

## 组网及说明

ADDC安全纳管标准方案

## 问题描述

点击同步失败



## 过程分析

升级流程为：控制器上传相应的特征库，点击同步后，通过FTP的方式将特征库传输到设备指定目录，设备加载相应的特征库文件，完成升级。

1、排查设备的logbuffer，可以看出控制器已经将文件推送到设备，设备执行失败。



2、控制器升级IPS特征库时，控制器先检测DIM主引擎所在板卡，然后修改addcadmin（远端用户）用户的默认存储目录

控制器下发修改命令，在设备看来就是控制器下发了一个本地用户addcadmin（本地用户），并且修改了默认路径

```
%Aug 23 14:56:06:195 2023 H3C XMLAGENT/6/XML_REQUEST: yuyao from 186.20.88.201,session id 1,message-id 342,receive edit-config request.<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-><edit-config><target><running/></target><><config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"><top xmlns="http://www.h3c.com/netconf/config:1.0"><UserAccounts><Management><Accounts xc:operation="merge"><Account><Name>yuyao</Name><FTP>false</FTP></Account></Accounts></Management></UserAccounts></top></config></edit-config></rpc>
```

随后下载特征库，此时用的是远端的addcadmin（远端用户）的来进行下载，所有还是下到flash下，最终返回失败。

3、控制器+M9K+远端认证场景下，控制器通过用户名addcadmin（远端用户）登陆防火墙时候，防火墙先去远端认证通过后允许控制器纳管，但是控制感知不到用户是远端用户还是本地用户

## 解决方法

建议控制器使用非远端用户进行特征库升级或防火墙本地升级特征库。