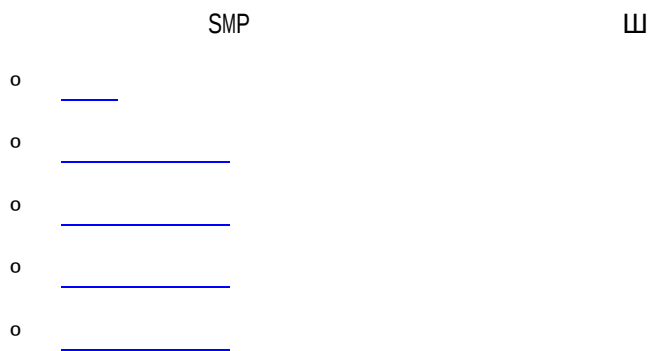


6.2.1		32
6.2.2		33
6.2.3		34
6.2.4		36
6.3		36
6.3.1		36
6.3.2		37
6.3.3		38
7		39
7.1		39
7.2		

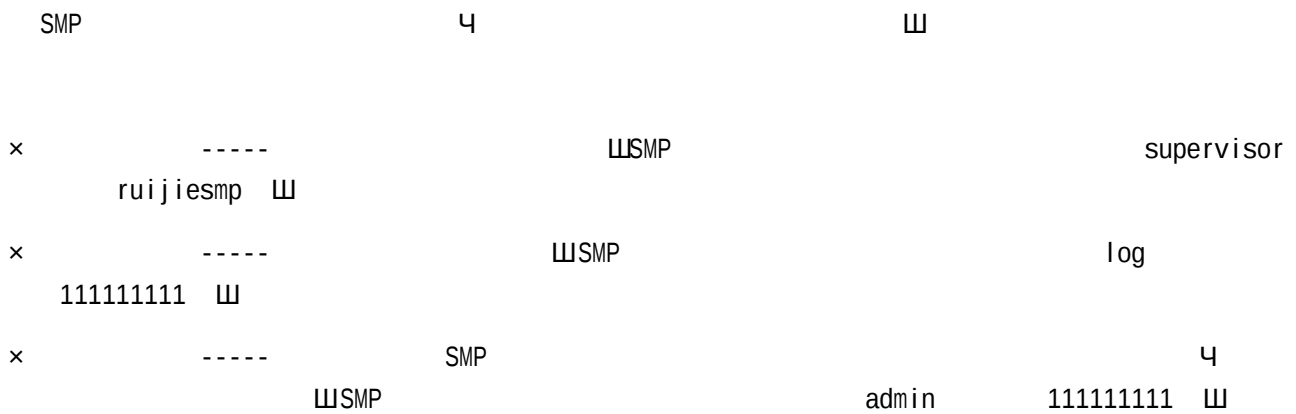
Red-Giant Security Management Platform (SMP)
Ш

Ш
Ш 4 4
Ш

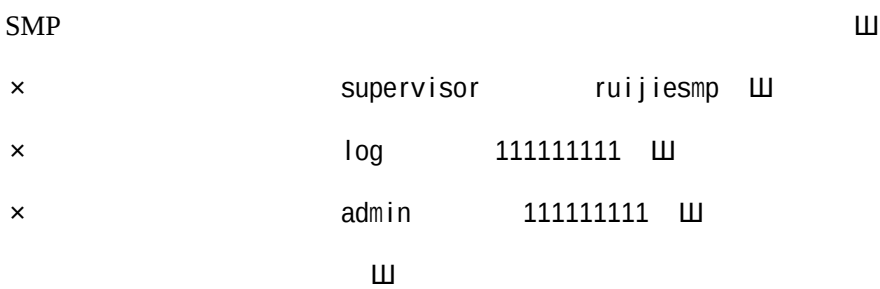
1



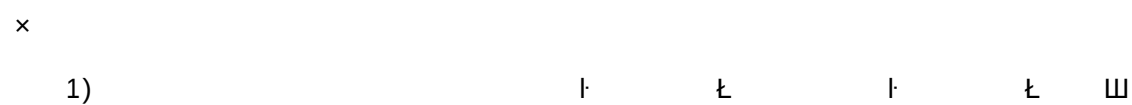
1.1



1.2



1.3



3) 1. 2. 3.

4) 卜 𠂔 𠂔

1.4

I L III

•

•



1.5

4 4 4 3

supervisor $\sqcup$

1.5.1

W

X

1) $\vdash \vdash \vdash \vdash \vdash$



2) | | | | | |

3) 1. 2. 3.

4)

p

1.5.3

o 9 20

o supervisor

x

1) 1 2 3 4 5

位置:系统用户管理 > 修改系统用户

* 用户名: admin ?

* 所属用户组: 系统管理员

密码: ?

密码确认:

真实姓名: 系统管理员

Email地址:

电话号码:

修改

重置

返回

2) 1 2 3 4 5

3) 1 2 3 4 5

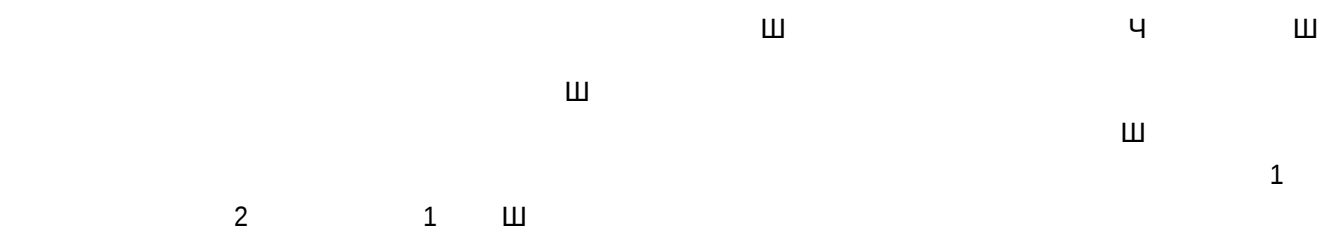
4) 1 2 3 4 5

5) 1 2 3 4 5

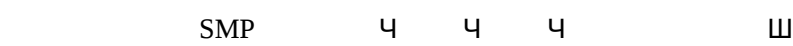
2



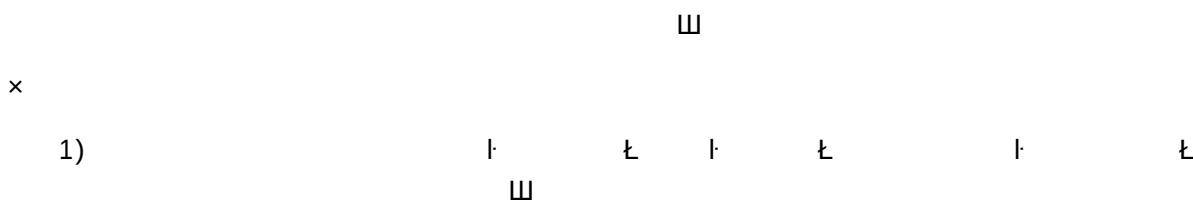
2.1



2.2



2.2.1



位置:用户管理 > 用户组 > 查询用户组

用户组名称:

用户组描述:

安全策略模板:

查询

重置

添加

删除所选

共2条记录 每页20条 第1页/共1页 GO

[首页] [上一页] [下一页] [尾页]

☐	用户组名称 ↑	用户组描述	安全策略模板 ↑	操作
☐	第一用户组		default	修改
☐	新建用户组		default	修改

2.2.3

×

1) 上 下 上 下 上 下 上 下 上

用户组 > 修改用户组

第一用户组

default

用户组名称:

安全策略模板:

用户组描述:

查看 如果用户所在的系统或设备绑定了安全策略模板，那么这里绑定的安全策略模板将

修改 重置 返回

- 2) 上 下 上
- 3) 上 下 上 下 上 下 上 下
- 4) 上 下 上
- 5) 上 下 上 下 上 下 上

2.3

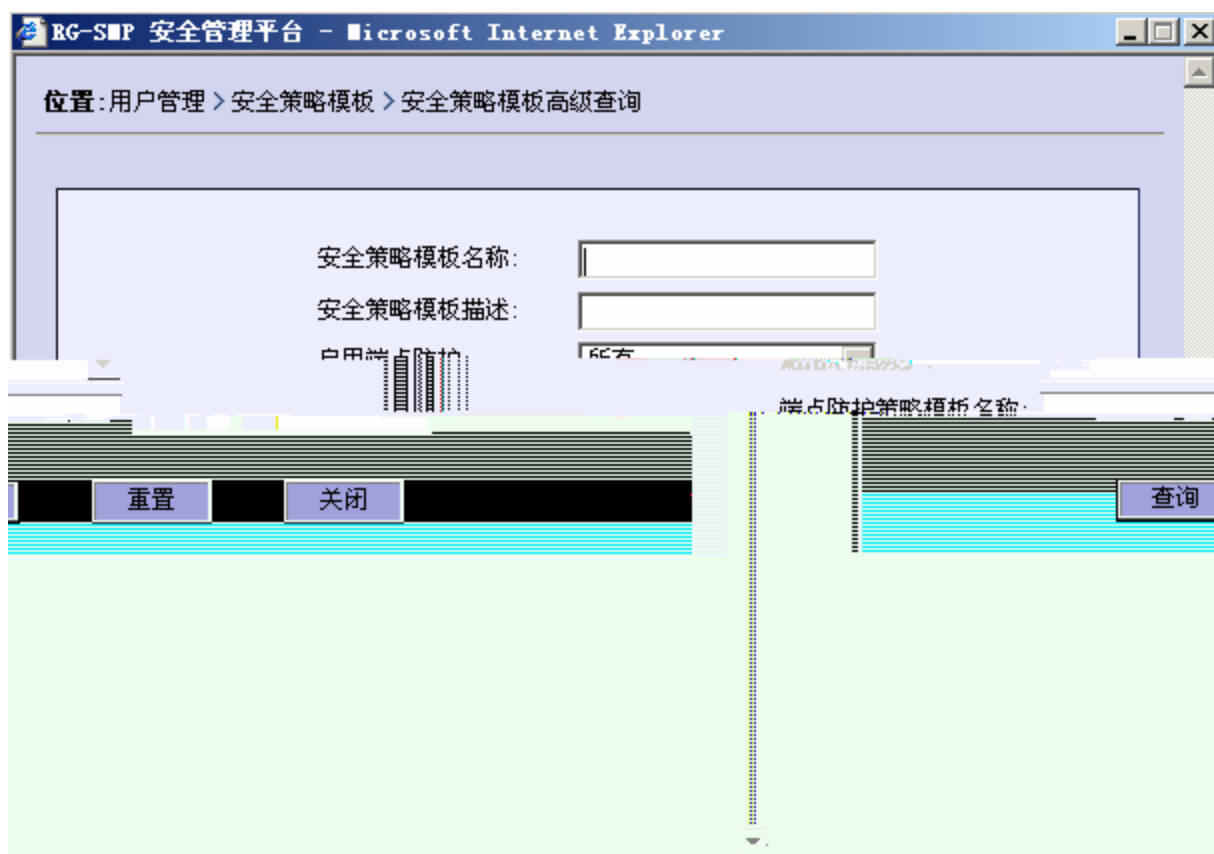
SMP 4 4 4 4 上

2.3.1

×

1) 上 下 上 下 上 下 上 下 上

上



5)

p l t l l l l l l l

p l t l l l l l l l

p l t l l l l l l l

W

W

٤ ١١

2.3.2

W

W

III

III

1.

