天翼云·SSL VPN

安全加固操作指南

天翼云科技有限公司

2022 年 7 月

目录

第 1 章 前言.....2
第 2 章 准备工作.....2
2.1 事前准备.....2
2.2 设备升级开放端口开启关闭方法.....2
2.3 设备加固.....4
2.3.1 补丁包实施.....4
第 3 章 注意事项.....10

第1章 前言

已知问题，近日天翼云在持续的产品加固自查过程中发现的，天翼云 SSL VPN 设备存在一个安全风险可被攻击者利用。对此，天翼云已推出安全补丁，强烈建议您在服务人员的协助下立即进行排查验证和补丁修复提前整理升级方案。

第2章 准备工作

2.1 事前准备

1、Windows PC 一台，用于升级，巡检等操作

2、补丁包 Security-reinforcement-patch-package.rar

3、升级工具 SANGFOR_Updater6.1

补丁包及工具下载地址：

https://oos-cn.ctyunapi.cn/downfile/2022download/SANGFOR_Updater6.1.zip

https://oos-cn.ctyunapi.cn/downfile/2022download/Security-reinforcement-patch-package.rar

2.2 设备升级开放端口开启关闭方法

51111 端口

对应服务：升级服务

关闭影响：不能通过升级服务客户端进行远程升级，仅关闭了外网的使用，不影响内网

注意事项：安全组需要放 51111 端口权限

开启方法：通过升级客户端升级加固补丁，需开启 51111 升级客户端：

方法一：登录 SSLVPN 控制台【系统设置】-【系统配置】-【运维配置】-升级维护

勾选“启用 LAN 口临时访问”，然后点击保存。

方法二：则需使用 IE 浏览器在①【系统设置】-【系统配置】-【控制台配置】-启用远程维护支持；②在【防火墙设置】-【过滤规则设置】-【本机规则】-启用允许外网使用升级客户端进行维护。

有该界面出现，表示端口打开成功

2.3 设备加固

2.3.1 补丁包实施

2.3.1.1 安全加固包

支持版本范围：7.5

M5.0-M768R2

补丁包影响范围

SP_SSL_AW_01 ：

M7.5及以上版本：升级会重启svpn服务，用户会重连导致无法访问资源，影响时间3分钟左右；

SP_SSL_WD_04 ：

升级会重启 boa 服务，影响 VPN 控制台登录和访问，影响时间：1 分钟；但不影响客户业务

补丁包实施流程

1、准备升级环境

1)准备一台安装 Windows 操作系统的 PC，连接 VPN 设备 LAN 口或者公网 IP；

2、实施流程

如果是单台设备，直接升级即可

如果是集群环境，无需拆集群，直接在分发器上升级，真实服务器会自动同步升级，

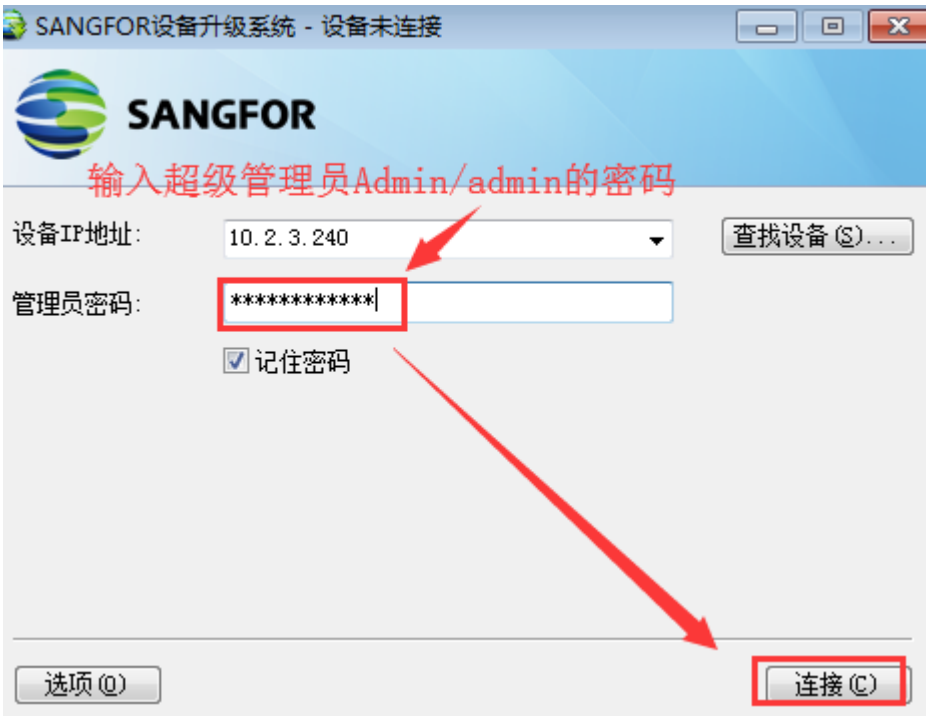
如果是分布式环境，先升级主节点，再升级从节点；如果节点是本地集群部署，按集群环境升级即可

