MSS 接入手册

版本: v1.0

日期: 20230801

目录

[第1章 配置IPSEC TUNNEL 3](#_Toc145077231)

[1.1 Tunnel-without NAT 3](#_Toc145077232)

[1.2 通信关系 4](#_Toc145077233)

[第2章 安装Splunk服务 5](#_Toc145077234)

[2.1 安装前准备 5](#_Toc145077235)

[2.2 安装步骤 7](#_Toc145077236)

[2.3 配置syslog-ng 9](#_Toc145077237)

[2.4 定时删除syslog产生的本地文件 11](#_Toc145077238)

[第3章 将数据接收至MSS平台 13](#_Toc145077239)

[3.1 syslog数据接入 13](#_Toc145077240)

[3.1.1 确认日志源 13](#_Toc145077241)

[3.1.2 新增索引 13](#_Toc145077242)

[3.1.3 新增文件监控 15](#_Toc145077243)

[3.2 Win&Linux数据接入 18](#_Toc145077244)

[第4章 客户用户配置 18](#_Toc145077245)

[4.1 新建用户、角色及app 18](#_Toc145077246)

[4.2 创建标准告警 22](#_Toc145077247)

[4.3 创建标准仪表板 22](#_Toc145077248)

# 网络配置

## Tunnel-without NAT

配置IPSEC TUNNEL

|  |  |  |
| --- | --- | --- |
|  | **用户** | **MSS** |
| 设备厂商 |  | Palo Alto |
| NAT-T | enable | enable |
| 公网IP |  | 52.83.157.233 |
| 标识（按需） | 52.83.157.233 |  |
| 兴趣流 |  | 192.168.72.0/23 |
|  |  |
|  |  |
|  |  |
| 本地标识（按需） |  | 52.83.157.233 |
| 预共享密钥 | \*\*\*\*\*\*\*\*\*\*\* | \*\*\*\*\*\*\*\*\*\*\* |
| Phase 1： | |  |
| Authentication Method | Pre-shared Key |  |
| Mode | Main | Main |
| Encryption | 3DES | 3DES |
| Authentication | MD5 | MD5 |
| DH Group | group2 | group2 |
| Lifetime | 86400 | 86400 |
|  |  |  |
| Phase 2： | |  |
| 隧道模式 | ESP | ESP |
| Encryption | 3DES | 3DES |
| Authentication | MD5 | MD5 |
| PFS DH Group | GROUP2 | GROUP2 |
| Lifetime | 28800 | 28800 |
| DPD间隔 | 30S | 30S |
| DPD超时时间 | 300S | 300S |

## 通信关系

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **源IP/组件** | **域名/IP** | **目标组件** | **域名/IP** | **端口** |
| Data forwarder | N/A | Indexers | 192.168.72.82/192.168.72.69 | 8089  9997 |
| Data forwarder | N/A | Mgmt | 192.168.72.100 | 8089 |
| MSS Jumper | 192.168.72.16 | Data forwarder | N/A | 8000 |
| Data forwarder | N/A | MSS Deployment server | 192.168.72.71 | 8089 |
| Data Sources | N/A | ForwardNLB | ForwardNLB-bb56931a38dc2089.elb.cn-northwest-1.amazonaws.com.cn | 515 |

# 安装Splunk转发器

## 安装前准备

准备一台服务器用于客户各种日志的转发与接收，服务器需要为Linux，kernel版本3.x以上；资源需要至少为8C16G,磁盘300GB。

NOTE：如需要将日志转发至MSS平台，则必须IPSec网络已通!

**远程登录服务器**

使用ssh连接或使用其他登录服务器的app进行登录

**设置主机名**

hostnamectl set-hostname $server\_name$

**开启防火墙指定端口**

systemctl status firewalld #查看防火墙状态

netstats -ntlp #查看端口使用情况(可选)