W

W

III

×

W

位置:用户管理 > 安全策略模板 > 添加安全策略模板

端点防护

--

* 安全策略模板具体信息请查看各标签卡项

返回

注意：重置功能将重置所有选项卡中的信息。

W



↑ ↓ ↑ ↓ ↑ ↓

↑ ↓ ↑

↑ ↓ ↑ ↓ ↑

Â]<1*+9 õ S

"¼ ä Ö

z ↑

z ↑ ↓

z ↑ ↓ ↑ ↓

z ↑

—

↑ ↓ ↑ ↓ ↑ ↓

↑ ↓

基本信息 端点防护

* 安全策略模板名称: default

安全策略模板描述: 默认安全策略模板!

* 安全策略模板具体信息请查看各标签卡项

修改

重置

返回

注意: 重置功能将重置所有选项卡中的信息。

2) 卜 乚 山

3) 卜 乚 卜 乚 卜 乚

4) 卜 乚 山

5) 卜 乚 “ ”

端点防护策略模板基本信息

杀毒软件联动

微软补丁更新

☐ 启用微软补丁更新

更新服务器设置

更新服务器类型: 不指定更新服务器

锐捷客户端更新

☒ 启用锐捷客户端更新

必须安装的补丁类型:

☐ 全部类型

☒ Service Pack

☐ 更新程序集

☐ 全部级别

☒ 紧急

☒ 安全更新程序

☐ 更新程序

☒ 重要

☒ 定义更新

☐ 工具

☒ 中

☒ 关键更新程序

☐ 驱动程序

☐ 低

☐ Feature Pack

☐ 其它

必须安装的补丁安全级别:

更新周期: 16 小时 (默认16小时)

WUA下载地址:

WUA (Windows更新代理)是微软提供的用于检查计算机上可用更新的组件。

☐ 更新过程采取安全措施

如果采取安全措施, 用户在完成补丁更新之前, 将按照端点防护处理方式进行处理 (如下警告消息、绑定端点防护模板等)。

微软客户端更新控制

☐ 启用微软客户端自动更新

☒ 禁用微软客户端自动更新

允许自动更新立即安装: 启用

配置自动更新: 自动下载并计划安装

计划安装日期: 每一天

计划安装时间: 10:00

添加

重置

返回

- o 山
- o 山
- o (4)山
- o WUA(Windows) WUA
- o 山
- o Windows 山
- o

Service Pack	Hotfix 4 4 山Service Pack 山



	Ш
--	---

Ш



3.3

SMP 4 4 4 4 山

3.3.1

×

1) 卜 乚 卜 乚 卜 乚 山

位置: 端点防护 > 杀毒软件联动 > 查询杀毒软件

杀毒软件名称:

联动方式:

所有类型

查询

重置

是否启用:

所有类型

添加

删除所选

[首页] [上一页] [下一页] [尾页]

共24条记录 每页20条 第1页/共2页 GO

检查限制	启用	操作
	☐	查看 修改
顺延天数	7	☐ 查看 修改

☐	杀毒软件名称	联动方式	检查项	
☐	江民2008及其以后的版本	强联动	杀毒引擎 不检查	
			病毒库 不检查	
☐	江民杀毒软件KV2007	弱联动	杀毒引擎 不检查	
			病毒库 检查	自适应
☐	卡巴斯基互联网安全套装8.0个人版	弱联动	杀毒引擎 不支持	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	卡巴斯基反病毒7.0个人版	弱联动	杀毒引擎 不支持	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	卡巴斯基反病毒7.0网络安全版	弱联动	杀毒引擎 不支持	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	Symantec AntiVirus企业版 8	弱联动	杀毒引擎 不检查	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	Symantec AntiVirus企业版 9	弱联动	杀毒引擎 不检查	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	Symantec AntiVirus企业版 10	弱联动	杀毒引擎 不检查	查看 修改
			病毒库 检查	自适应顺延天数 7 ☐ 查看 修改
☐	安博士杀毒软件 V3 VirusBlock2005	弱联动	杀毒引擎 检查	查看 修改
			病毒库 不支持	自适应顺延天数 7 ☐ 查看 修改
☐	McAfee VirusScan V10.0	弱联动	杀毒引擎 不检查	查看 修改
			病毒库 不检查	☐ 查看 修改
☐	McAfee VirusScan Enterprise 8.5.0i	弱联动	杀毒引擎 不检查	查看 修改
			病毒库 不检查	☐ 查看 修改

2) 卜 乚 卜 乚 山

3) 卜 乚 卜 乚 山

4) 山

5) p 卜 乚 卜 乚 山 卜

p 卜 乚 山

山

p 卜 乚 山

位置: 端点防护 > 杀毒软件联动 > 修改杀毒软件

基本信息

- * 杀毒软件名称: 江民2008及其以后的版本
- ☐ 检查杀毒引擎版本
- ☒ 检查病毒库版本
- * 版本检查方式: 自适应
- * 病毒库自适应顺延天数: 7

注意: 请输入病毒库自适应顺延天数, 它用来限制用户的病毒库最长可以不更新的天数

病毒扫描

- ☐ 认证后立即执行内存扫描
- ☐ 启用全盘扫描

杀毒软件监视

- ☐ 全部监视
- ☐ 文件监视 ☐ 网页监视 ☐ 邮件监视
- ☐ 脚本监视 ☐ 即时通信监视

处理方式

- * 杀毒软件不合格时提示信息: 请升级江民杀毒软件
- 杀毒引擎及病毒库升级: 杀毒软件自动升级

修改

重置

返回

2)

位置: 端点防护 > 杀毒软件联动 > 修改杀毒软件

基本信息

- * 杀毒软件名称: 江民杀毒软件KV2007
- ☐ 检查杀毒引擎版本
- ☒ 检查病毒库版本
- * 版本检查方式: 自适应
- * 病毒库自适应顺延天数: 7

