

# מבוא

.



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		

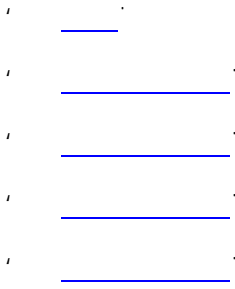
FYX! ; ] Ubh' GYWf] hmi AUbU[ YaYbh' D' UhZcfa GADL

ž

ž

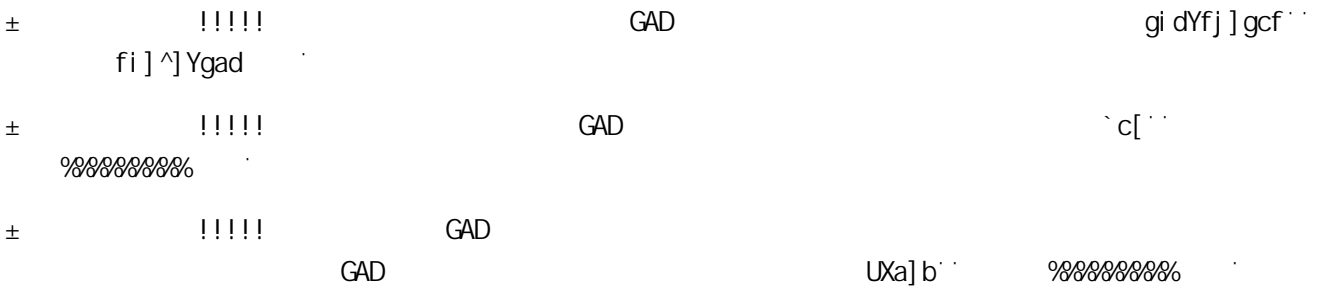
%

GAD



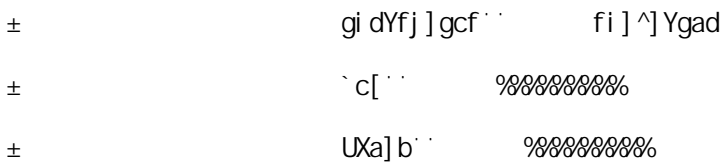
%'

GAD



%&

SMP



%'

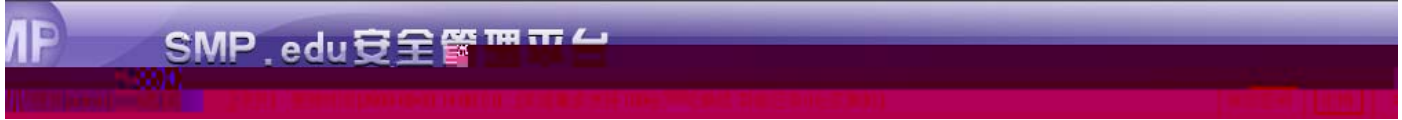
±

%&



&L

't  
(t  
%(



%)

supervisor

%) "%

±  
%



&t  
't  
(t

Ø

%)'''

- &\$

gi dYfj ]gcf

±

%

位置:系统用户管理 > 修改系统用户

* 用户名:	<input type="text" value="admin"/>	?
* 所属用户组:	<input type="text" value="系统管理员"/>	▼
密码:	<input type="text"/>	?
密码确认:	<input type="text"/>	
真实姓名:	<input type="text" value="系统管理员"/>	
Email地址:	<input type="text"/>	
电话号码:	<input type="text"/>	

修改

重置

返回

&t

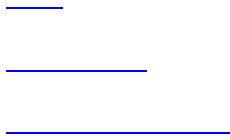
't

(t

)t

&

GAD



&" %

%

& %

&" &

SMP

&" &" %

±

%

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:

共2条记录 每页20条 第1页/共1页 GO

[\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

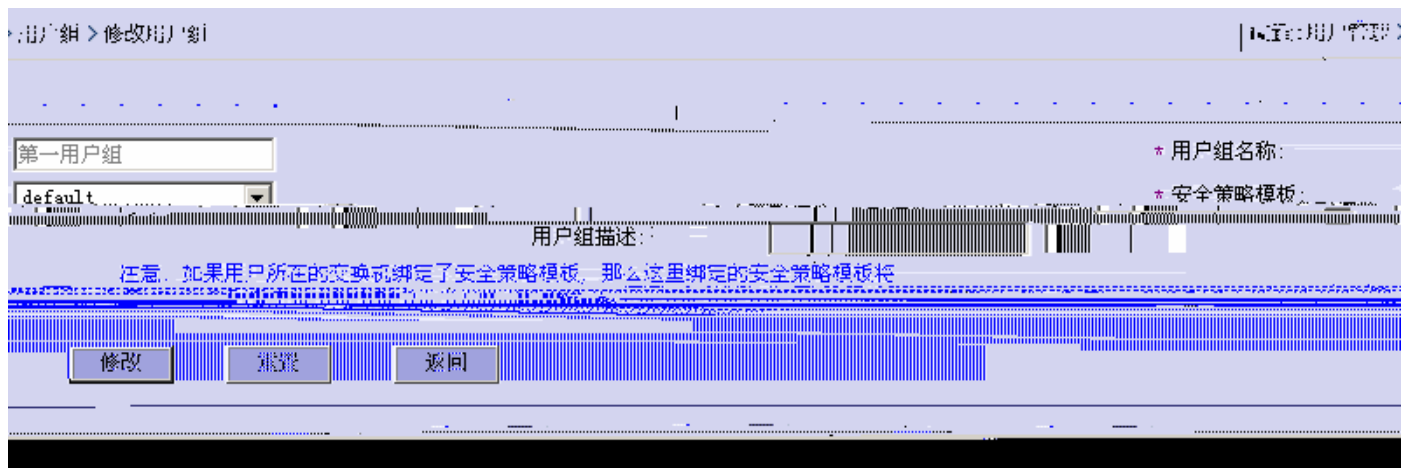
<input type="checkbox"/>	用户组名称 ↑	用户组描述	安全策略模板 ↑	操作
<input type="checkbox"/>	第一用户组		default	<a href="#">修改</a>
<input type="checkbox"/>	新建用户组		default	<a href="#">修改</a>



&"&"'

±

%&



&&

'&

(&

)&

&"'

SMP

&" "%

±

%&

位置: 用户管理 > 安全策略模板 > 查询安全策略模板

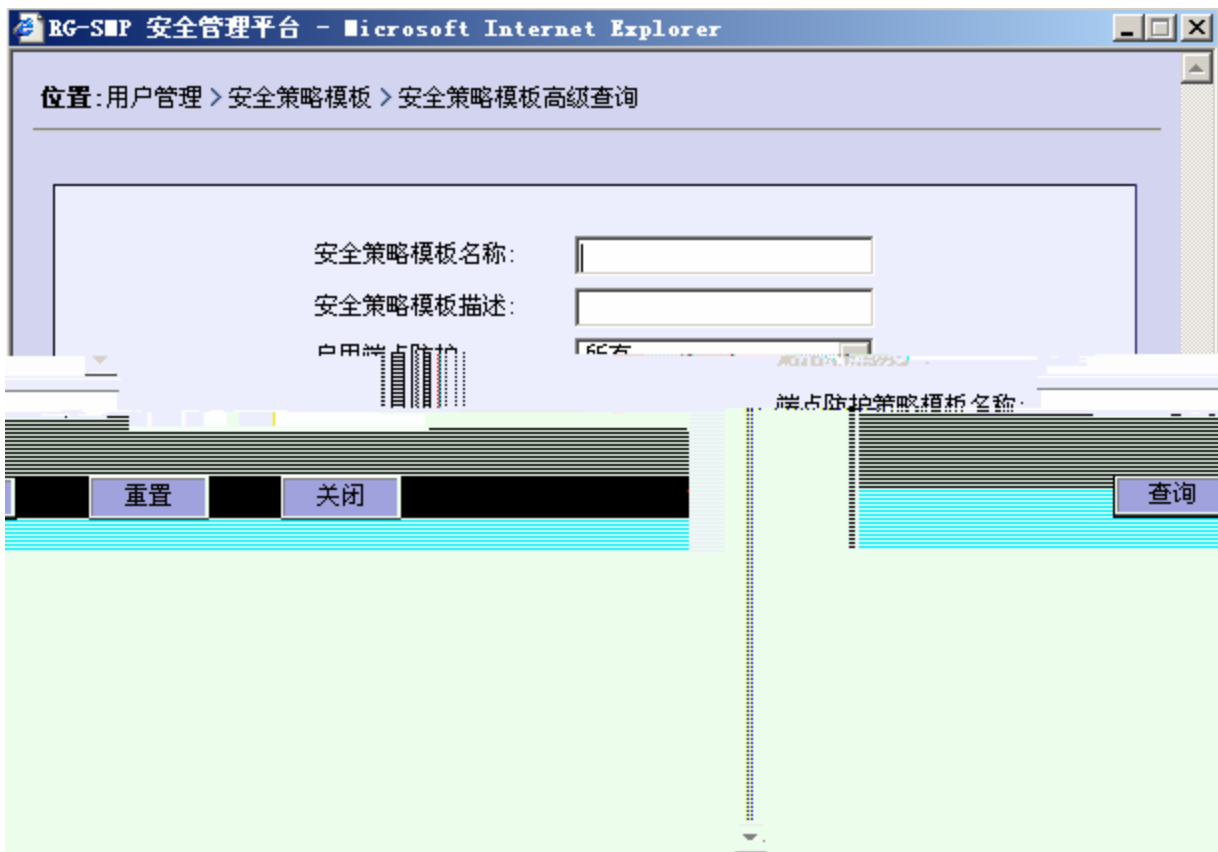
安全策略模板名称:  安全策略模板描述:    [高级查询](#)