1）设备实施流程

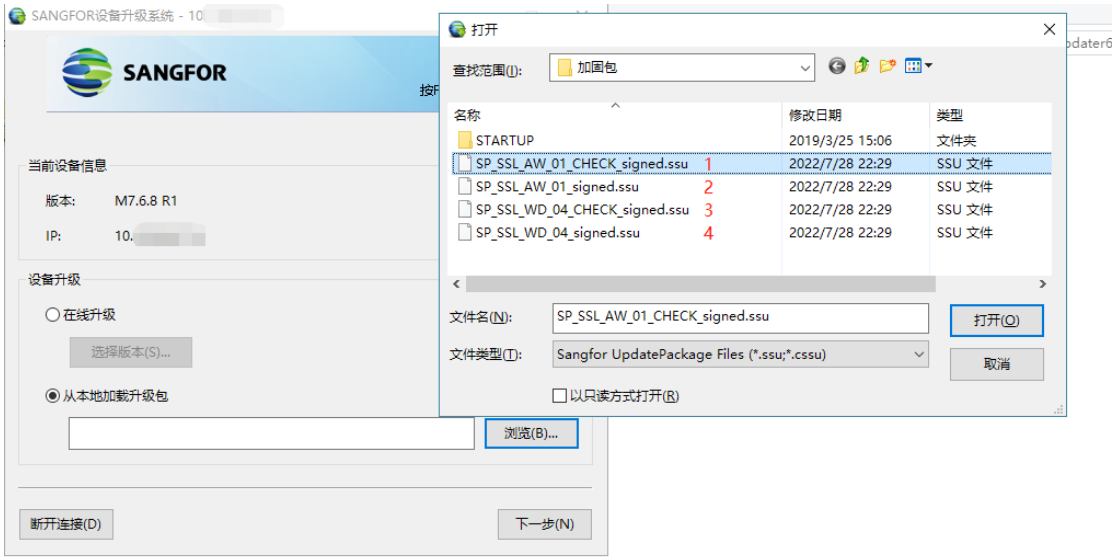
首先使用升级客户端 Sangfor Updater 6.1 加载相应的补丁包的 Check 包检测补丁包的是否与其他补丁或定制冲突，Check 包加载完成显示升级成功后，再加载补丁包；补丁包加载完成提示升级成功后，查看设备版本信息有对应的补丁包字段即完成实施。

