



某科技集团 Checkpoint 防火墙 升级方案

北京一实天勤科技有限公司

2023. 4

目录

一、 升级原因	1
二、 升级准备	1
2.1 配置备份	1
2.2 升级包准备	3
2.3 管理服务器快照	4
三、 升级步骤	4
3.1 升级管理服务器	4
3.2 升级备机	5
3.3 主备切换，升级主机	5
3.4 主备切换，恢复网络	6
四、 回退计划	6
五、 时间节点表	7

一、升级原因

因当前软件版本 R80. 30 原厂已经停止支持, 故需根据官方要求进行版本升级, 本次升级到 R81. 10。

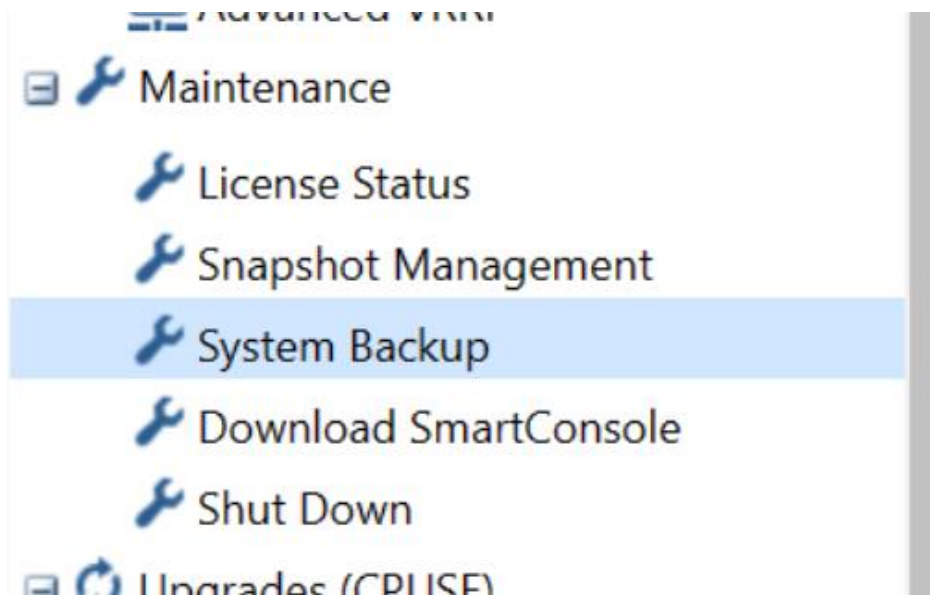
二、升级准备

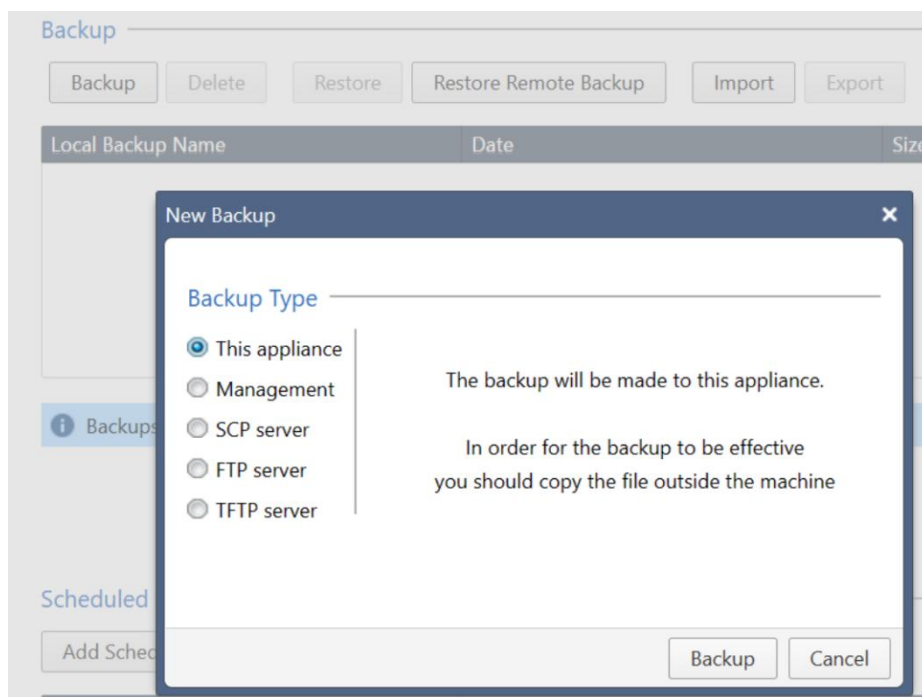
为保证在规定时间内完成升级, 并确保升级之后遇特殊情况设备可顺利回退, 需做如下升级准备。