操作	安全策略模板名称	安全策略模板描述
使用该安全策略模板! <a href="#">查看</a> <a href="#">修改</a>	default	默认安全策略模板, 新学习到的用户组将默认

&L

'L

(L



)L

Ø

Ø

Ø

∅

∅

&"' "&

' t

' &

%\*

±

%

位置: 用户管理 > 安全策略模板 > 添加安全策略模板

基本信息

端点防护

\* 安全策略模板名称:

安全策略模板描述:

\* 安全策略模板具体信息请查看各标签卡项

添加

重置

返回

注意: 重置功能将重置所有选项卡中的信息。

&t

启用端点防护  
端点防护策略模板: 未选择

成功提示信息:

模板名称:   
描述:

注意: 如果没有任何端点防护策略模板信息, 请先到“端点防护”中添加!

<input type="checkbox"/>	模板名称	描述
<input type="checkbox"/>	端点防护模板	

清空  模板名称  描述

<input type="checkbox"/>	模板名称	描述
<input type="checkbox"/>	端点防护模板	

功能: 重置

Â j<1\*+9 õ S

"¼ ä Ö

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。

&#

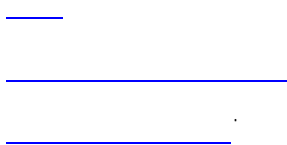
't

(t

)t

“ ”

GAD



' "%

±

2008

±

' "&

SMP

' "&"%

±

%

查询

重置

端点防护策略模板名称:

用户组:

是否启用微软补丁更新:


除所选


添加

册

[首页] [上一页] [下一页] [尾页]

共1条记录 每页20条 第1页/共1页 GO

是否启用微软补丁更新 	操作
否	<a href="#">修改</a>

<input type="checkbox"/>	端点防护策略模板名称 	描述
<input type="checkbox"/>	端点_A	

&t

't

(t

Ø

Ø

Ø

Ø

' "&"&

' t

' &

%

±

1)



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
- 安全更新程序
- 定义更新
- 关键更新程序
- Feature Pack
- 更新程序集
- 更新程序
- 工具
- 驱动程序

必须安装的补丁安全级别:

- 全部级别
- 紧急
- 重要
- 中
- 低
- 其它

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, 用户在未完成补丁更新之前, 将按照端点防护处理方式进行处理 (如下发警告消息、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:

配置自动更新:

计划安装日期:

计划安装时间: 10:00

WUA(Windows )

WUA

Windows

Gyfj ] W' DUW	<chZ] l Gyfj ] W' DUW



--	--



SMP

''''%

±

%&

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:

查询

重置

是否启用:

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	杀毒软件名称	联动方式	检查项		
	<input type="checkbox"/>	查看 修改	江民2008及其以后的版本	强联动	杀毒引擎	不检查	
	<input type="checkbox"/>	查看 修改	江民杀毒软件KV2007	弱联动	病毒库	不检查	
顺延天数	7	查看 修改			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6.0个人版	弱联动	杀毒引擎	不支持	查看 修改
			卡巴斯基反病毒7.0个人版	弱联动	病毒库	检查	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
			Symantec AntiVirus企业版 8	弱联动	病毒库	检查	查看 修改
			Symantec AntiVirus企业版 9	弱联动	杀毒引擎	不检查	查看 修改
			Symantec AntiVirus企业版 10	弱联动	病毒库	检查	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
			McAfee VirusScan V10.0	弱联动	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

&&

'七

(七

)七

Ø

Ø

Ø

Ø

''''&



+

%&

\* (

#

±

%&

位置: 端点防护 > 杀毒软件联动 > 添加杀毒软件

基本信息

\* 杀毒软件名称:

\* 进程名称:

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。

处理方式

\* 杀毒软件名称:



SAVETHE

\*

添加

重置

返回

&&

' 匕

( 匕

) 匕

''''''

±

%&

**基本信息**

\* 杀毒软件名称:

检查杀毒引擎版本

检查病毒库版本

\* 版本检查方式:

\* 病毒库自适应顺延天数:

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:

杀毒引擎及病毒库升级:

&

**基本信息**

\* 杀毒软件名称:

检查杀毒引擎版本

检查病毒库版本

\* 版本检查方式:

\* 病毒库自适应顺延天数:

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:

     \* 升级服务器URL:

'七

基本信息

\* 杀毒软件名称:

\* 进程名称:

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。

网址方式:

\* 杀毒软件安装程序URL:

验证地址

修改

重置

返回

(七

)七

\*七

七

(

GAD

5FD

("%

5FD

5FD

5FD

(" &5FD

5FD

5FD

5FD

±

%

5FD

5FD

位置: 网络攻击防范 > 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
<a href="#">查看</a>	192.168.203.150	00D0F82233AD	S3250	S3250-48	网关	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">查看</a>	192.168.203.2	00D0F8A65AF7	4F_HJ_5750	S5750S-24GT/12 SFP	网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<a href="#">查看</a>	192.168.203.3	00D0F822A219	4F_HJ_5760	S5760-24GT/4SFP	网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	192.168.203.90	00D0F8BC9556	SMP	S2126G	网关	<input type="checkbox"/>	<input type="checkbox"/> <a href="#">查看</a>

返回网络攻击防范系统配置页面

返回配置系统IP地址和子网掩码配置页面

&

'

5FD

5FD

(

5FD

5FD

)

5FD

)

' \_\_\_\_\_  
' \_\_\_\_\_  
' \_\_\_\_\_  
' \_\_\_\_\_

)"%

57@

±

't

(t

∅

∅

)""&

+

'&

%

±

%

管理 - 网络访问控制 / 访问控制模板 / 添加或上除访问模板...

访问控制模板名称:	<input type="text"/>	*
访问控制模板描述:	<input type="text"/>	*
目的IP:	<input type="text"/>	*
子网掩码:	<input type="text" value="255.255.255.255"/>	*
目的MAC:	<input type="text"/>	*
目的端口:	<input type="text"/>	*
协议选择:	<input type="text" value="不选择"/>	

&

'七

(七

)七

)"'"

±

%&

位置: 网络访问控制 > 访问控制模板 > 修改端点防护模板

* 访问控制模板名称:	端点防护模板
访问控制模板描述:	
* 目的IP:	192.168.203.50
* 子网掩码:	255.255.255.255
目的IP:	