（1）打开升级客户端，输入 SSL 设备 IP 地址和控制台超级管理员 admin/Admin 的密

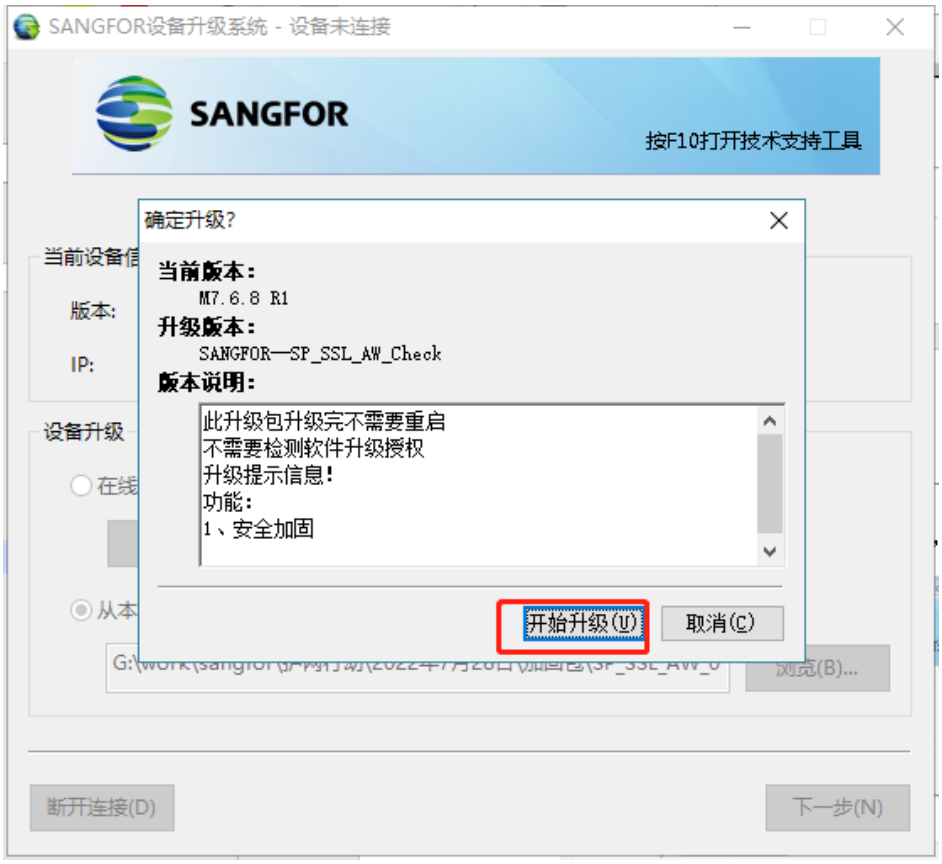
码，然后连接设备。



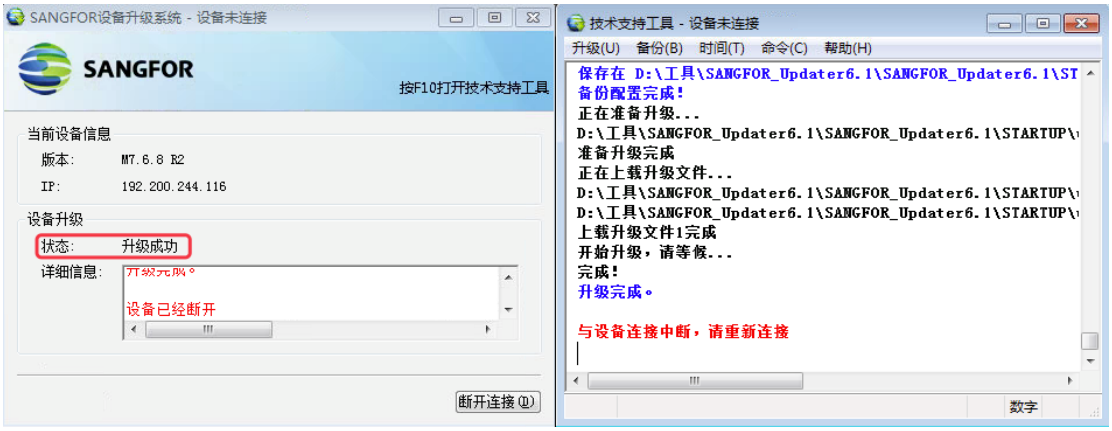
(2)选择从本地加载补丁包的 Check 补丁包，点击 下一步 按钮。



