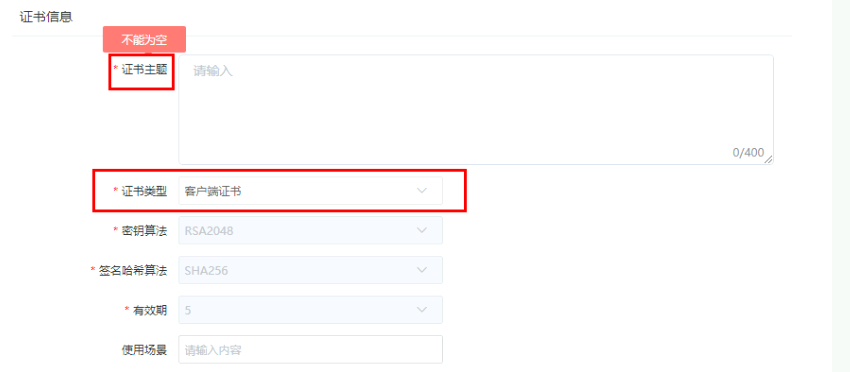
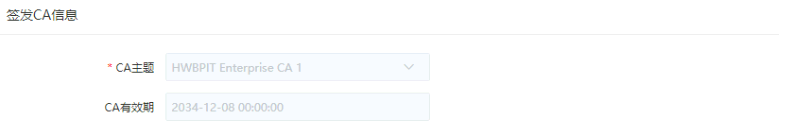
* Jenkins和Hi1823项目的关系？
  + 推测：Jenkins安装插件之后需要创建一个项目并生成一个workspace（[6.2 Jenkins构建，签名任务配置](#_mpnuq45fuf3a)），将Jenkins.xml放置在workspace中，而Jenkins.xml中签名文件的path字段说明是相对于workspace的相对路径，并且包含后缀为“desc”的文件。推测这两个workspace是同一个workspace，创建一个Jenkins项目其workspace就是Hi1823项目的根目录，执行Jenkins Signature plugin时候根据xml找到需要签名的文件。
* Master插件和slave的关系？
  + 推测：Jenkins理论上Master和slave应该可以部署在同一台机器上，Master负责与用户交互，slave负责执行实际的任务。因此可以把获取的Master 插件和slave插件都安装在41上安装Jenkins环境中
* Jenkins插件如何获得签名代理的ssl通信根？（[5.1.2 脚本安装slave插件](#_wa28z6zg6r42)）
  + 推测：xml中配置了代理服务的ip，Jenkins slave安装脚本使用自动方式获取通信根需要配置签名代理中脚本的安装绝对路径，推测在执行时将ip和路径结合获得ssl通信根
  + 问题：如何确定签名代理中脚本安装的绝对路径？