注意: 请输入病毒库自适应顺延天数, 它用来限制用户的病毒库最长可以不更新的天数

处理方式

- * 杀毒软件不合格时提示信息: 江民杀毒软件KV2007
- 验证地址
- * 升级服务器URL:

修改

重置

返回

3)

:

基本信息

* 杀毒软件名称:

冰点

* 进程名称:

ice.exe

注意: 杀毒软件名称必须与该杀毒软件在“添加删除程序”显示的名称一致, 否则客户端无法识别该杀毒软件是否已安装。

验证方式:

* 杀毒软件安装程序URL:

http://ice.com

验证地址

修改

重置

返回

- 4) 卜 乚 山
- 5) 卜 乚 卜 乚 卜 乚 山
- 6) 卜 乚 山
- 7) 卜 乚 卜 乚 山

SMP

山

o

o

ARP

4.1

山

ARP

山

ARP

山

ARP

山

4.2ARP

ARP

山

山

ARP

山

ARP

山

×

1)

山

ARP

山

ARP

山

位置: 网络攻击防护 > ARP欺骗免疫 > 配置ARP欺骗免疫

☒ 启用ARP欺骗免疫功能

[] [尾页] 共4条记录 每页 20 条 第 1 页/共1页 GO [首页] [上一页] [下一页]

操作	网关IP	网关MAC	网关名称	网关类型	应用模式	启用ARP欺骗免疫	支持静态模式
查看	192.168.203.150	00D0F82233AD	S3250	S3250-48	网关	☐	☐
查看	192.168.203.2	00D0F8A65AF7	4F_HJ_5750	S5750S-24GT/12SFP	网关	☒	☐
查看	192.168.203.3	00D0F822A219	4F_HJ_5760	S5760-24GT/4SFP	网关	☒	☐
	192.168.203.90	00D0F8BC9556	SMP	S2126G	网关	☐	☐

返回到设备列表

返回到设备列表

2)

山

3)

ARP

山

4)

ARP

山

5)

ARP

山

5

- o _____
- o _____
- o _____
- o _____

5.1

ACL

Ш

×

Ш

Ш



- 3) 卜 𠂇 卜 𠂇 𠂇
- 4)

5.3.2

- | | | | | |
|---|-------|----|----|----|
| 0 | 1 * 2 | 32 | 16 | 33 |
| 0 | 4 | 33 | | |

×

1) 1 2 1 2 1 2 3

配置 - 网络访问控制 / 访问控制模板 / 添加新访问控制模板...

访问控制模板名称：

访问控制模板描述：

目的IP：

子网掩码：

目的MAC：

目的端口：

协议选择：

不选择

添加

重置

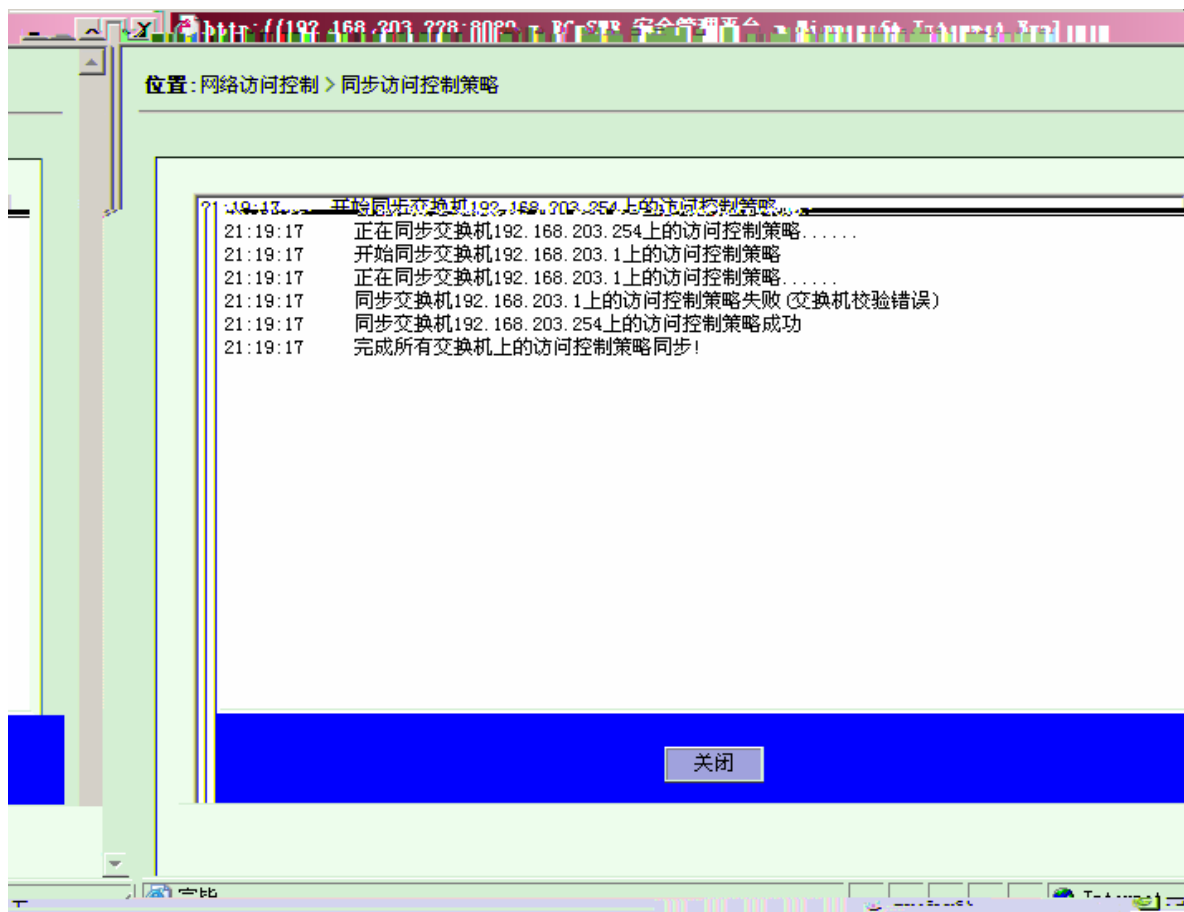
返回

- 2) 1 2 3
- 3) 1 2 3 4 5
- 6
- 4) 1 2 3
- 5) 1 2 3 4 5

5.3.3

[illegible][illegible]