firewall-cmd --zone=public --add-port=8089/tcp --permanent

firewall-cmd --zone=public --add-port=9997/tcp –permanent

firewall-cmd --zone=public --add-port=8000/tcp –permanent

firewall-cmd --zone=public --add-port=514/udp --permanent

#永久开启端口号为tcp:8089、tcp:9997、tcp:8000、udp:514的三个端口。

**修改ulimit参数**

命令行输入如下代码（重启后失效）：

ulimit -n 1048576

ulimit -u 1048576

ulimit -d 1048576

编辑/etc/security/limits.conf文件：

vi/etc/security/limits.conf

在文件尾部添加如下代码，保存并退出：

\* soft nofile 1048576

\* hard nofile 1048576

\* soft nproc 1048576

\* hard nproc 1048576

下次重启服务器后永久生效。

验证配置是否生效：

ulimit -a

查看输出结果中open files、User processes、Data segment size三项，若显示其值为1048576则表示修改成功。

**关闭THP**

查看当前THP模式：

cat /sys/kernel/mm/transparent\_hugepage/enabled

cat /sys/kernel/mm/transparent\_hugepage/defrag

值是 always 则表示当前THP处于运行状态，命令行输入如下命令关闭THP：

echo never > /sys/kernel/mm/transparent\_hugepage/enabled

echo never > /sys/kernel/mm/transparent\_hugepage/defrag

重启服务器后失效，若要永久关闭THP，可在.service文件中添加如下内容：

编辑service文件：

vi /etc/rc.d/rc.local

复制如下内容，保存并退出：

if test -f /sys/kernel/mm/transparent\_hugepage/enabled; then

echo never > /sys/kernel/mm/transparent\_hugepage/enabled

fi

if test -f /sys/kernel/mm/transparent\_hugepage/defrag; then

echo never > /sys/kernel/mm/transparent\_hugepage/defrag

fi

为其添加可执行权限：

chmod +x /etc/rc.d/rc.local

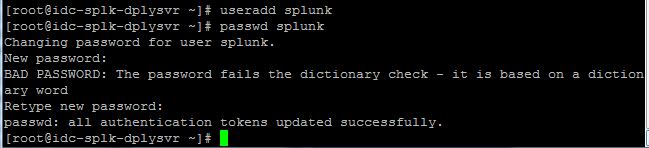
下次重启服务器后可再次查看当前THP模式，值是never则成功永久关闭

cat /sys/kernel/mm/transparent\_hugepage/enabled

cat /sys/kernel/mm/transparent\_hugepage/defrag

**创建splunk管理员用户（非必须）**

useradd splunk #新建用户splunk，由于没有为其分配所属组，所以splunk用户所属组将默认为splunk用户组。



**设置splunk用户的密码(非必须)**

passwd splunk

#设置密码命令，之后输入密码并确认

#splunk用户的密码为:$splunk\_passwd$

## 安装步骤

通过Splunk官方文档下载最新版Splunk Enterprise安装包，以Splunk9.1.0为例：

wget -O splunk-9.1.0.2-b6436b649711-Linux-x86\_64.tgz "https://download.splunk.com/products/splunk/releases/9.1.0.2/linux/splunk-9.1.0.2-b6436b649711-Linux-x86\_64.tgz"

将安装包放置到转发器的/opt目录中，并解压

mv splunk-9.1.0.2-b6436b649711-Linux-x86\_64.tgz /opt #该命令是目的是将splunk安装在/opt目录下

tar zxvf splunk-9.1.0.2-b6436b649711-Linux-x86\_64.tgz #解压安装包，安装splunk

以root用户启动Splunk进程

chown –R root:root splunk #将splunk文件的拥有者改为splunk用户组下的root用户

/opt/splunk/bin/splunk start -accept-license #第一次启动需要输入用户名密码，用户名默认为admin，密码可设置为Password@123

#NOTE:如果客户不允许以root用户启动Splunk进程，则创建一个splunk用户用于运行splunk进程，并将上述代码中”root”更改为“splunk”，并在splunk进程中运行启动命令

查看Splunk进程状态

/opt/splunk/bin/splunk status

开启web-ssl服务并授权

splunk enable web-ssl -auth admin:passwd

开启web-ssl服务，-auth 身份认证，在其后输入splunk进程的用户名及密码

停止splunk进程

/opt/splunk/bin/splunk stop

为splunk用户开启splunk的开机自启动权限

/opt/splunk/bin/splunk enable boot-start –user root

#若以splunk用户启动splunk进程，则需要先进入root用户再运行此命令并将命令中”root”改为”splunk”

将配置文件包上传至服务器：



将该配置包放置到/opt/splunk/etc/apps目录中，并解压。

解压后重启splunk服务

/opt/splunk/bin/splunk start

验证配置是否生效

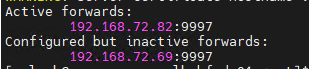
/opt/splunk/bin/splunk show deploy-poll

回显如下：



/opt/splunk/bin/splunk list forward-server

回显如下(两个IP需要至少有一是Active forward):