## 1 申请客户端权限认证证书

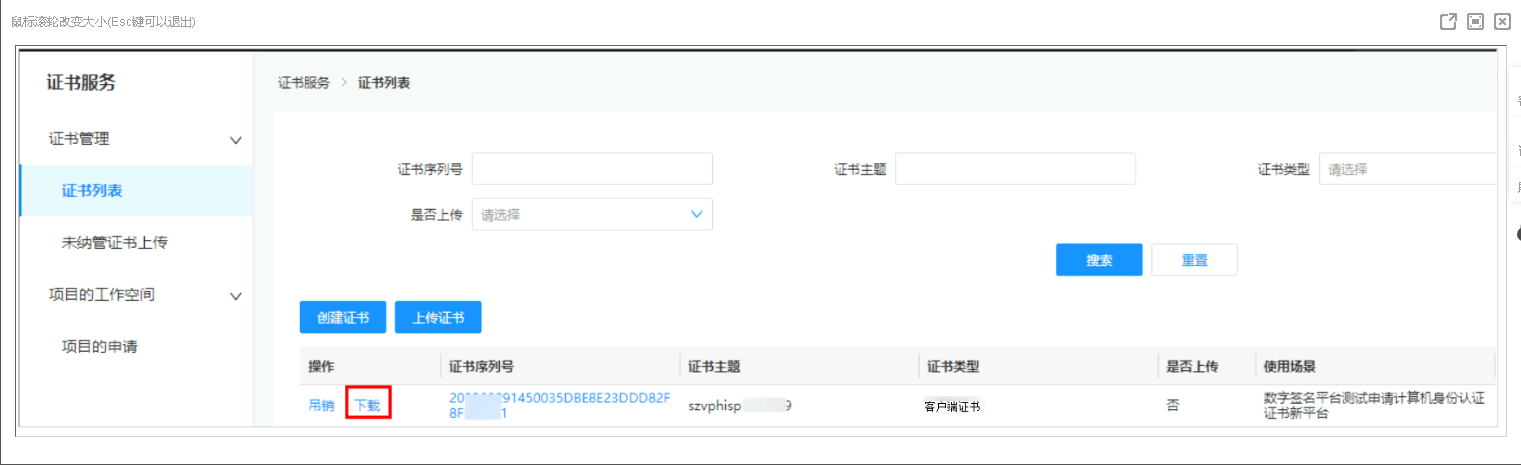
签名代理需要申请IT客户端证书、签名平台权限才能接入签名平台（1、2）

（判断这里的客户端应该是签名代理）

1. 访问申请页面：https//his.huawei.com/cmsAui/
2. 创建证书
3. 提供包括应用信息、证书主题、证书类型等后提交申请，等待审批



1. WeLink应用号接收审批信息



## 2 申请客户端签名权限

### 2.1 申请开通数字签名平台访问权限

访问数字签名服务平台：https.//signcenter.clouddragon.huawei.com/Signcenter/

点击客户端用户注册

填写注册信息、相关项目信息

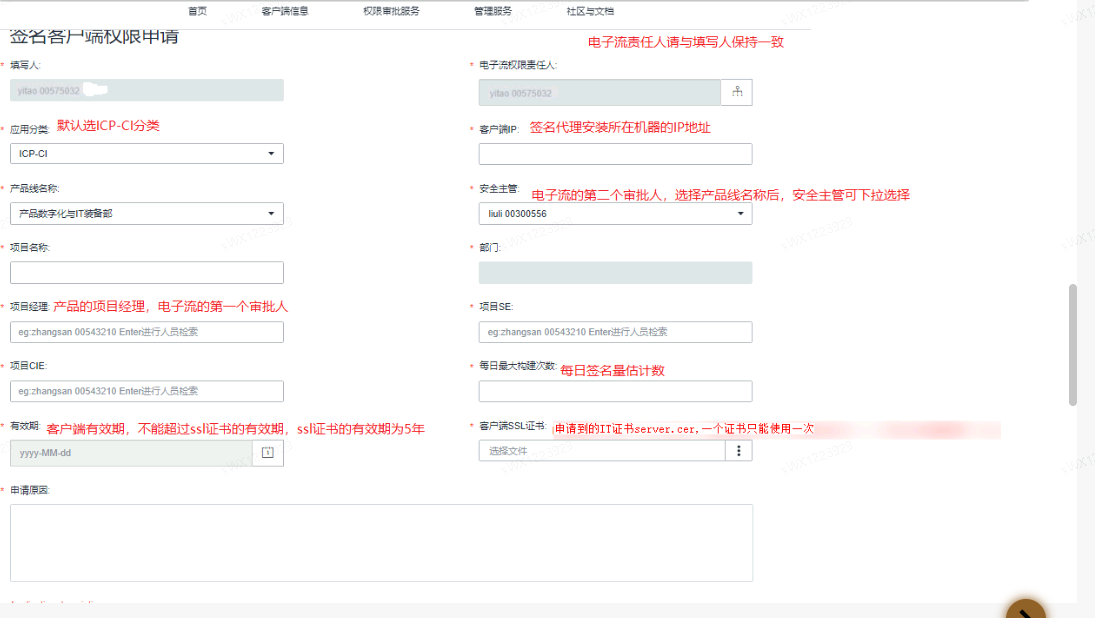


等待审批

### 2.2 申请签名客户端权限

1.访问环境: https://signcenter.clouddragon.huawei.com/SignCenterl

2.选择菜单:权限审批服务--》权限申请--》权限申请服务,填写申请并提交





申请关键信息包括：

* 客户端IP（代理服务的IP地址）
* 申请获得的客户端权限认证证书（只能用一次，签名代理与签名服务之间认证）
* 产品线名称，签名标准等

## 3 订阅签名中心API接口

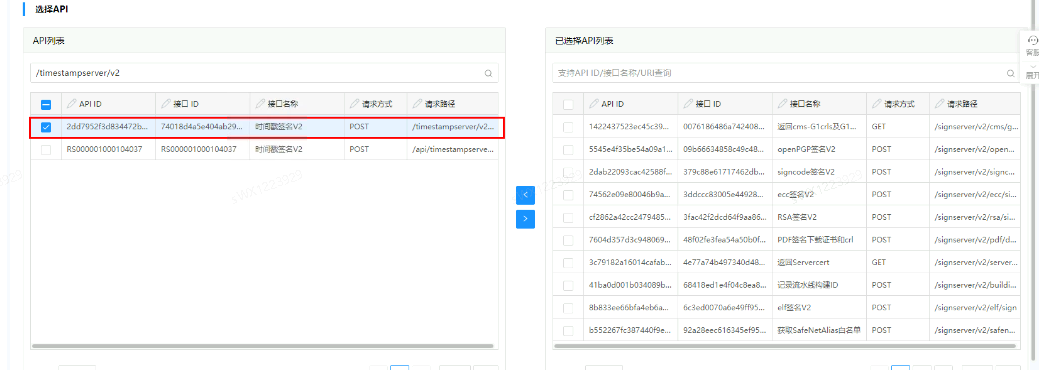