5.4



位置: 设备管理 > 交换机 > 查询交换机

交换机ID

交换机名称

新增交换机

新增策略

查询

添加

高级查询

新增交换机

新增配置模板

添加

批量添加

删除所选

同步访问控制策略

1/1页/共1页 GO [首页] [上一页] [下一页] [尾页]

共3条记录 每页20条 第1

交换机MAC	交换机类型	交换机配置模板	操作
00D0F8A65AF7	其它类型	网关配置模板	查看 修改 相关策略
00D0F8BF9EB4	S2150G	zy1-21-SW	查看 修改 相关策略
00D0F8BC9558	S2126G	接入配置模板	查看 修改 相关策略

交换机IP
192.168.203.1
192.168.203.254
192.168.203.90

2) 卜 乚 山 卜 乚

3) 卜 乚 卜 乚 山

4) 卜 乚 卜 乚 山 卜 乚

5) 山 山

ARP 山

p 卜 乚 卜 乚 卜 乚 山

p 卜 乚 卜 乚 卜 乚

×

1) 上 上 上 上 上 上 上

式: 否 未选择

* 交换机IP: * 是否VRRP部署模: * 交换机配置模板

* 交换机名称: 未选择

交换机位置: 备注:

- 如果交换机IP是VRRP部署模式下的虚拟IP, 请配置为VRRP部署模式, 这时候获取交换机信息时, 才能获取到正确的虚拟MAC。若获取虚拟MAC失败, 表示交换机软件不支持这种获取方式, 这时请手动输入交换机MAC信息。
- 交换机上的用户将优先应用交换机配置模板绑定的安全策略模板。 □ 右当交换机配置模板未绑定安全策略模板时, 将应用设备默认的安全策略模板。