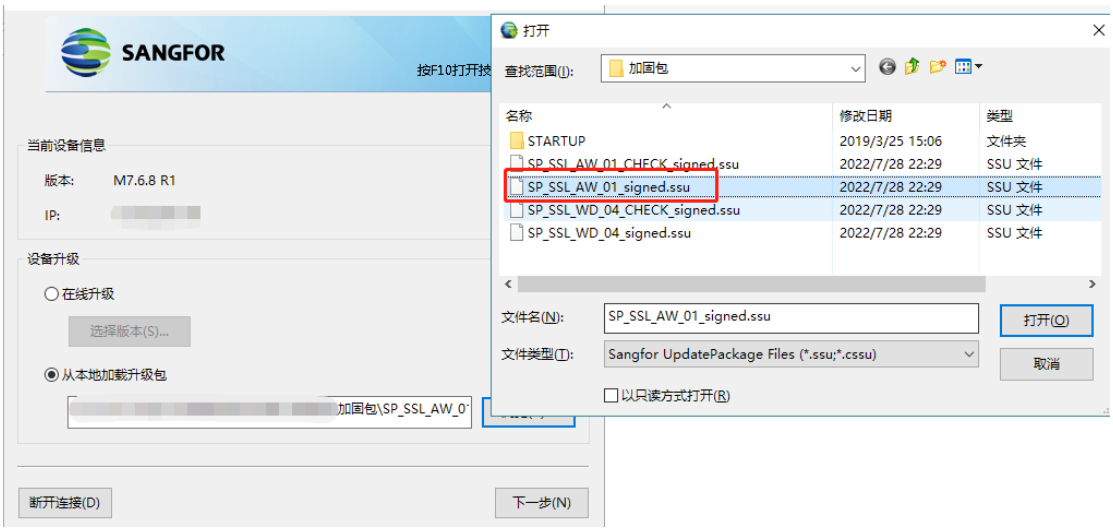
(3)再次确认升级，点击 确认升级 。



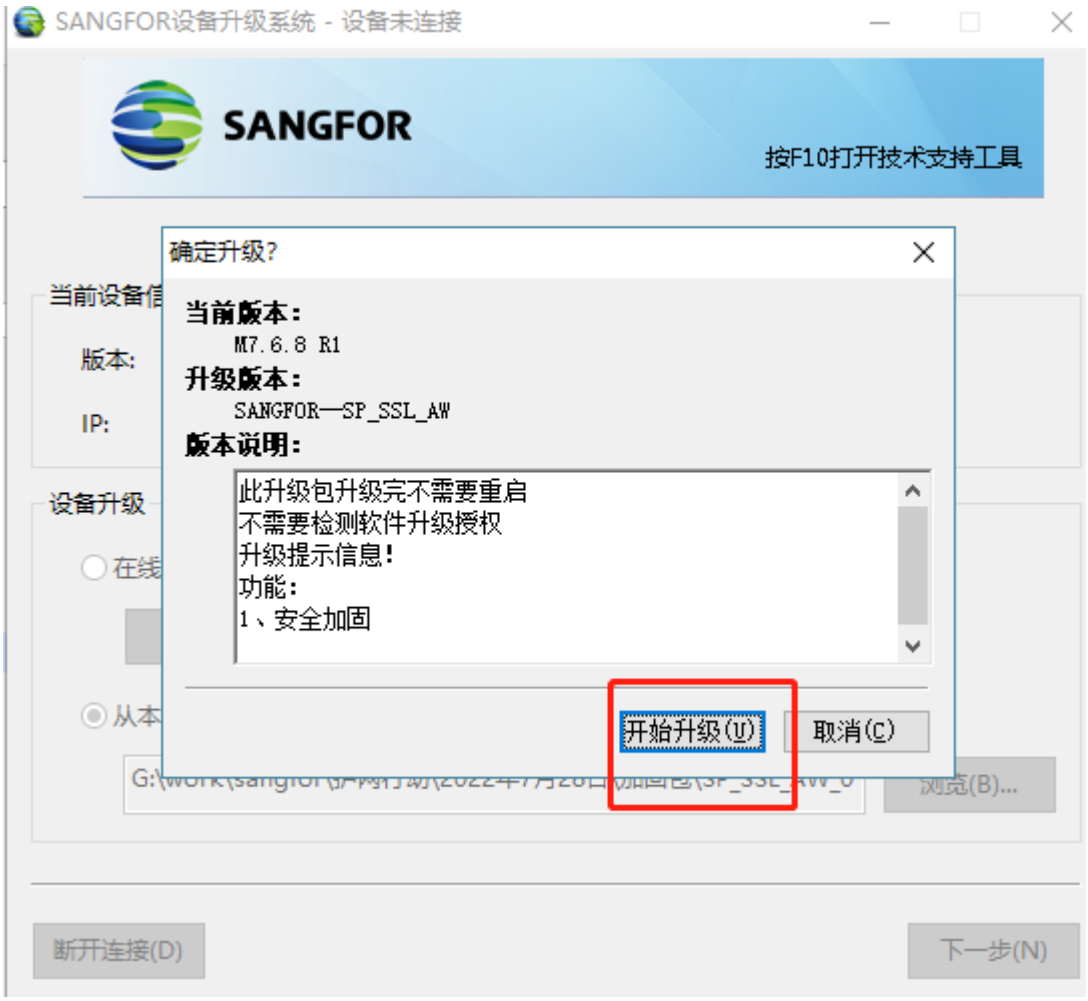
（4)确认升级后，等待一段时间，会提示升级完成，则代表检测通过，可以实施补丁包。