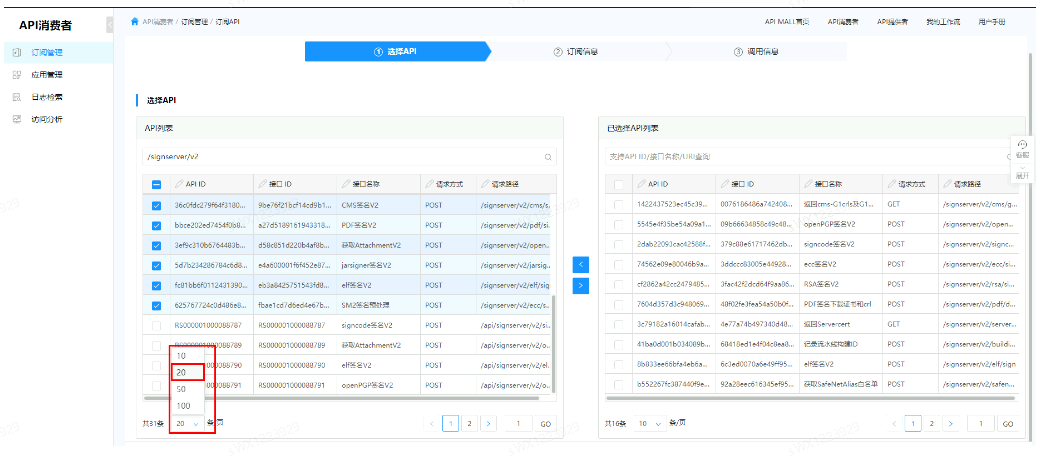
### 3.1 订阅签名中心API接口

访问：https://console.his.huawei.com/apimall/#/buyer/batchSubscribe?app id=huawei.eip.apigw

1. 新建



1. 选择API，搜索关键字：“/signserver/v2”选择其下的16个接口，“/timestampserver/v2”其下的1个接口



1. 下一点，确定订阅信息，订阅有效期等
2. 提交

### 3.2 订阅云龙API接口（用于cloudbuild2.0）

签名代理5.1.23及以上版本需要调用两个云龙接口

1. 注册DEVUC“/ssoproxysyr/v2/appids/appid/token”接口
2. 注册build2.0"/build-project-api/records/recordld/checklnBuild"接口

## 4 签名代理安装

### 4.1 使用自动安装脚本

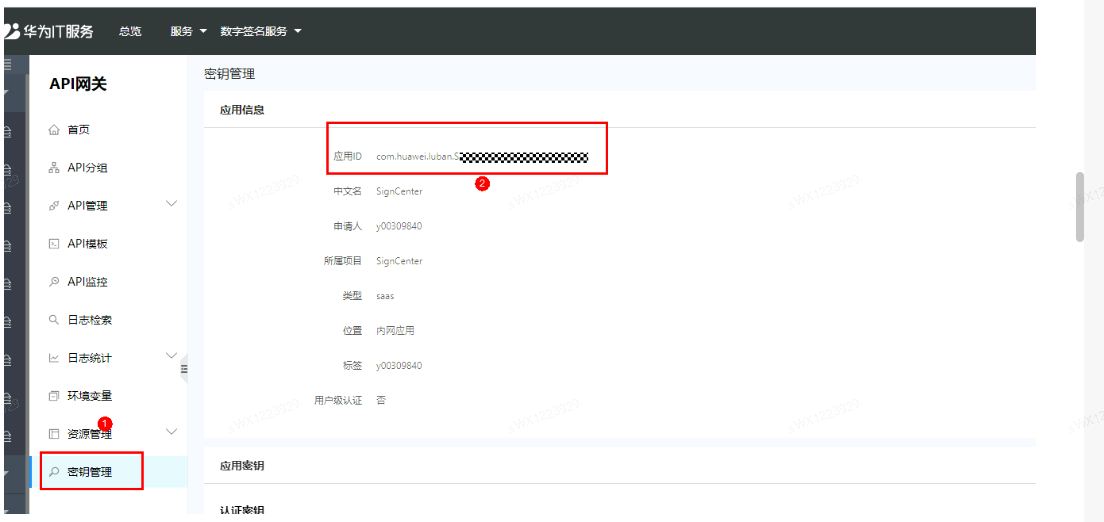
1. 获取下载脚本：https://pbm.ipdhuawei.com/pdmcore/plmhelpui/prod/item/?prodCode=pki& filename=resource/proxy install.zip
2. 配置脚本：proxy\_install/install\_conf/**install.conf**