交换机信息 添加 重置 返回 获取

2) 上 上 IP 上 上

3) 上 上 上 上

4) 上 上 上

5) 上 上 上 上 上

6.2.3

上 * 上 上

×

1) 上 上 上 上 上 上 上

位置: 设备管理 > 交换机 > 批量添加交换机

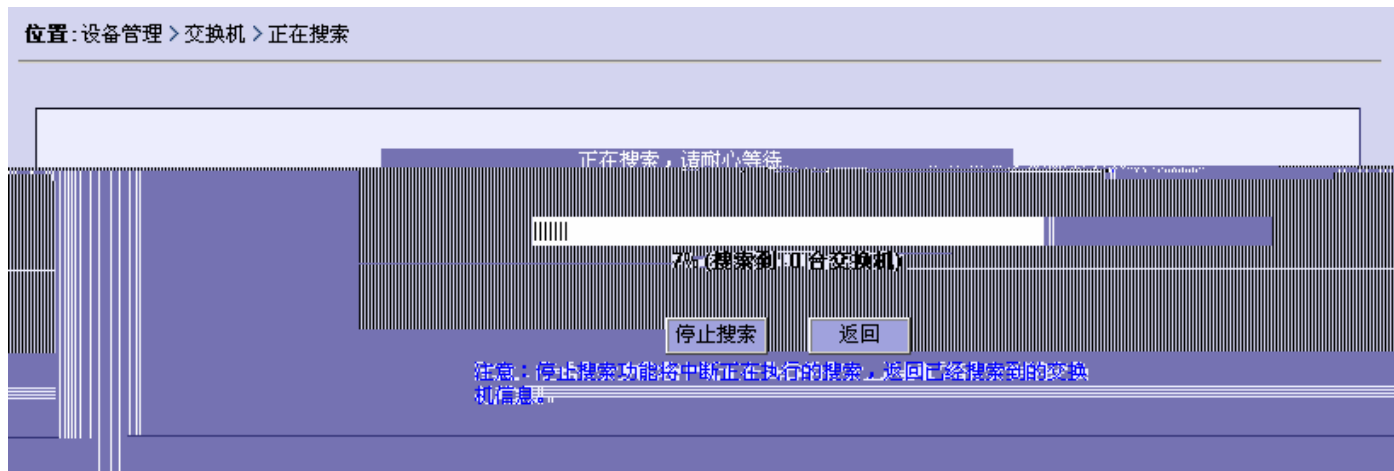
* 开始IP: * 结束IP: * 交换机配置模板: 未选择

开始搜索 重置 返回

2) “ ” 上

3) 卜 乚 卜 乚 山

4) 卜 乚 卜 乚
SMP

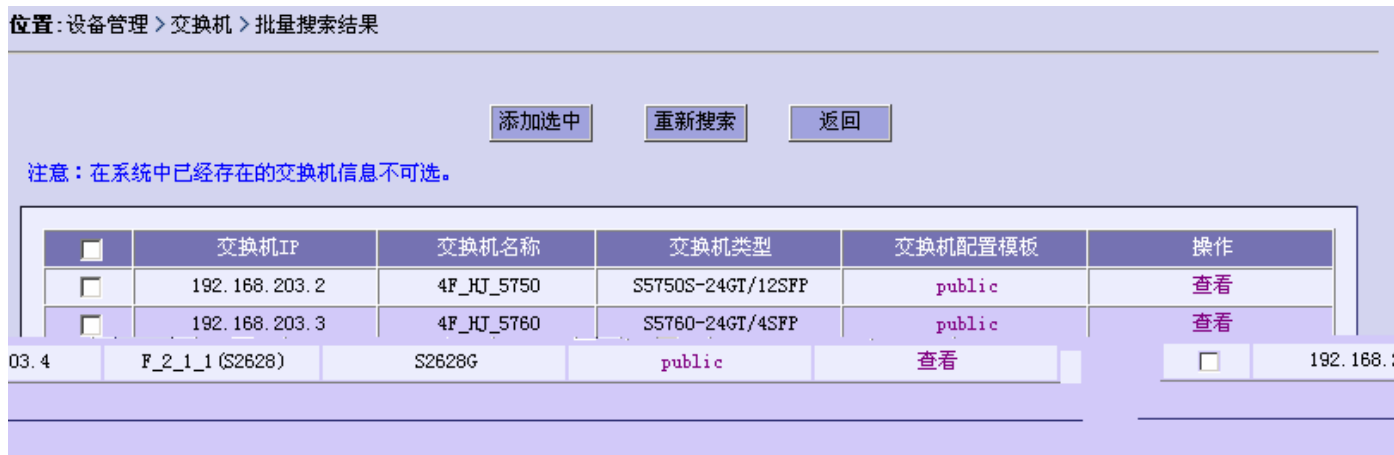


5) 山

6) 卜 乚 卜 乚 山

7) 卜 乚 卜 乚 山

8) 100 卜 乚 卜 乚



9) 卜 乚 卜 乚

10) 卜 乚 卜 乚 山

11) 卜 乚 卜 乚 山

12) 卜 乚 山

13) 卜 乚 山

6.2.4

- [illegible]

x

- 1) 1 2 1 2 3

交换机IP: 192.168.203.158		
是否VRRP部署模式: 是		
交换机名称: xxx_jieru		* 交换机名称:
虚拟机MAC: 001AA9102BCA		* 虚拟机MAC:
交换机类型: S3750		交换机名称:
交换机位置: S3750-48		交换机类型:
备注: Ruijie Gigabit Routing S		交换机位置:
		备注:

下的虚拟IP，请配置为VRRP部署模式，这时候获取交换机信息时，才能获取到
 未取，表示交换机软件不支持这种获取方式，这时请手动输入交换机MAC信息。

交换机配置模板绑定的安全策略模板，只有当交换机配置模板未绑定安全策略模
 板的安全策略模板。

- 2) $\begin{array}{ccccc} & & \vdash & \vdash & \\ & \sqcup & & & \vdash & \vdash & \\ & & & & & & \vdash & \vdash & \end{array}$
- 3) $\begin{array}{ccccc} & \vdash & \vdash & & \sqcup & \\ & & & & & & & & \end{array}$
- 4) $\begin{array}{ccccc} & \vdash & \vdash & \vdash & \vdash & \sqcup & \\ & & & & & & & & \end{array}$

6.3

- У У У Ш

6.3.1

x

- [illegible]

È x

[illegible]

4) | | | | |

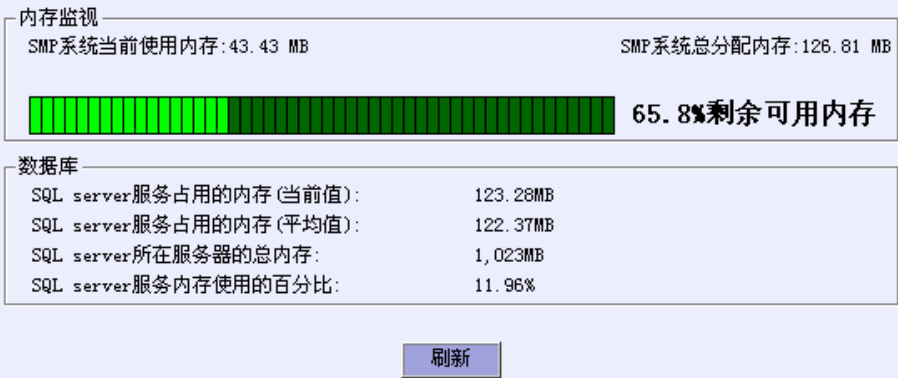
1. * 1

[illegible]

注意：如果这里绑定了安全策略模板，相关交换机上的用户将应用这里配置的安全策略模板。而用户所在用户组绑定的安全策略模板将失效。

4) |· ¤ |· ¤ ≡

SMP



2) 卜 亡 山

7.4

SMP 山

×

1)

位置: 系统自诊断 > 设备配置诊断 > 查看诊断结果

交换机IP	192.168.203.1
交换机配置模板	网关配置模板
交换机应用模式	网关
交换机软件版本	未知
在线用户数	0
使用策略数	0
上次操作失败动作	下发超时时长配置报文
上次操作失败时间	2008-01-19 03:52:05
可能原因:	● 交换机不存在或IP配置错误 ○ 交换机与交换机间存在配置冲突 ○ 交换机配置与模板不匹配

关闭

٤

位置: 系统自诊断 > 设备配置诊断 > 建议连接用户数和安装策略数

注意: 对于桌面类型的交换机, 建议端口到桌面, 即每个端口下一个用户。以下表格针对的是支持GSN方案的交换机, 其它类型的交换机不支持安装策略, 最多用户数建议请参考相应的交换机文档。

交换机类型	最多用户数建议 (非桌面接入模式)	最多策略数建议
S2126G	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (224) 条; 每个千兆口 (110) 条;
S2150G	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (224) 条; 每个千兆口 (110) 条;
S21-STACKING	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (224) 条; 每个千兆口 (110) 条;
S3750-24	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3750-48	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3750E-24	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3750E-48	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3750-24 (UB)	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3750-48 (UB)	每八个百兆口 (80) 个; 每个千兆口 (40) 个;	每八个百兆口 (250) 条; 每个千兆口 (122) 条;
S3760-48T4SFP	每个千兆口 (1000) 条; 每台交换机 (1000) 条;	每个千兆口 (1000) 条; 每台交换机 (1000) 条;
S3760-12SFP	每个千兆口 (1000) 条; 每台交换机 (1000) 条;	每个千兆口 (1000) 条; 每台交换机 (1000) 条;
S3760-24	每个千兆口 (1000) 条; 每台交换机 (1000) 条;	每个千兆口 (1000) 条; 每台交换机 (1000) 条;
S3760-48x2	每个千兆口 (1000) 条; 每台交换机 (1000) 条;	每个千兆口 (1000) 条; 每台交换机 (1000) 条;