Splunk配置完成

## 配置syslog-ng

关闭selinux服务

vi /etc/sysconfig/selinux

#在文件中将selinux修改为disable

SELINUX=disable

退出并保存

然后CLI中输入命令setenforce 0使其状态改为permissive

停止并关闭rsyslog 服务

systemctl stop rsyslog #停止rsyslog服务

systemctl disable rsyslog #关闭rsyslog服务

离线安装syslog-ng相关组件

以下四条命令为最小化安装程序组件，需要当前目录下有这几种安装包，若没有，可使用wget命令在网上下载或先下载在本机上并使用sftp等方式传输到服务器。

NOTE：一下rpm包仅针对Enterprise Linux 7版本，即(CentOS 7, RHEL 7, Rocky Linux 7, AlmaLinux 7)，对于其他版本的linux服务器需要下载同名的其他rpm包

rpm -ivh ivykis-0.36.2-2.el7.x86\_64.rpm #安装ivykis组件

rpm -ivh eventlog-0.2.13-4.el7.x86\_64.rpm #安装eventlog组件

rpm -ivh libnet-1.1.6-7.el7.x86\_64.rpm #安装libnet组件

rpm -ivh syslog-ng-3.5.6-3.el7.x86\_64.rpm #安装syslog-ng组件

导入syslog-ng配置

mv r.conf /etc/syslog-ng/conf.d/

#若当前目录下有该文件，则将该文件移动到/etc/syslog-ng/conf.d目录下。

#若没有该文件，则在/etc/syslog-ng/conf.d中使用vi r.conf命令新建并编辑r.conf文件。

具体syslog-ng配置

在r.conf中输入以下配置信息：

########## source add by Ryo-Ohki ##########

source s\_src1 {

udp(ip(0.0.0.0) port(514));

};

source s\_src2 {

tcp(ip(0.0.0.0) port(515));

};

# ########## destination add by Ryo-Ohki ##########

destination d\_dest1 {

file( "/opt /log/${HOST}/${SOURCEIP}/${YEAR}\_${MONTH}\_${DAY}.log" create-dirs(yes) dir-perm(0755) perm(0644) );

};

destination d\_dest2 {

file( "/opt /log/${HOST}/${SOURCEIP}/${YEAR}\_${MONTH}\_${DAY}.log" create-dirs(yes) dir-perm(0755) perm(0644) );

};

# ########## log defined add by Ryo-Ohki ##########

log { source(s\_src1); destination(d\_dest1); };

log { source(s\_src2); destination(d\_dest2); };

启动syslog-ng

systemctl restart syslog-ng

查看syslog-ng状态

systemctl status syslog-ng

测试syslog-ng能否正确的接收日志

logger -d -n $self\_ip$ -P 514 “test message”

运行完成后进入/opt/log/目录，若存在，名为：

/opt/log/$self\_ip$/$self\_ip$/$当前日期$

的文件即表示syslog-ng配置无误。

## 定时删除syslog产生的本地文件

由于syslog存储的文件会随着事件增长越来越多，磁盘空间会出现不足的问题，因此需要定时删除syslog存储在本地的文件以避免此情况的发生。

创建定时删除脚本

cd /opt/

mkdir celogs/

cd celogs/

vi clear\_expired\_logs.sh

在文件中复制如下内容：

#!/bin/bash

##### 可修改变量

LOG\_PATH=/opt/log

R\_TIME=6

#R\_TIME参数值+1表示数据存在本地的时间，(R\_TIME=6表示本地存7天)

##### 以下内容不要修改

SCRIPT\_PATH=$(cd "$(dirname "$0")"; pwd)

FILE\_NAME=`/bin/date +"%Y-%m-%d"`

find $LOG\_PATH -name '\*.log' -mtime +${R\_TIME} -type f >> $SCRIPT\_PATH/${FILE\_NAME}.log

find $LOG\_PATH -name '\*.log' -mtime +${R\_TIME} -type f -exec rm {} \;