* proxy.version: 要安装的签名代理版本
* proxy\_download.url: 改版本的下载地址
* 默认5.1.19，需要其他版本可以访问<https://build.huawei.com/build/project/buildToolManage?tab=aidTool>, 搜索“SignatureProxy”选择合适的版本，修改版本号和下载地址

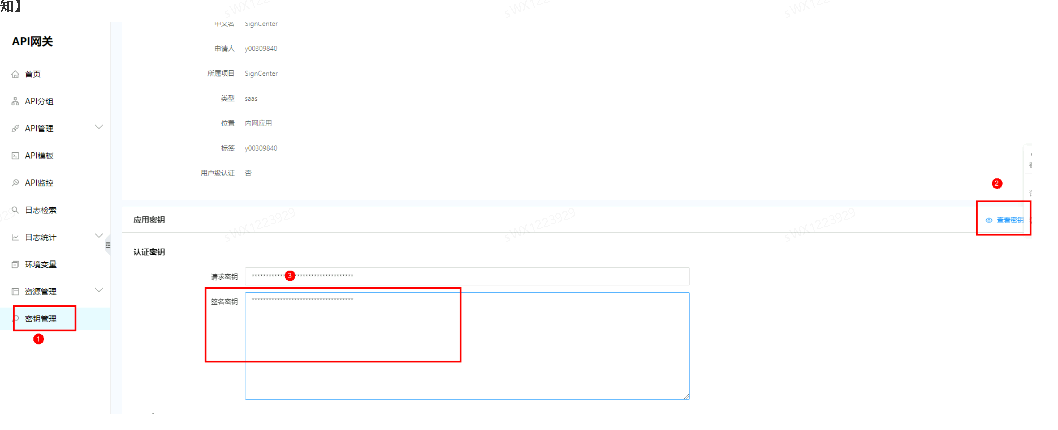


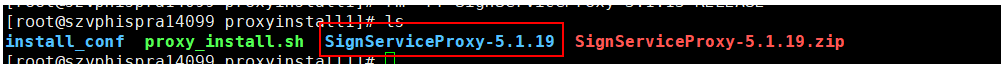
1. 配置cert\_new.pfx(流程IT密钥库)
   1. 拷贝[1 申请客户端权限认证证书](#_oa32cwoct2m)中获得的私钥与公钥证书到install\_conf目录下，重名为private.key和server.cer，修改install.conf中的itpfx.pass为自定义的pfx证书秘钥
   2. 如果获得的是pfx文件，则重名为cert.pfx，itpfx.pass填写流程it提供的pfx密码
2. enablejenkinsbuild
   1. 默认为true，表示使用jenkins模式；若是使用cloudbuild2.0模式，则false
3. 配置app.id
   1. 访问：https://console.hic.huawei.com/apigw portals/#/app/key（[3 订阅签名中心API接口](#_cnx448mehx9q)）， 获取app.id

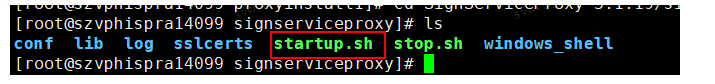


* 1. 配置app.sign.key: 获取签名秘钥原文，进行SCC加密
     1. 需要获取并安装、配置SCC
     2. 调用 ./CryptoAPl-e APIGW中查询到的签名密钥明文-f/usr/local/seccomponent/conf/scc.conf， 将获得的密文复制到app.sign.key





1. 执行安装脚本 proxy\_install.sh
   1. 
   2. 
   3. 进入SignServiceProxy-xx/signserviceproxy目录