不选择

重置

返回

修改

&#

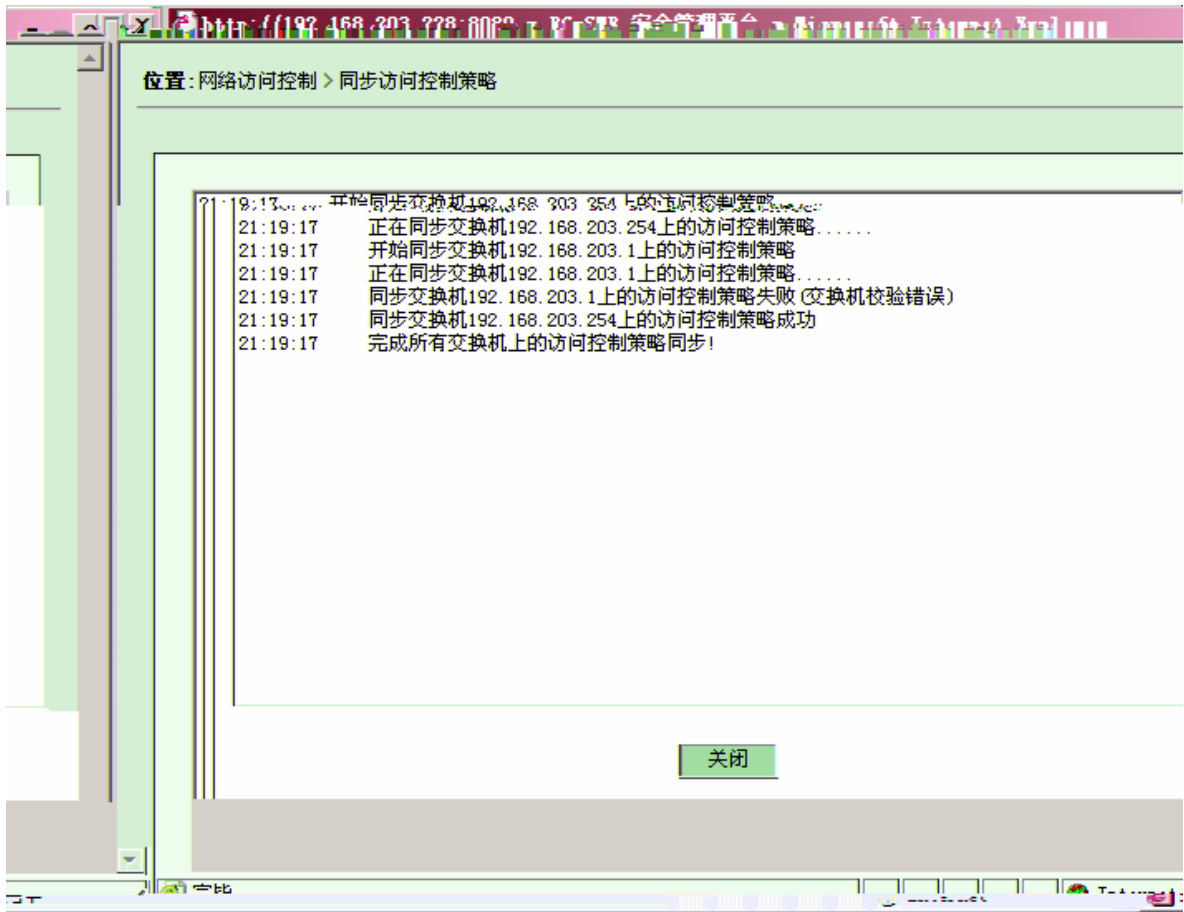
'&#

(&#

)&#

)"("

±





名称: \_\_\_\_\_ 交换机ID: \_\_\_\_\_ 交换机IP: \_\_\_\_\_  
配置模板: \_\_\_\_\_ 交换机类型: \_\_\_\_\_ 查询 高级查询

[添加](#) [批量添加](#) [删除所选](#) [同步访问控制策略](#)

条 第1页/共1页 GO

[首页] [上一页] [下一页] [尾页]

共3条记录 每页20

交换机IP ↑	交换机MAC ↑	交换机类型 ↑	交换机配置模板	操作
168.203.1	00D0F8A65AF7	其它类型	网关配置模板	<a href="#">查看</a> <a href="#">修改</a> <a href="#">相关策略</a>
58.203.254	00D0F8BF9EB4	S2150G	zy1-21-SW	<a href="#">查看</a> <a href="#">修改</a> <a href="#">相关策略</a>
68.203.90	00D0F8BC9556	S2126G	接入配置模板	<a href="#">查看</a> <a href="#">修改</a> <a href="#">相关策略</a>

<input type="checkbox"/>	交换
<input type="checkbox"/>	192.
<input type="checkbox"/>	192.1
<input type="checkbox"/>	192.1

&t

't

(t

)t

∅

5FD

∅

∅

±

%

式:

\* 交换机IP:

\* 是否VRRP部署模:

\* 交换机配置模板:

\* 交换机名称:

交换机类型:

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.
- 交换机上的用户优先级应用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去绑定安全策略模板.