为脚本添加可执行权限

chmod +x /opt/log/clear\_expired\_logs.sh

测试脚本无误

运行脚本，查看目录中是否新建对应当前日期的文件

./clear\_expired\_logs.sh

Less /opt/log/$当前日期$.log

该文件中应为配置的会被删除的文件的文件名清单

配置crontab 定时删除任务

crontab -e

添加如下内容

30 23 \* \* \* /bin/sh /opt/celogs/clear\_expired\_logs.sh >/dev/null 2>&1

# 将数据接收至MSS平台

## syslog数据接入

本文档以管理网中的数据源为例，其他网络区域的数据可以根据网络区域修改适当修改操作。

本节中，以某客户长亭WAF的syslog日志接入为例

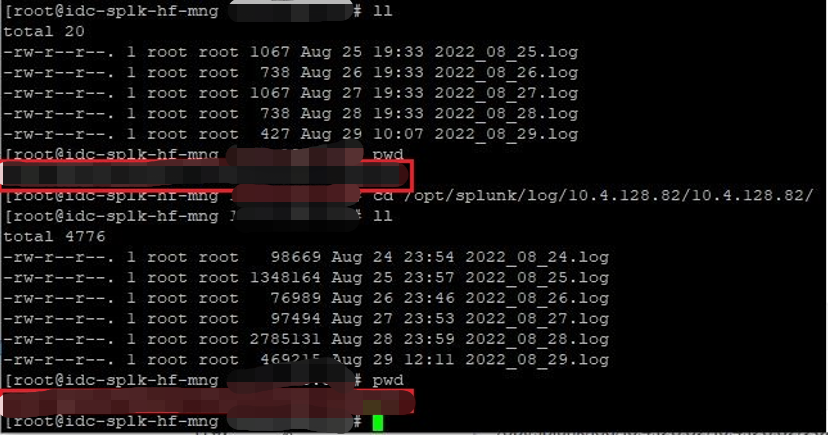
### 确认日志源

1. 登录该syslog数据源所对应区域HF的CLI界面(管理网HF：10.19.1.20)
2. 进入/opt/splunk/log目录下查看该syslog数据源的IP，并在数据源详细列表中根据IP查询其对应的index及sourcetype名称。

例：长亭WAF的syslog日志在HF中的本地目录为：

/opt/log/xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx/及

/opt/log/xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx/



### 新增索引

（若splunk中安装了config explorer，则也可在web界面中直接进行编辑）

1. 进入MSS AWS控制台，新建s3存储桶；

进入链接：<https://cn-north-1.console.amazonaws.cn/s3/buckets?region=cn-northwest-1>

点击创建存储桶

输入存储桶名称,命名规则eccom-mss-s3volume-$客户简称$

其余配置均不做更改，点击创建存储桶

1. SSH进入管理服务器(192.168.72.100)的命令行
2. 进入splunk用户

su splunk

1. 新增index配置项

cd /opt/splunk/etc/master-apps/org\_all\_indexes/local

vi indexes.conf

在文件中断加入：

[volume:eccom-mss-s3volume-$客户简称$]

storageType = remote

path = s3://remotedb

remote.s3.endpoint = https://eccom-mss-s3volume-allbrightlaw.s3.cn-northwest-1.amazonaws.com.cn

remote.s3.access\_key = $7$lWhazfzZiw+bpiMb0gXTbXNTz7d4wXGSm+BHx1l+ezKyEdLnM80zP8sEVpL5dhQxtWM7dw==

remote.s3.secret\_key = $7$5DzH0zK90ldzQApHgotwquH3qpdgwmsOh4kmH025TXXvxFIIWRdIzLiD0sCCnQLgmXDNZwpnyEeUCcmagAESRYlU0uQTg7vA

remote.s3.auth\_region = cn-northwest-1

remote.s3.encryption = sse-s3

在文件末尾添加如下配置项：

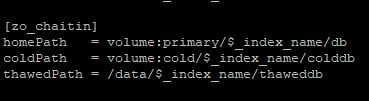
[$该syslog日志对应的index名称$]

homePath = volume:primary/$index名称$/db

coldPath = volume:primary/$index名称$/colddb

thawedPath = $SPLUNK\_DB/$index名称$/thaweddb

remotePath = volume:eccom-mss-s3volume-$客户简称$/$index名称$



1. 验证配置集(此步骤需在splunk用户下进行)

/opt/splunk/bin/splunk validate cluster-bundle --check-restart -auth admin:$passwd$

验证配置集会产成一个编码，此编码为配置集下发编码，仅当此编码与下发配置所产生编码相同时才表示配置下发成功。

1. 下发配置(此步骤需在splunk用户下进行)

/opt/splunk/bin/splunk apply cluster-bundle --answer-yes -auth admin:$passwd$

1. 查看配置下发状态(此步骤需在splunk用户下进行)