## 5 签名插件安装

## 5.1 使用自动安装脚本

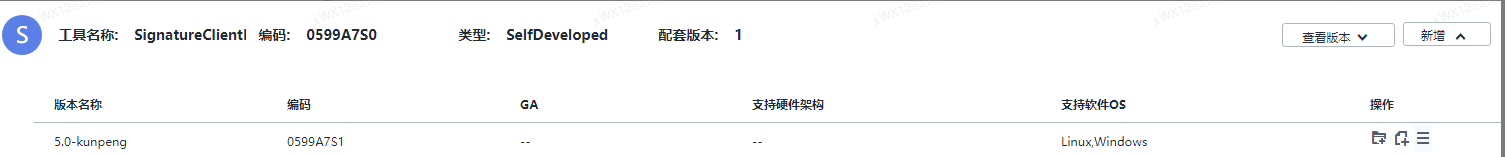
需要在签名代理上已经执行安装脚本

根据使用的模式：若是使用jenkins模式，脚本只会安装slave插件，还需要先安装master插件

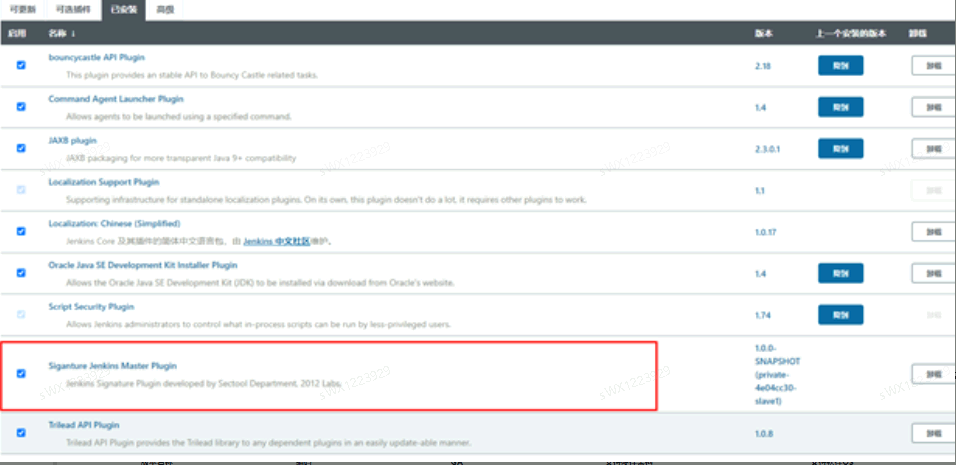
Master 和slave是否是同一台机器（安装在41上）？

### 5.1.1 Master插件安装

1. 访问： [https://build.huawei.com/build/project/buildToolmanage?tab=aidTool，](https://build.huawei.com/build/project/buildToolmanage?tab=aidTool%EF%BC%8C) 搜索”SignatureClientMaster”，下载最新版本

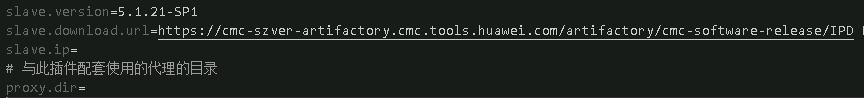


1. 使用web访问jenkins页面，点击manage Jenkins - Mange Plugin - 高级，选择刚才下载的插件，上传插件文件
2. 插件安装完成

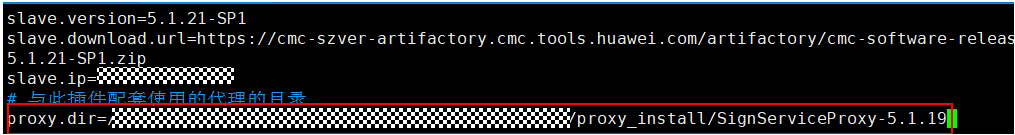


### 5.1.2 脚本安装slave插件

1. 获取脚本： https:/pbm.pd.hu awei.com/pdmcore/plmhelpui/prod/item/?prodCode=pki& filename=resource/sianslave install.zip
2. 进入slave\_install\_conf目录，配置文件slave\_install\_conf.conf

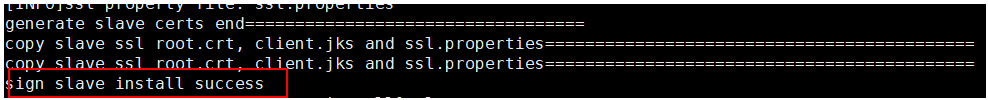


1. 使用和[4.1 使用自动安装脚本](#_r2n4uadtwg5k)一样的方式修改版本和下载（看教程截图，签名插件的版本是5.1.21-SP1，配套的签名代理的版本是5.1.19，所以应该签名插件和签名代理的版本不用匹配）
   1. 访问[https://build.huawei.com/build/project/buildToolManage?tab=aidTool，](https://build.huawei.com/build/project/buildToolManage?tab=aidTool%EF%BC%8C) 搜索“SignatureClient”
2. 配置签名插件执行机ip
3. 配置ssl通信根
   1. 方式一：配置签名代理的安装目录到proxy.dir, 安装脚本自动从目录中获取ssl通信根（安装脚本并没有配置签名代理的ip, 脚本如何自动获取签名代理的ssl通信根？）



* 1. 方式二：将签名代理安装时生成的ssl通信根手动复制到slave\_install\_conf目录中
     1. 注：签名代理SignServiceProxy-XX/**sslRootCerts**目录下的三个文件，**root.jks、root.crt、root.properties**