&

=D

't

(t

)t

\*"&"

±

%

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:

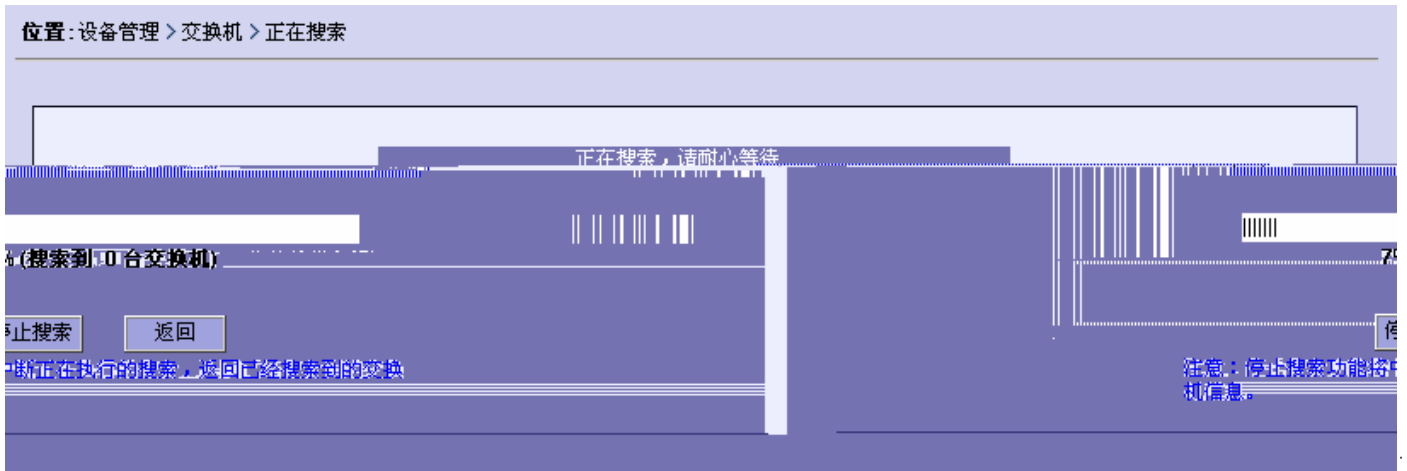
&

“ ”