2.1 配置备份

进行硬件设备备份:

登录设备界面 选择 Maintenance- System Backup





选择 backup。完成后将文件下载到本地。

进行管理服务器配置备份；

命令行运行 expert 进入专家模式，

```
CP-SMC> expert
Enter expert password:

Warning! All configurations should be done through clish
You are in expert mode now.
```

cd \$FWDIR/bin/upgrade_tools/, 运行 ./migrate export 202304.tgz,
执行前关闭 smart console 客户端软件。

```
You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y

Copying required files...
Compressing files...

The operation completed successfully.

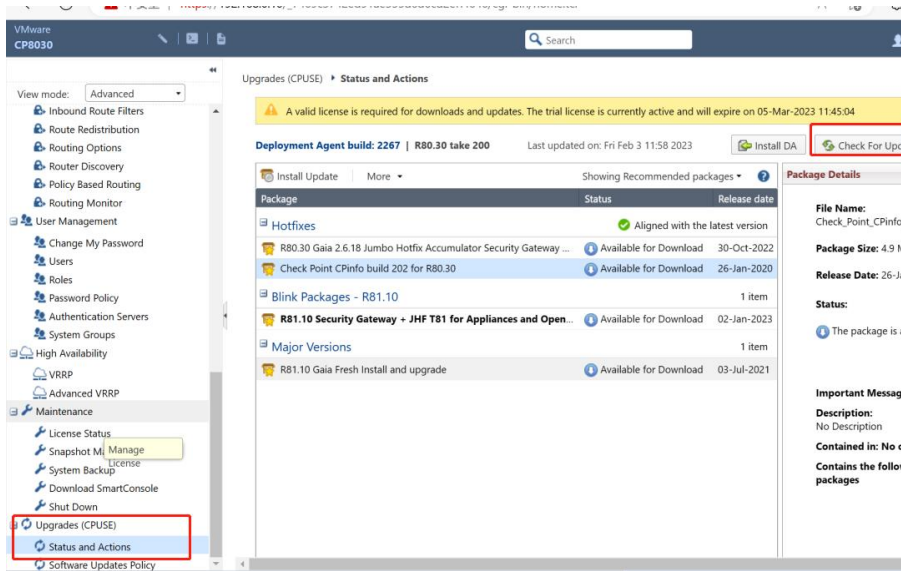
Location of archive with exported database: /opt/CPsuite-R80.40/fw1/bin/upgrade_
tools/20230105.tgz

[Expert@CP-SMC:0]#
```