/opt/splunk/bin/splunk show cluster-bundle-status -auth admin:$passwd$

查看配置下发状态也可看到验证配置集编码，每台索引节点的编码与验证配置集编码相同，且状态为success即配置下发成功。

1. 在搜索头的web界面中搜索新增的index，若可以搜到数据，则表示配置成功。
2. 轮询重启索引器(可选,若相关数据较长时间后仍无法在搜索头中检索到，则执行此步骤)

/opt/splunk/bin/splunk rolling-restart cluster-peers

### 新增文件监控

（若splunk中安装了config explorer，则也可在web界面中直接进行编辑）

1. SSH登录Deployment Server(192.168.72.71)的CLI界面(若该客户转发器并未连接至DS，则直接登录到客户转发器上进行配置，直接登录至客户转发器时，需将本节中“/opt/splunk/etc/deployment-apps”目录更改为“/opt/splunk/etc/apps”目录)
2. 进入splunk用户

su splunk

1. 在/opt/splunk/etc/deployment-apps中新建对应客户的下发目录

cd /opt/splunk/etc/deployment-apps

mkdir TA\_$客户简称$\_syslog\_inputs

cd /opt/splunk/etc/deployment-apps/TA\_$客户简称$\_syslog\_inputs/local

1. 在inputs.conf文件中新增文件监控

vi inputs.conf

在文件末尾新增如下几行：

[monitor:///opt/log/$syslog日志的主机名$/$日志源IP$]

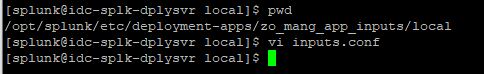
index = $该日志对应的index$

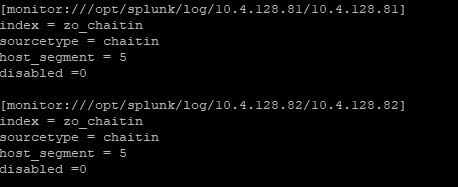
sourcetype = $该日志对应的sourcetype$

host\_segment = 3

disabled = 0

本例中，新增配置项如下：





1. 新建serverclass

*NOTE：如果不是通过DS管理客户转发器而是直接登录客户转发器进行配置，则略过5、6、7三步。*

进入DS的web界面，点击设置🡪转发器管理🡪服务器类，新建一个服务器类，为其添加客户端(即该客户转发器)，随后保存并退出

NOTE:不要在此处直接添加刚刚新建的APP！

1. 下发app

点击应用，找到新建的app，点击编辑，勾选“重新启动splunk”，随后将其加入刚刚新建的服务器类中。

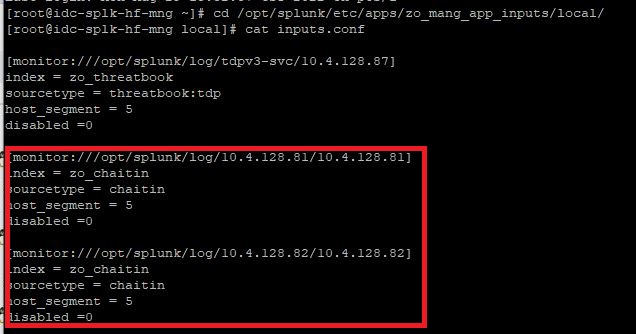


1. 验证配置新增成功(可选)

SSH进入管理网HF，查看下发的配置。

/opt/splunk/bin/splunk list monitor

在该文件中可以看到新增的monitor配置项即表示配置成功。



## Win&Linux数据接入

操作前提：该服务器的agent以完成安装(安装步骤详见agent安装手册)