'七

(七

SMP



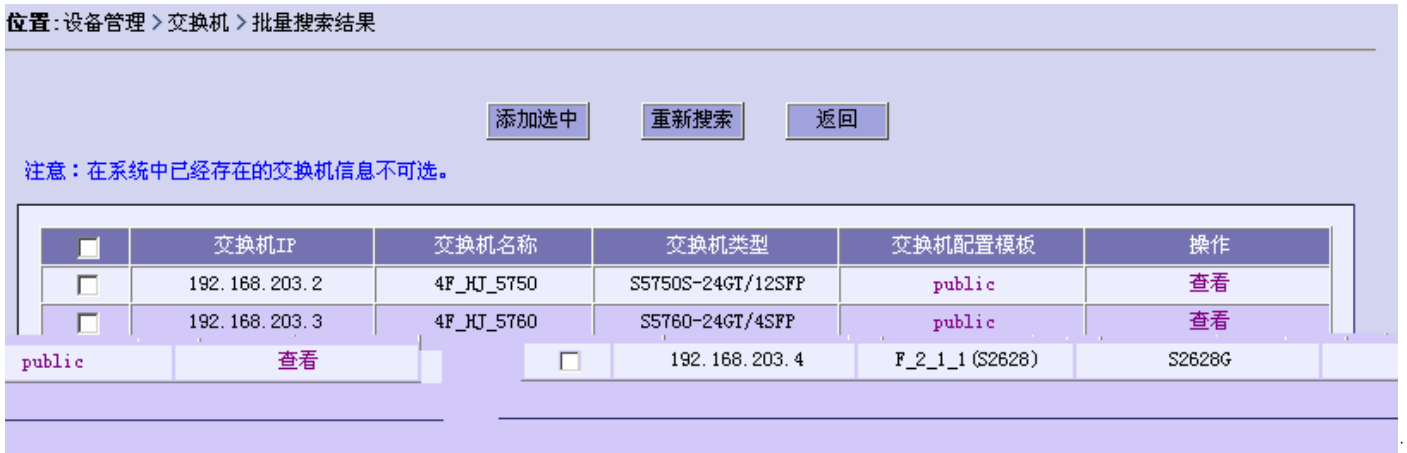
)七

\*七

七

,七

%\$\$



-七

%比

%&

%&

%七

\*"&"(

=D

5FD

±

%

设备管理 > 交换机 > 修改交换机

交换机IP:  \*

是否VRRP部署模式:  \*

虚拟IP:  \*

虚拟MAC:  \*

交换机名称:

交换机类型:

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  
 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  
 定的安全策略模板。

- 如果交换机IP是VRRP部署模式正确的虚拟MAC, 若获取虚拟MAC:
- 交换机上的用户将优先应用交板, 才会应用用户所在用户组绑

&t

't

(t

\*''

\*'' "%

±

%

È x

\* 交换机配置模板名称:

\* 应用模式:

\* 接入模式:

\* SNMP协议版本:  ?

\* 安全公共名:  ?

安全策略模板:

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。

添加

重置

返回

&

'

4)

\* " " "

+

±

%

\* 交换机配置模板名称:

\* 应用模式:

\* 接入模式:

\* SNMP协议版本:  ?

\* 安全公共名:  ?

安全策略模板:

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。

返回

修改

重置

&

'

(

+

GAD

‡

内存监视

SMP系统当前使用内存: 43.43 MB

SMP系统总分配内存: 126.81 MB



65.8% 剩余可用内存

数据库

SQL server服务占用的内存 (当前值):	123.28MB
SQL server服务占用的内存 (平均值):	122.37MB
SQL server所在服务器的总内存:	1,023MB
SQL server服务内存使用的百分比:	11.96%

刷新

&

+ "(

SMP

±

%

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:	<ul style="list-style-type: none"> <li>● 交换机不存在或IP配置错误</li> <li>○ 配置与交换机硬件规格不匹配</li> <li>○ 交换机配置与策略模板不匹配或有配置错误,如版本或安全策略冲突等</li> </ul>

关闭

)七

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	
S21260	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;	
S21900	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-STACK100	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;	
S2750E-24	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;	
S3750-48	每八个百兆口(250)条; 每个千兆口(122)条;	S3750-48	每八个百兆口(250)条; 每个千兆口(122)条;
S3750E-24	每八个百兆口(250)条; 每个千兆口(122)条;	S3750E-24	每八个百兆口(250)条; 每个千兆口(122)条;
S3750E-48	每八个百兆口(250)条; 每个千兆口(122)条;	S3750E-48	每八个百兆口(250)条; 每个千兆口(122)条;
S3750-24 (10B)	每八个百兆口(250)条; 每个千兆口(122)条;	S3750-24 (10B)	每八个百兆口(250)条; 每个千兆口(122)条;
S3750-48 (10B)	每八个百兆口(250)条; 每个千兆口(122)条;	S3750-48 (10B)	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;	S3760-48T4SFP	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;	S3760-12SFP	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;	S3760-24	每个千兆口(1000)条; 每台交换机(1000)条;
S3760-48-2.0	每个千兆口(1000)条; 每台交换机(1000)条;	S3760-48-2.0	每个千兆口(1000)条; 每台交换机(1000)条;

关闭

+")

±

%

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 Go [首面] [上一面] [下一面] [尾面]

操作	交换机IP ↑	发送报文数 ↑	最后发送报文时间 ↑	
添加交换机	192.168.0.54	1	9999-07-01 10:00:00	T 1

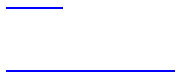
&t

't HY bYh hY bYh

(t

)t

SMP



, "%

GAD

SMP

, "&



)匕

Ø

GAD

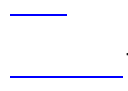
GAD

Ø

Ø

Ø

GAD



- "%

±

SMP

SMP

± G5A

=D GAD

G5A

%&+" \$" \$" %

±

)