关闭

7.5

1)

↑

↑

↑

↑

↑

↑

↓

位置: 系统自诊断 > 活动设备检测 > 查询活动设备检测

☒ 自动删除一周前记录

共1条记录, 每页20条, 第1页/共1页 [首页] [上一面] [下一面] [尾页]

操作	交换机IP ↑	发送报文数 ↑	最后发送报文时间 ↑
添加交换机	192.168.200.51	1	2025-09-09 01:00:00

2)

↑

↑

↓

↓

3)

↑ Telnet

telnet

↓

4)

↑

↑

↑

↑

↑

↑

↓

↓

↓

↓

↓

↑

↑

↑

↓

5)

↑

↑

8

SMP

o

o

8.1

Ш SMP

Ч

Ш

SMP

Ч

Ч

Ш

8.2

http://192.168.203.168:8080 - RG-SMP 安全管理平台 - Microsoft Internet Explorer

位置: 在线用户 > 查询在线用户 > 高级查询

用户名:

用户组:

用户IP:

用户MAC:

交换机IP:

交换机端口:

上线时间(开始):

上线时间(结束):

在线时长(从): 小时 分 秒

在线时长(至): 小时 分 秒

完毕 Internet

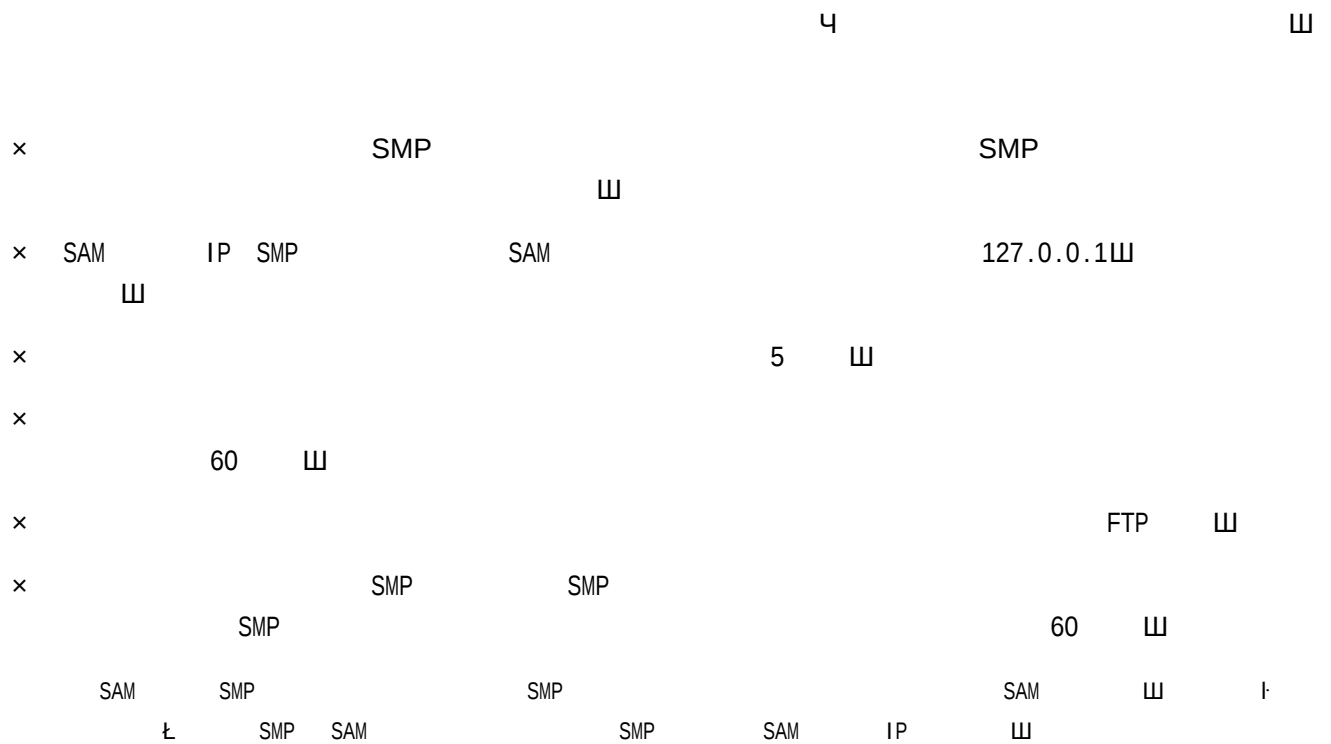
5)

p l t W
 o W
 o SMP W
 o SMP W
 p l t W
 W
 p W
 p l t l t W

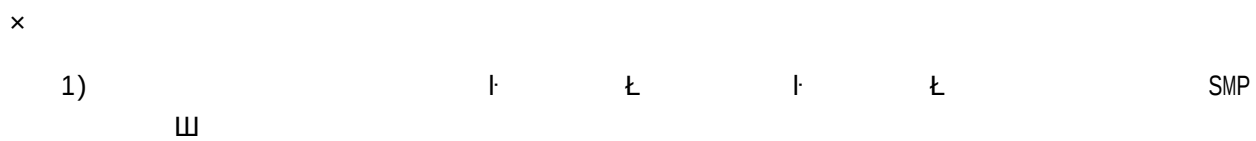
9



9.1



9.2



位置: 系统配置

接入用户控制

账号分隔, 如"192.168.1.2"正常。

分钟 (默认为60分钟)