1. 执行安装脚本



成功后获得带ip后缀的插件目录

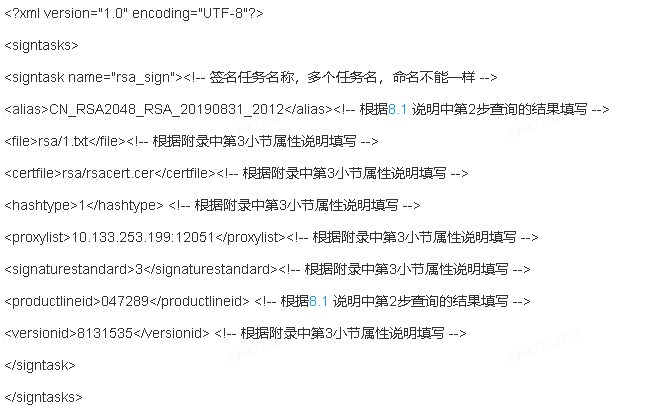


1. 对于Jenkins模式，进入插件目录，复制SignatureJenkinsSlave-x.x.xx（安装完毕的插件目录）到对应执行机（slave.ip所在的机器）使用

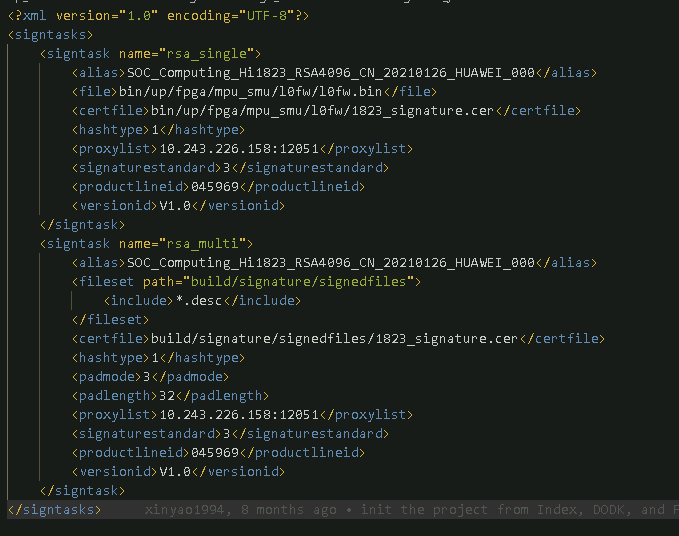
## 6 签名任务配置

### 6.1 Jenkins.xml 签名任务文件配置说明

xml文件格式参考：



模板 signconf\_jenkins.xml：



参数值查询（alias、productlineid）：

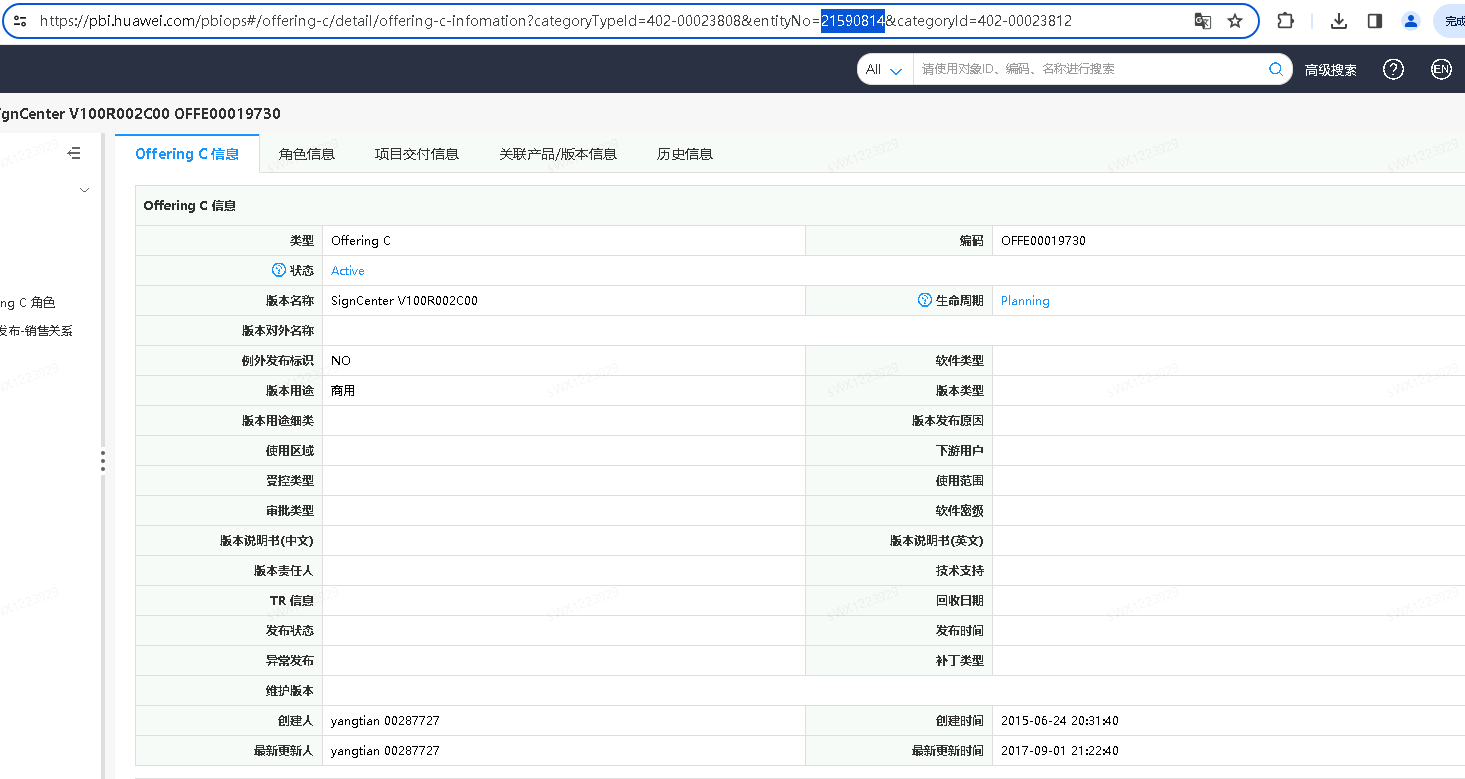
1. 访问：<https://signcenter.clouddragon.huawei.com/SignCenter/home> ,点击客户端信息，搜索[2 申请客户端签名权限](#_cvh4hxxkxf8l)注册的ip地址（签名代理的ip：**10.243.226.158**）



