

知 A2020-G堡垒机访问权限规则不生效

堡垒机

刘宏宇 2019-11-26 发表

组网及说明

现场使用堡垒机纳管了一台虚拟机，虚拟机内添加了很多设备的rdpapp服务。

环境如下：



问题描述

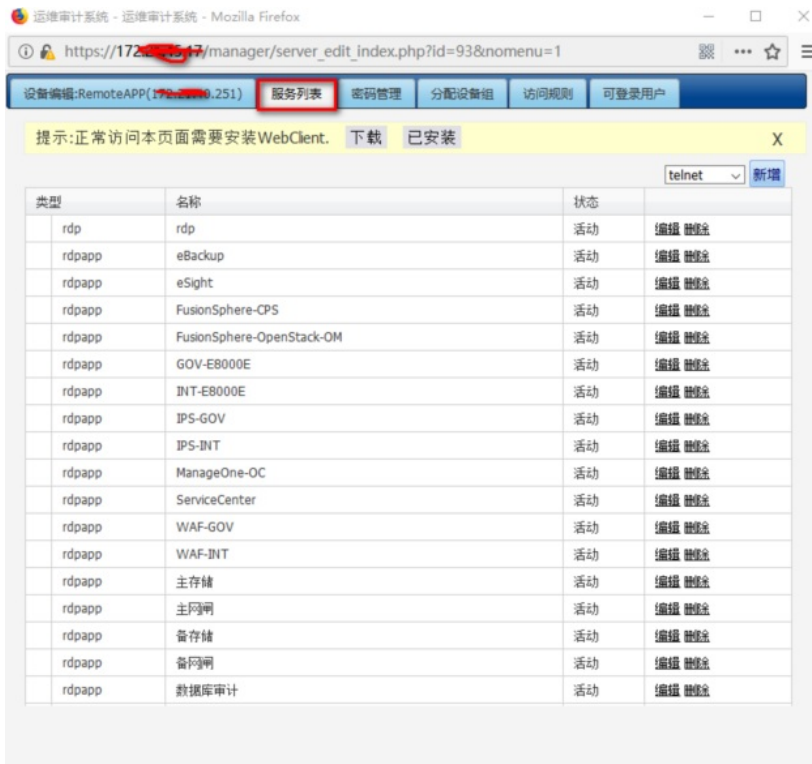
现在想让用户xxx仅可访问虚拟机中某三台设备的rdpapp服务，但是按照下图去配置对应普通用户登陆后还是可以访问虚拟机提供的所有rdpapp服务。

配置如下：

目标设备：



服务列表：



所属访问规则：



可登录用户：



访问权限规则：

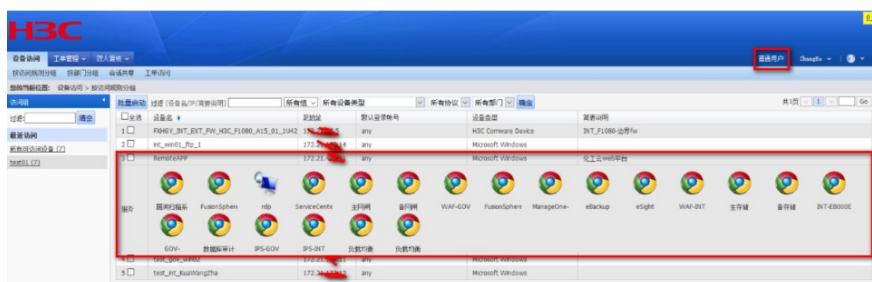


访问权限规则明细：



在这里可以看到服务名称中仅勾选了两台WAF和一台漏扫。

但是实际使用对应的普通账户登录后查看：



很明显该用户实际可以访问的服务不止在访问规则中允许的三个。

过程分析

明明在对应访问权限规则的服务名称中仅勾选了三个，为什么实际登陆后可以访问虚拟机提供的所有服务呢？

测试1：规则中勾选服务协议但是不勾选对应服务名称

您的当前位置: 权限控制 > 访问权限 > 编辑规则

创建者: admin (缺省管理员)

规则名称: xjytest

设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式)