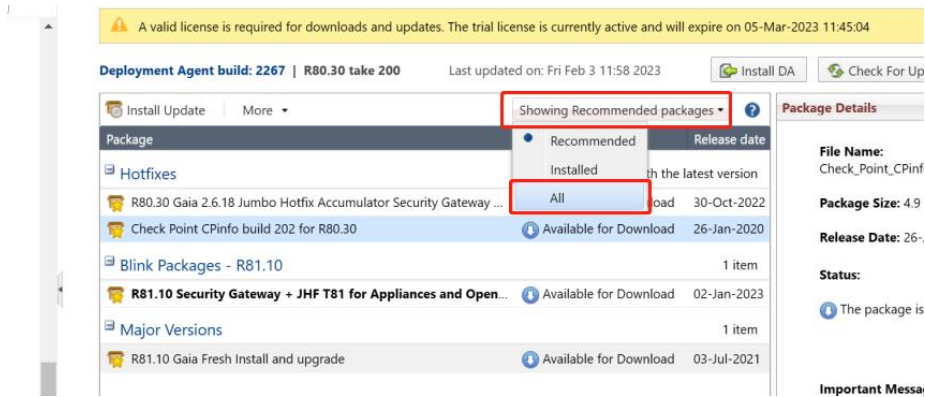
```
[Expert@CP-SMC:0]# ls
20230105.tgz          migrate                pre_upgrade_verifier
del_revision_files   migrate.conf          puv_report_generator
gtar                  plugin_pack.conf      test.tgz
gzip                  plugin_pack_compare   update_inspect_files
ips_upgrade_tool     plugin_upgrade_matcher
mgmt_puv.sh          ppidb.conf
[Expert@CP-SMC:0]#
```

2.2 升级包准备

提前准备好设备的可用升级包，登录设备 WEB 界面，在 Upgrades -Status and Actions 下 check For Update 下载需要的安装包。



可切换查看所有可用的安装包



右键进行安装包的验证。



系统会验证结果，显示 Installation Upgrade is allowed 后，进行 Download。

2.3 管理服务器快照

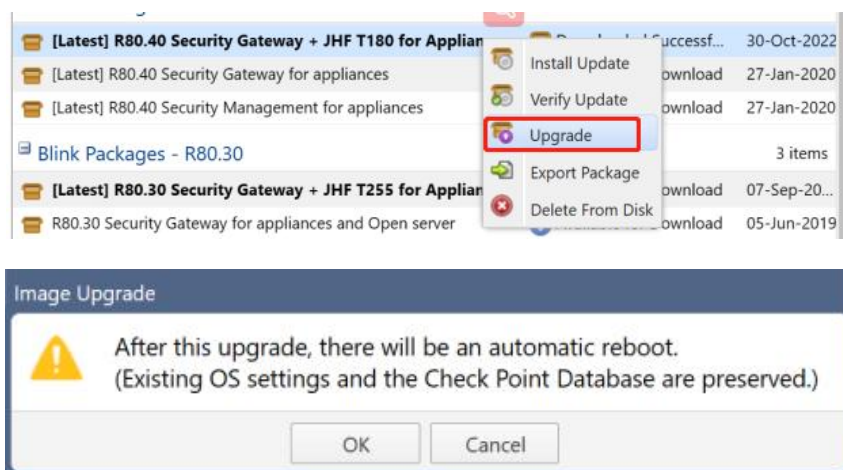
为快速进行配置服务恢复，建议在升级之前，由虚拟机管理员进行管理服务器虚拟机镜像。

三、升级步骤

3.1 升级管理服务器

首先升级管理服务器，整体过程预计 1 小时：

在 web 界面，下载升级包界面，对应下载的安装包右键，选择 Upgrade 即可。



The package is installing: 45%

Step	Duration	Info
Initialization	0s	initializing
Preparation	8s	verifying the packag
Validation	6s	
Installation	1m2s	

升级完成后，系统会自动重启，显示升级后的版本。

3.2 升级备机

升级备机，整体过程预计 1 小时：升级步骤同管理服务器，不再赘述，升级完成后，查看设备状态，设备运行无误后，准备升级主机。

3.3 主备切换，升级主机

命令行运行 `cphaprob stat` 或 `show cluster state`，查看 HA 状态，Local 是当前操作主机。

```
Cluster Mode: High Availability (Active Up) with IGMP Membership
ID           Unique Address  Assigned Load  State      Name
1 (local)    [redacted]      100%          ACTIVE     CP-FW1
2            [redacted]      0%            STANDBY   CP-FW2
```