进入该客户HF的web界面，查看该服务器是否被正确注册到客户HF

进入设置🡪转发器管理🡪客户端，查看列表中是否有该服务器的IP，若没有，需检查agent安装情况；若有，则正常。

新建用于Win/Linux的add-on下发的serverclass，并编辑下发。

在客户端一栏中，新增该服务器的IP(可选)。

重新装载该serverclass

命令行输入如下代码：

/opt/splunk/bin/splunk reload deploy-server -class mang\_HF\_addon

在搜索头中验证数据输入

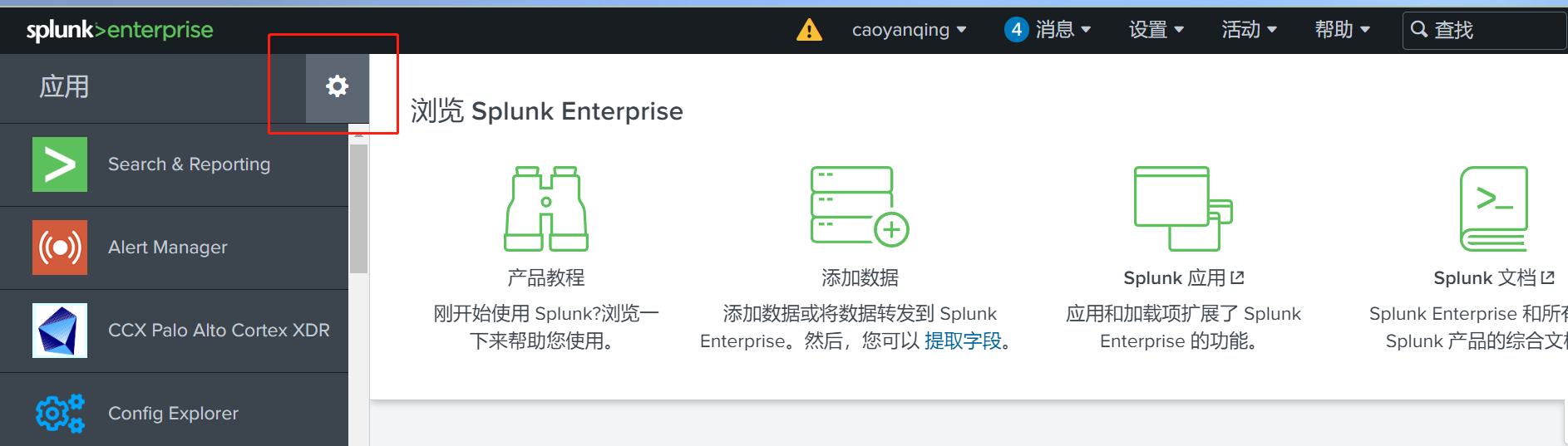
搜索index = $index\_name$,查看出现结果的host字段，若含有该服务器的主机名，则表示数据输入成功。