定期检测用户在线状态

* SAM服务器IP:

192.168.203.60

注意: 可以配置多个SAM服务器 (IP地址不能使用VLB群集地址, 必须使用SAM的本地IP地址)。IP之间使用逗号分隔, 如"192.168.2.23"。配置成功后, 您可通过"系统自诊断>系统服务诊断"来查看SMP同SAM服务器的联动是否正常。

端点防护

* 状态检测周期:

1分钟 (默认为5分钟)

* 配置文件更新周期:

5分钟 (默认为60分钟)

* 配置文件更新服务器:

ftp://smp:smp@192.168.203.32:21

其他功能

* 访问控制策略同步周期:

60

修改

重置

- 2) 卜 乚 卜 乚 卜 乚 山
- 3) 卜 乚 卜 乚 山

系统信息

用户管理

端点防护

网络攻击防治

网络访问控制

设备管理

位置: 日志管理 > 查询日志信息

日志类型: 所有类型

日志内容:

日志的创建时间 (开始):

日志的创建时间 (结束):

查询

重置

共1545条记录 每页50条 第1页/共31页 GO

系统日志

2008-07-30 14:03:36

system

admin(127.0.0.1)登录成功!

系统日志

2008-07-30 14:03:28

system

log(127.0.0.1)成功退出系统!

系统日志

2008-07-30 13:58:07

system

log(127.0.0.1)登录成功!

系统日志

2008-07-30 13:58:02

system

admin(127.0.0.1)成功退出系统!

系统日志

2008-07-30 13:58:34

system

admin(127.0.0.1)登录成功!

系统日志

2008-07-30 13:58:21

system

RG-SMP系统启动成功!

系统日志

2008-07-30 13:58:20

system

启动定时删除一周前活动设备检测任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时检查用户状态任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时检查数据库占用内存任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时更新交换机信息任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时清除可信ARP任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时检查TrapReceive线程任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时检查安全策略配置文件更新任务成功!

系统日志

2008-07-30 13:58:20

system

启动定时删除日志任务成功!

2) 卜 乚 卜 乚

山

3) 卜 乚 卜 乚 山

4) 山

10.2.2

山

×

1) 卜 乚 卜 乚 山

系统信息

日志管理

位置: 日志管理 > 查询日志信息

日志类型: 所有类型

日志的创建时间 (开始):

日志的创建时间 (结束):

查询

重置

删除所选

删除本次查询所有记录

配置日志参数

共85条记录 每页 条 第1 页/共5页 GO

[首页] [上一页] [下一页] [尾页]

	日志类型 ↑	创建时间 ↑	创建管理员 ↑	日志内容
☐	操作日志	2008-08-04 17:00:31	log	删除本次查询所有日志信息成功!
☐	操作日志	2008-08-04 17:00:22	log	删除本次查询所有日志信息成功!
☐	系统日志	2008-08-04 16:59:47	system	log(192.168.203.54)登录成功!
☐	系统日志	2008-08-04 16:59:42	system	admin(192.168.203.54)成功退出系统!

系统日志

2008-08-04 16:39:39

system

admin(192.168.203.34)登录成功!

system	admin(192.168.203.54)登录成功!
system	admin(192.168.203.54)成功退出系统!
system	admin(192.168.203.34)登录成功!
system	admin(192.168.203.22)登录成功!
system	admin(192.168.203.34)登录成功!
system	用户(tx:192.168.203.34)端点防护检测成功!

☐	系统日志	2008-08-04 16:11:59
☐	系统日志	2008-08-04 16:11:50
☐	系统日志	2008-08-04 15:55:42
☐	系统日志	2008-08-04 15:52:10
☐	系统日志	2008-08-04 14:29:43
☐	端点防护日志	2008-08-04 13:46:02

2) 卜 乚 卜 乚 卜 乚

乚 山

3) 卜 乚 卜 乚 山

4)

p 卜 乚 山

p 卜 乚 山

p 卜 乚 卜 乚 卜 乚 山

p 山

10.2.3

山

×

1) 卜 乚 卜 乚 卜 乚 山

49 53

位置: 日志管理 > 配置日志参数

日志参数配置

☐ 自动删除 (1~100)*

天以前的端点防护日志

☐ 自动删除 (1~100)*

天以前的操作日志

☐ 自动删除 (1~100)*

天以前的系统日志

☐ 自动删除 (1~100)*

天以前的客户端信息日志

修改

重置

返回

2) 1 2 1 2

 2 3

3) 1 2 3

4) 1 2 1 2 3

11 FAQ



SMP supervisor http://127.0.0.1:8080/smp/index.jsp : ruijiesmp



SMP IP



SMP HTTP HTTPS SMP /

服务器配置

服务器配置项

服务器安装路径: D:\RG-SMP

HTTP 协议 ☒ 设置HTTP 端口: 8080

HTTPS协议 ☒ 设置HTTPS端口: 8443

JVM内存分配池初始容量 (MB): 256

JVM内存分配池最大容量 (MB): 512

JVM PermSize初始容量 (MB): 128

JVM PermSize最大容量 (MB): 128

数 据 连 接 池 初 始 容 量 (个): 5

数 据 连 接 池 最 大 容 量 (个): 50

☒ 操作系统启动时自动启动

取消 确定



web

/ HTTP HTTPS

Ш

WEB

Ш



І Ł

session

SMP

IE
IE

І

Ł

І

Ł

Ш

SMP

Ш



І

Ł

SMP

Ч

Ч

Ш

`	~	!	@	#	\$	%	^	&	*
(	)			[	]	{	}		
_	-	=	+	,	.				
;	:	“	”	‘	’	<	>		
ŀ	Ł	І	Ł	...	‰	Ч	Ш		

Э

!