在 Active 的设备运行 `ClusterXL_admin down`，会使当前主机状态为 down 状态，使得流量切换至备机。

```
Cluster Mode: High Availability (Active Up) with IGMP Membership
ID           Unique Address  Assigned Load  State      Name
1 (local)    [redacted]      0%            DOWN       CP-FW1
2            [redacted]      100%          ACTIVE     CP-FW2
```

切换时正常状态最多丢失 3 个数据包，查看业务状态，业务顺利迁移到备机后，进行主机升级，如不正常切换主备状态，停止升级，执行回退。升级步骤同上，不做赘述，升级过程预计 1 小时。

3.4 主备切换，恢复网络

主机升级完成后，命令行运行 `cphaprob stat` 或 `show cluster state` 查看主机状态，在当前主机输入 `ClusterXL_admin down`，切换主备状态

ID	Unique Address	Assigned Load	State	Name
(local)		0%	STANDBY	CP-FW1
		100%	ACTIVE	CP-FW2

切换后观察业务是否正常，如正常升级成功，如不正常切换主备状态。

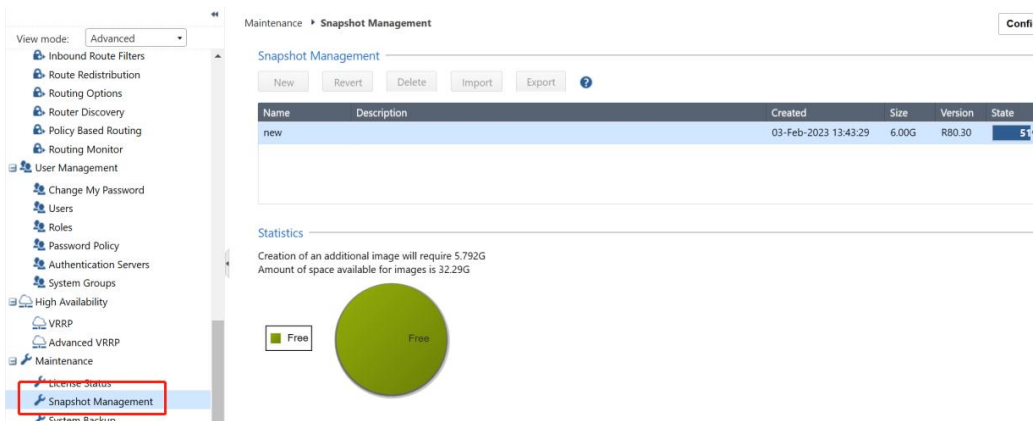
业务正常后测试一下遗留问题是否依然存在，如存在继续更新 Case

四、回退计划

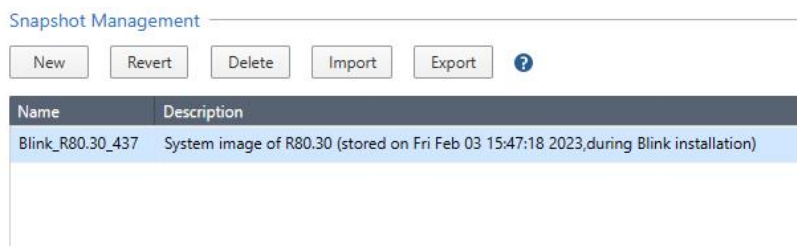
当升级出现意料之外的计划时，优先保障业务，采取回退措施。

管理服务器回退时，直接联系虚拟机管理员恢复设备快照。

硬件设备回退时，在设备 Web 界面点击 Snapshot Mangement ，



升级安装前，安装进程会再次自动执行系统快照，回退执行 revert，可以退回到升级安装前版本。



五、时间节点表

全部升级需要 3-3.5h 如下为时间节点表。

序号	内容	时长	是否完成	备注
1	管理服务器升级	1h		
2	备机升级	1h		
3	主备切换	1s-2s		
4	业务查看	10min		
5	主机升级	1h		
6	主备切换	1s-2s		
7	业务查看	10min		