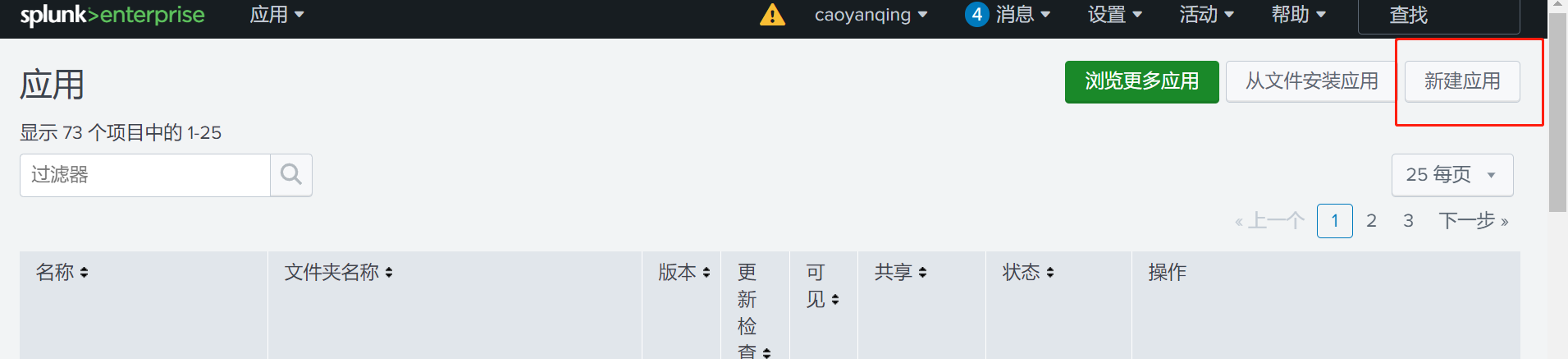
# 客户用户配置

## 新建用户、角色及app

新建app

进入MSS搜索头，点击管理应用🡪新建应用

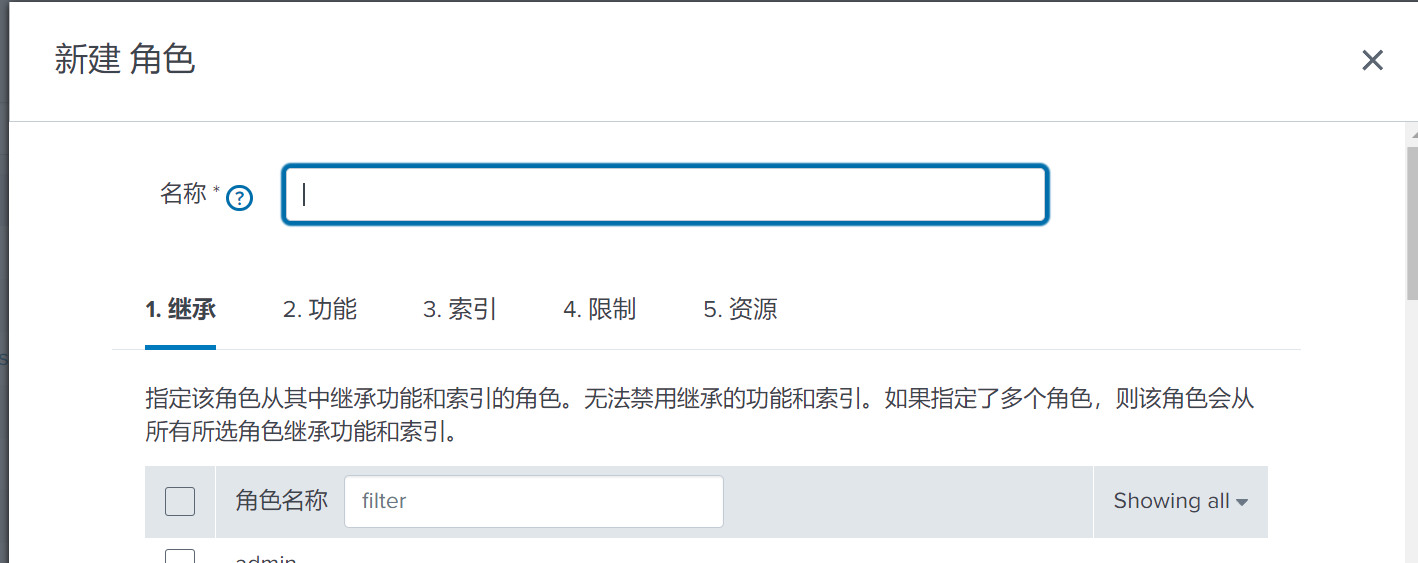




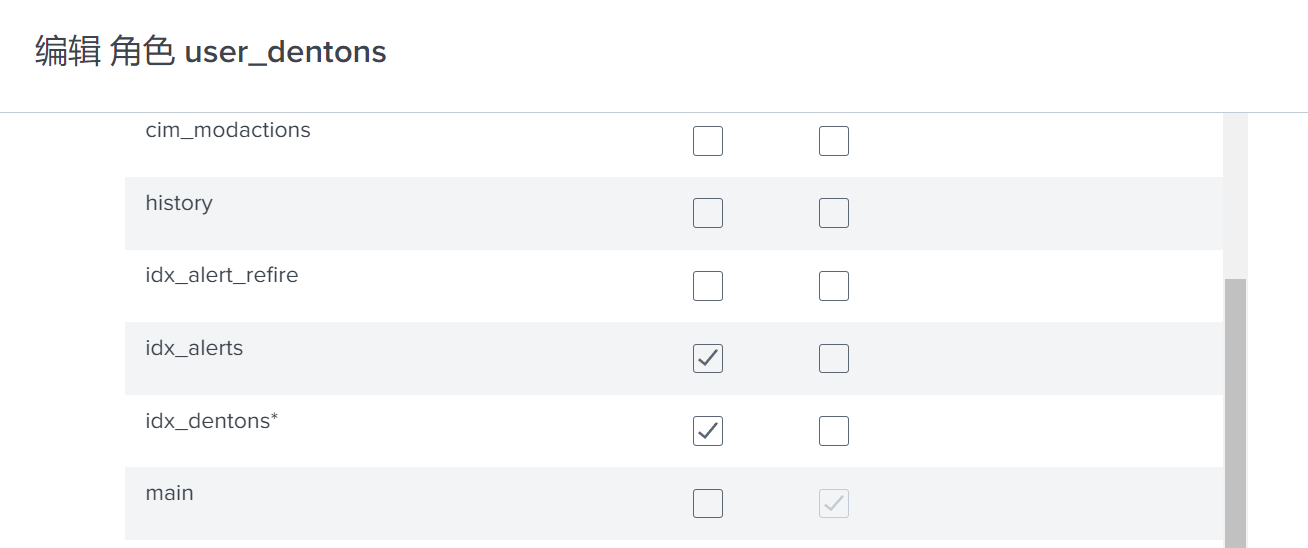
输入应用名称即应用文件夹名称。命名规则：应用名称：MSS App for $客户简称$；应用文件夹名称：splunk\_app\_for\_$客户简称$