1. producelineid=BUID
2. alias=证书/公钥

其他参数值：

* file: 待签名的文件，文件路径相对于工程目录
* fileset：配置多个文件签名
  + path属性配置文件查找起始路径，可以是相对路径或者绝对路径
  + include属性，配置签名文件，支持后缀通配符
* hashtype：摘要算法，1-sha256，……
* proxylist：签名代理列表，签名代理的ip加端口号，配置多个时中间加分号
* Signaturestandard：3-RSA签名
* versionid：度量参数，度量平台根据该值确认产品是否做了构建签名，填写**产品的版本信息**。根据实际构建版本号填写，需要配置为产品C版本，查询FAQ:http://3ms.huawei.com/hgroup/3532079/thread 7318035.h
  + 访问PBI网站 http:/pbi.huawei.com/
  + 展开产品目录树，点击需要查看的产品信息
  + 弹出网址中的entityNo=xxxx,就是versionid



产品的版本信息是否知道？模板上填的是v1.0是否需要更改？

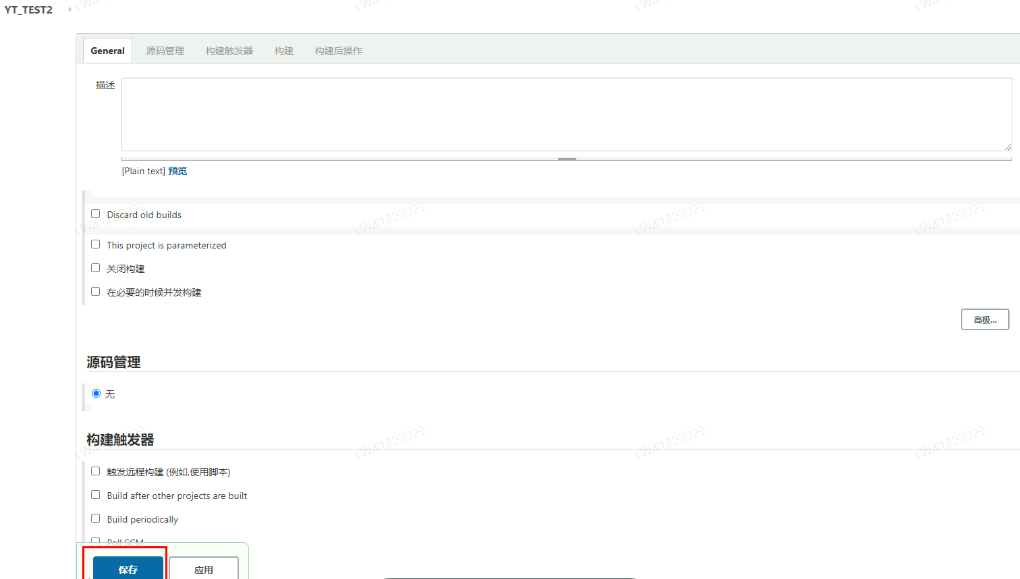
* crlfile: CMS参数 crl文件的保存路径，相对于workspace路径(配置路径可自动下载，用于签名验证)当**CMS密钥别名中包含G2/G3/G4/G5的蜜钥别名，crlfile参数无需配置，签名过程不再下载CRL文件**
* certfile: RSA/ECC/SOC参数，这个参数表示rsa/eCC/SOC签名私钥对应验证用证书的保存路径，这个路径相对于workspace的路径，这个证书可以提取公钥用于校验（signconf\_jenkins.xml中对应的路径下并没有指定的文件）
* padmode：RSA-PSS参数，可选，默认为0，只有当签名标准为RSA时才起作用
  + 0：使用PKCS1v15填充
  + 1：使用PSS填充，随机数与哈希值等长，其余填0
  + 2：使用PSS填充，随机数填满所有空白
  + **3：使用PSS填充，随机数长度由padLength指定，其余填0**
  + 4：纯加密算法
* padlength：RSA-PSS参数 当padmode为3时有效，指定填充长度，取值范围： 摘要长度(字节)~(RSA密钥长度-摘要长度-2) (字节)