（5)点击断开连接，再次重新连接上设备后，选择补丁包，点击 下一步 加载升级

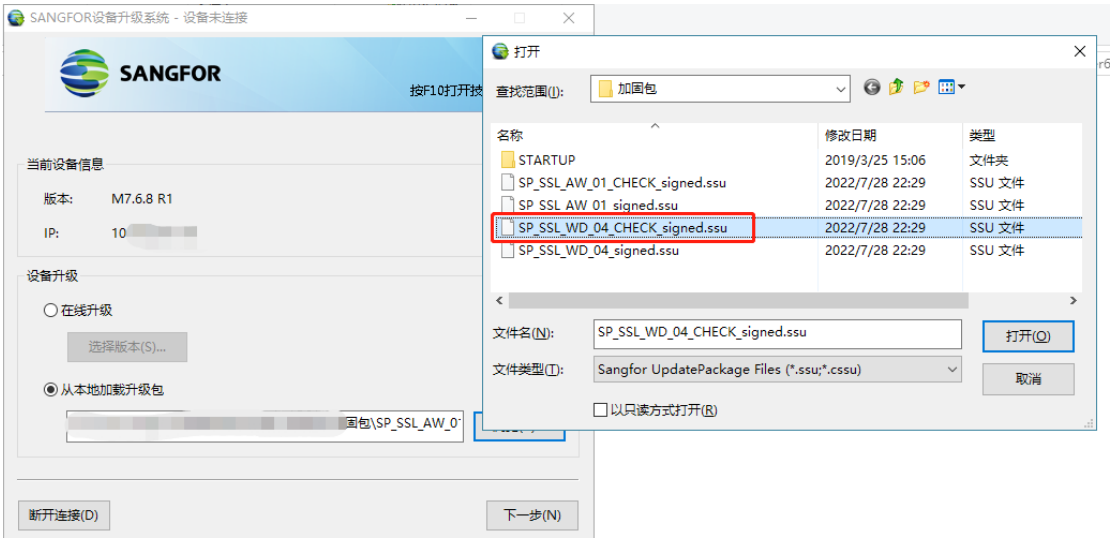


（6）再次确认升级，点击 开始升级 。

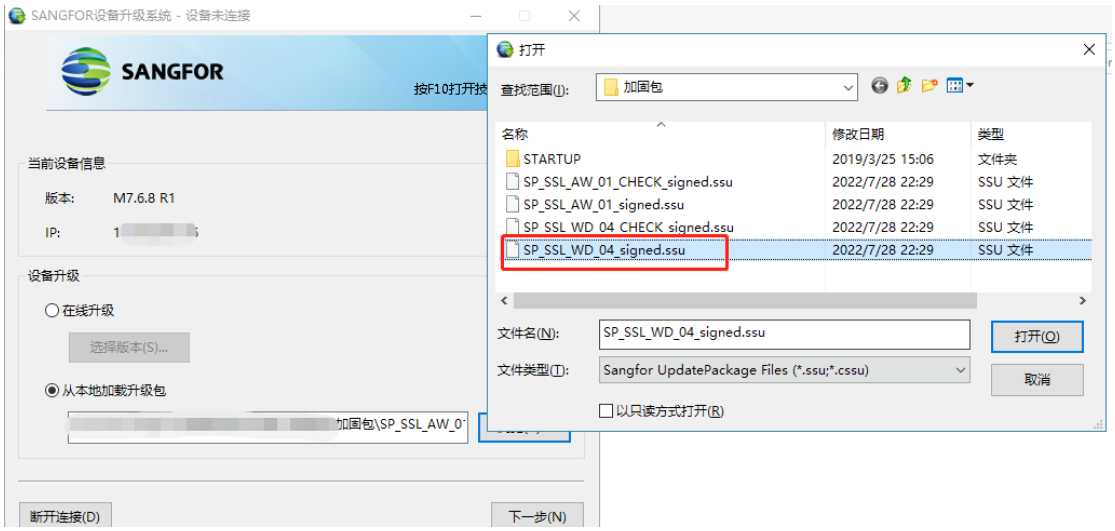


（7）确认升级后，等待一段时间，提示升级完成，补丁包完成升级。

（8)点击断开连接，再次重新连接上设备后，选择补丁包，点击 下一步 加载升级，通过升级工具加载 SP_SSL_WD_04_CHECK_signed.ssu 包升级，检查当前设备是否能升级（返回“升级完成”即说明可以升级此次补丁包，否则当前设备不支持升级此次补丁包）