部门: ROOT

服务类型: ☒ 字符终端 ☐ 图形终端 ☒ 文件传输

服务协议: ☒ telnet ☒ ssh ☒ rdp ☒ vnc ☒ rdpapp ☒ ftp ☒ sftp

服务名称: ☐ rdp ☐ sftp
☐ ssh ☐ ssh2
☐ ssh3 ☐ telnet

访问设备时生成事件

事件级别: None

标题:

磁盘映射: ☒ 允许使用

剪贴板: ☐ 下行 ☐ 上行

剪切板复制文件: ☐ 下行 ☐ 上行

普通用户登陆后:

最近访问

所有可访问设备 (1)

xjytest (1)

批量启动 过滤 (设备名/IP/简要说明) 所有组 所有设备类型 所有协议 所有部门 确定

☐ 全选	设备名	IP地址	默认登录帐号	设备类型
☐	M9000	172.31.0.18	无	H3C Comware Device

服务

ssh2 ssh3 ssh telnet sftp rdp

可见对应协议下的服务名称就算没有勾选也可以使用

测试2：勾选服务名称但是不勾选对应的服务协议

您的当前位置: 权限控制 > 访问权限 > 编辑规则

创建者: admin (缺省管理员)

规则名称: xjytest

设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式)

部门: ROOT

服务类型: ☐ 字符终端 ☐ 图形终端 ☐ 文件传输

服务协议: ☐ telnet ☐ ssh ☐ rdp ☐ vnc ☐ rdpapp ☐ ftp ☐ sftp

服务名称: ☒ rdp ☒ sftp
☒ ssh ☒ ssh2
☐ ssh3 ☒ telnet

访问设备时生成事件

事件级别: None

标题:

磁盘映射: ☒ 允许使用

剪贴板: ☐ 下行 ☐ 上行

剪切板复制文件: ☐ 下行 ☐ 上行

普通用户登陆后:

最近访问

所有可访问设备 (1)

xjytest (1)

批量启动 过滤 (设备名/IP/简要说明) 所有组 所有设备类型 所有协议 所有部门 确定

☐ 全选	设备名	IP地址	默认登录帐号	设备类型
☐	M9000	172.31.0.18	无	H3C Comware Device

服务

telnet sftp ssh2 rdp ssh

可见就算不勾选服务协议，但是勾选了对应的服务名称用户也可以正常使用

测试3：勾选服务协议，但是不勾选所有对应服务名称(勾选ssh的服务协议，但是三个ssh的服务名称只勾选ssh和ssh3)

您的当前位置: 权限控制 > 访问权限 > 编辑规则

创建者: admin (缺省管理员)

规则名称: xjytest

设备排序: 全局缺省 (终端登录菜单中的目标设备排序方式)

部门: ROOT

服务类型: ☐ 字符终端 ☐ 图形终端 ☐ 文件传输

服务协议: ☐ telnet ☒ ssh ☐ rdp ☐ vnc ☐ rdpapp ☐ ftp ☐ sftp

服务名称: ☐ rdp ☐ sftp
☒ ssh ☐ ssh2
☒ ssh3 ☐ telnet

访问设备时生成事件

事件级别: None

标题:

磁盘映射: ☒ 允许使用

剪贴板: ☐ 下行 ☐ 上行

剪切板复制文件: ☐ 下行 ☐ 上行

普通用户登录后:

最近访问	批量启动	过滤 (设备名/IP/简要说明)	所有组	所有设备类型	所有协议	所有部门	确定
所有可访问设备 (1)	☐ 全选	设备名	IP地址	默认登录帐号	设备类型		
xjytest (1)	1	M9000	172.31.0.18	无			
	服务						
		sftp	ssh2	ssh3	ssh		

可以看到, 就算服务名称没有勾选ssh2, 但是对应用户登录后还是可以使用ssh2的服务

综上所述:

访问权限规则中“服务协议”与“服务名称”是“或”的关系, 但是服务协议的优先级又高于服务名称。
也就是说服务协议和服务名称二选一普通用户都可以正常使用对应的服务, 但是在勾选了服务协议(ss h)的情况下, 即使不勾选属于该服务协议的某一个服务名称(ssh2), 普通用户也能正常使用该服务协议对应的所有服务(ssh1、ssh2、ssh3)。

解决方法

现场在访问权限规则中不勾选rdpapp服务协议, 只勾选允许的服务名称后问题解决。