### 6.2 Jenkins构建，签名任务配置

1. 打开Jenkins web管理端并登录，新建item



1. 进入任务配置页面，先不设置，直接点击保存



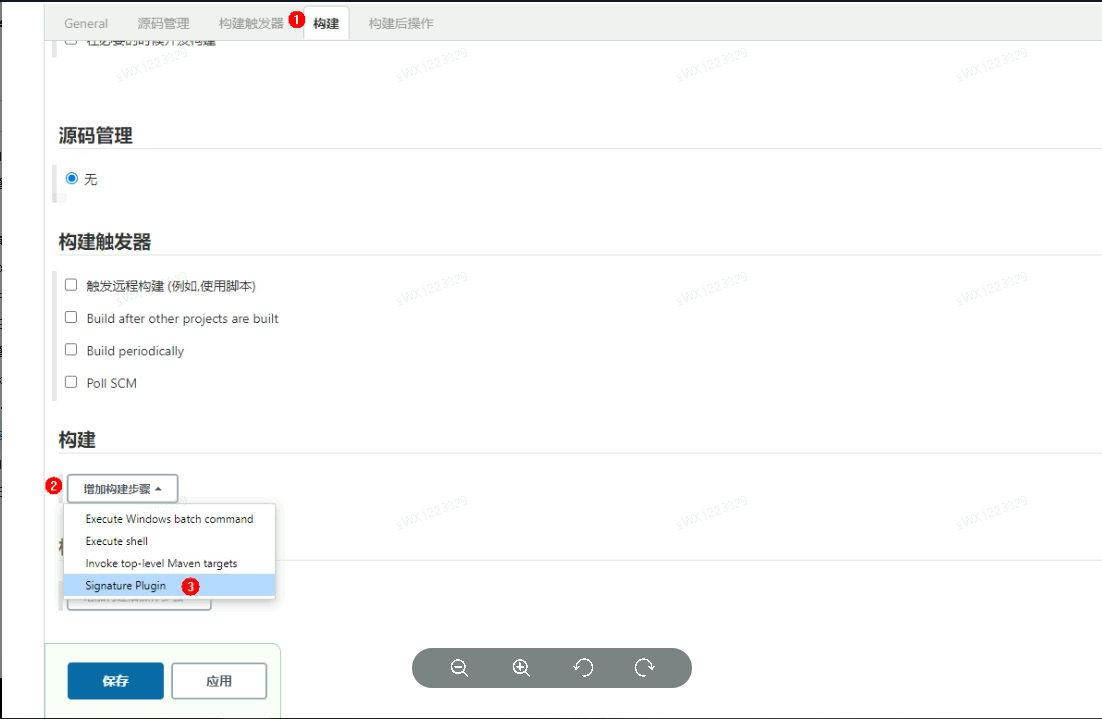
1. 进入创建的任务，选择build now



1. 构建完成之后进入构建详情，选择控制台查看输出信息，发现项目创建了工作文件夹



1. 在工作文件夹下放置签名任务配置xml文件（signconf\_jenkins.xml）
2. 选择一个工程，进入配置，增加构建步骤，选择Signature plugin



这里说的不清楚，Signature plugin 和刚才扔进去的xml文件怎么发挥作用？

还是说在Jenkins中直接构建刚才那个空项目，然后签名插件安装的Signature plugin就会通过xml知道要签名的文件以及签名代理的地址，然后执行plugin，实现通过签名代理完成签名？