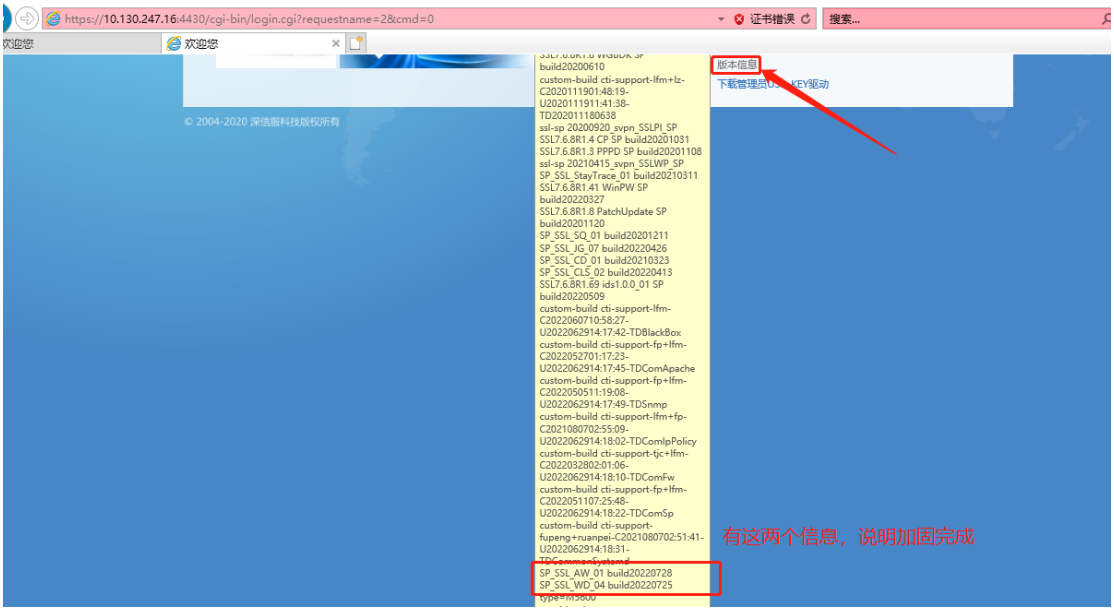


（9)点击断开连接，再次重新连接上设备后，选择补丁包，点击 下一步 加载升级，通过升级工具加载 SP_SSL_WD_04_signed.ssu 包升级，检查当前设备是否能升级（返回“升级完成”即说明可以升级此次补丁包，否则当前设备不支持升级此次补丁包）



2.3.1.2 安全加固完成标志

查看设备的版本信息有对应的补丁包名称 SP_SSL_WD_04、SP_SSL_AW_01，说明升级成功。



2.3.1.3 补丁包回退

实施完补丁包需验证业务是否有异常，若出现不可控的异常问题，在短时间不能解决的，应尽快恢复业务，回退方式如下：

appversion 中从下往上依次回滚

集群环境下回滚：不用拆分集群，先回滚分发器，再回滚真实服务器

双机环境下回滚：需要拆分双机，每台设备都需要回滚

分布式环境下回滚：不用拆分分布式，先回滚主节点，再回滚从节点

SP_SSL_WD 包回滚步骤：

回退步骤：

1、进入设备后台

2、执行命令：cd /hislog/cti-support/SP_SSL_WD/

3、执行命令：setsid ./cti-support.sh -roll

4、等待 15s，回滚操作完成

SP_SSL_AW 包回滚步骤：

回退步骤：

1、进入设备后台

2、执行命令：cd /hislog/cti-support/SP_SSL_AW/

3、执行命令：setsid ./cti-support.sh -roll

4、等待 15s，回滚操作完成

第3章　注意事项

1、升级完成后需要登录 sslvpn 控制台，关闭升级维护访问选项。

2、安全组放开 51111 端口访问权限需要删除。