±

\*\$

±

: HD

±

GAD

GAD

\*\$

GAD

G5A

GAD

GAD

G5A

GAD

G5A

GAD

G5A

=D

- " &

±

%

GAD

接入用户控制

逗号分隔, 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MLB群集地址, 必须使用SAM的本地IP地址)。IP之间使用  
3, 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

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

&

'

%\$

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

[首页] [上一页] [下一页] [尾页]

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 13:56:34	system	admin(127.0.0.1)登录成功!
系统日志	2008-07-30 13:56:21	system	RG-SMP系统启动成功!
系统日志	2008-07-30 13:56:21	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 13:56:20	system	启动定时检查用户状态任务成功!
系统日志	2008-07-30 13:56:20	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 13:56:20	system	启动定时更新交换机信息任务成功!
系统日志	2008-07-30 13:56:20	system	启动定时清除可信ARP任务成功!
系统日志	2008-07-30 13:56:20	system	启动定时检查TrapReceive线程任务成功!
系统日志	2008-07-30 13:56:20	system	启动定时检查安全策略配置文件更新任务成功!
tem	启动定时删除日志任务成功!		
		系统日志	2008-07-30 13:56:20 sys

&t

't

(t

%\$" &" &

±

%t



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

&t

't

(t

%%: 5E'

GAD \hhd. ##%&+" \$" "\$" % , \$, \$#gad#] bXYI " ^gd'  
gi dYfj ] gcf . fi ] ^] Ygad

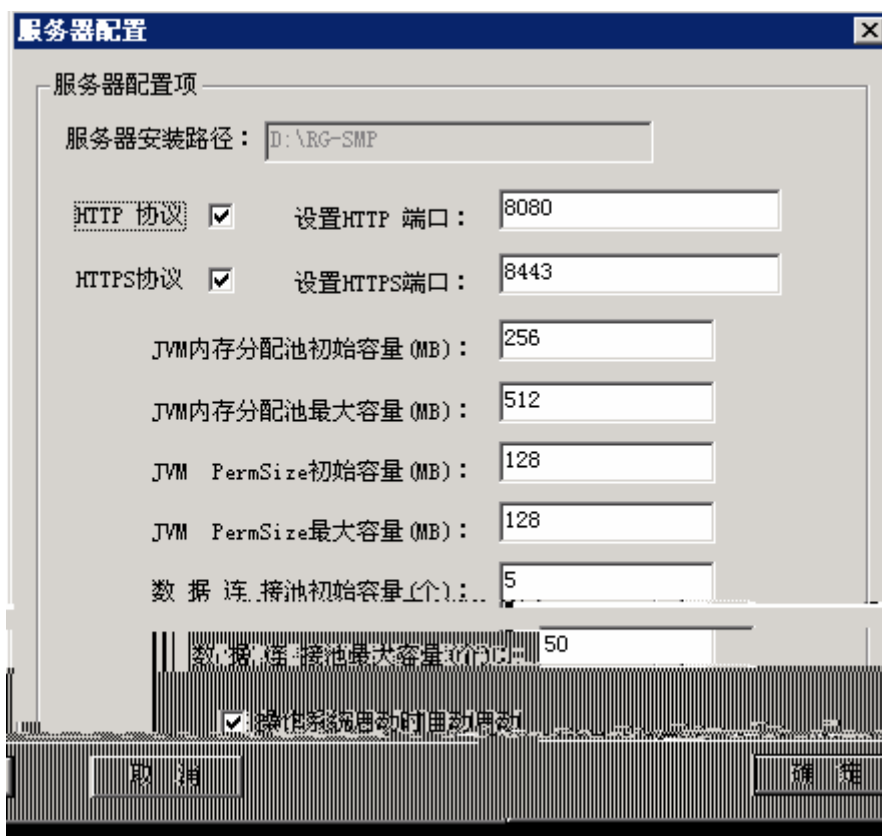
GAD

=D

SMP <HHD <HHDG

GAD #

<HHD <HHDG



kVv

#

<HHD

<HHDG

gYgg] cb

GAD =9  
=9

GAD

GAD

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

