CAS 7.0批量禁用虚拟机vnc端口的方法

杨海严 2020-07-10 发表

组网及说明

对安全性要求高的单位，一般要求将CAS虚拟机端口禁用，本文提供CAS 7.0采用iptables实现批量禁用虚拟机vnc端口的方法。

配置步骤

已开发脚本工具 set_vnc_port（见本文附件）

（1） 上传脚本到CVK主机，添加脚本可执行权限

（2） 执行 ./set_vnc_port disable脚本，会自动禁止该CVK上的vnc 5900～5999端口

（3） 执行完后，使用 iptables -L -n 查看结果

扩展：

set_vnc_port.sh disable 禁用vnc端口，所有的ip都不能访问

set_vnc_port.sh enable 启用vnc端口

set_vnc_port.sh disable "ip1,ip2,ip3..." 禁用vnc端口，指定的ip可以访问VNC端口

set_vnc_port.sh enable "ip1,ip2,ip3..." 启用vnc端口，同时删除指定ip的iptables规则（需要指定ip，才能够清除所有的iptables规则）

配置关键点

防止主机重启配置失效， 保存iptables规则，CVK的操作方法如下：

1. 所有的iptables规则配置完成之后，将规则保存配置文件中 iptables-save > /etc/iptables.rules

2. 修改/etc/rc.local文件，在exit 0之前添加，如下：

```
touch /var/run/cas_cvk
/opt/bin/util_cvk_reserved_mem.sh
/usr/bin/set-printk-console 2
/opt/bin/open-iscsi_check.sh
/opt/bin/util_remove_audio.sh
/usr/bin/python /opt/bin/set_irq_affinity.pyc execute
/usr/bin/python /opt/bin/inspection_mem_cpufreq_init.pyc
iptables-restore < /etc/iptables.rules
exit 0
```

附件下载：set_vnc_port【适用CAS7.0】.zip