新建角色

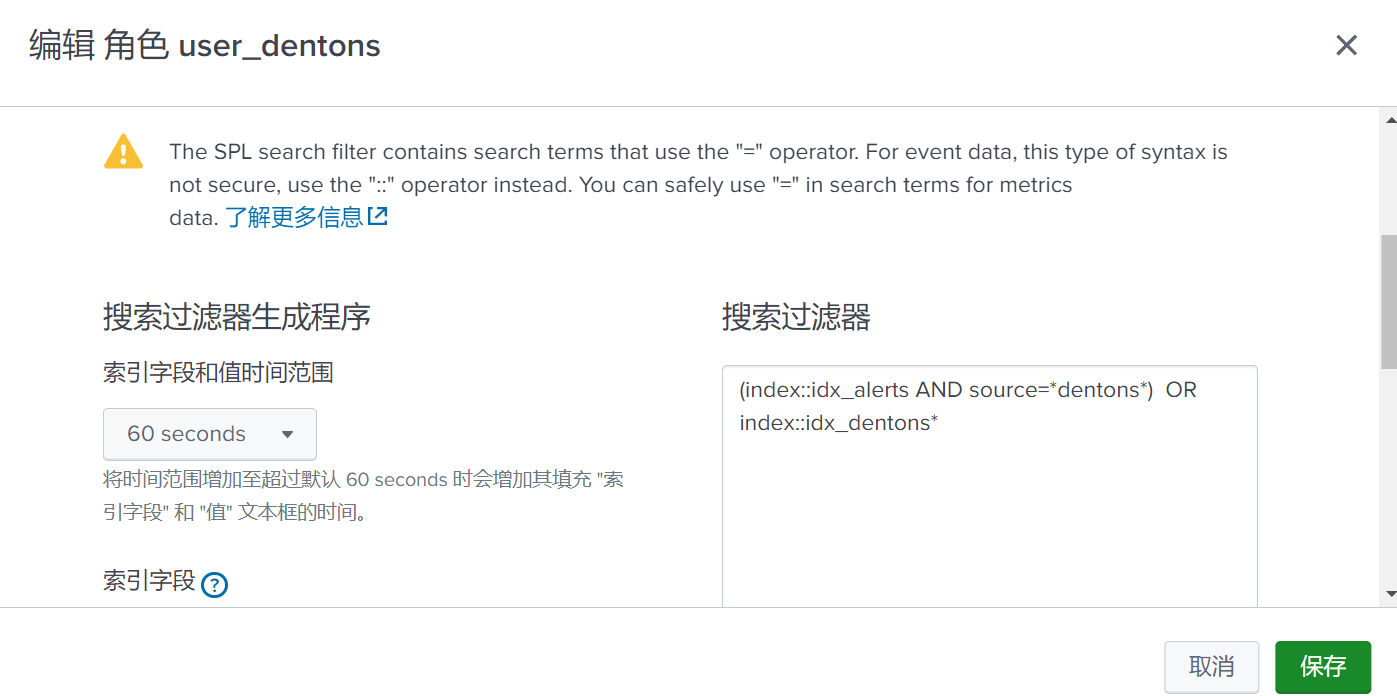
1. 点击设置🡪角色🡪新建角色，输入角色名称。命名规则：user-$客户简称$，随后修改角色权限



1. 继承：角色mss-user
2. 功能：新增accelerate\_datamodel，其余均不做改动
3. 索引：添加idx\_$客户简称$\*以及idx\_alerts



1. 添加限制：搜索过滤器中添加(index::idx\_alerts AND source=\*$客户简称$\*) OR index::idx\_$客户简称$\*



1. 保存

新建用户

1. 点击设置🡪用户🡪新建用户，输入用户名称。命名规则：$客户简称$
2. 为其设置密码：密码规则为20为随机密码包含数字字母下划线等
3. 修改默认应用为对应客户应用



1. 为其分配对应刚刚新建的角色



1. 取消勾选“首次登录需要修改密码”
2. 保存

修改应用权限

点击应用🡪管理应用，找到为该客户新建的应用，点击“权限”

修改权限为admin、power可写，admin、power、客户对应用户可读。

修改“应用所选角色权限到”为“仅此应用”

## 创建标准告警

从当前已有的标准的客户app中复制其全部告警到新客户的应用中，并适配告警

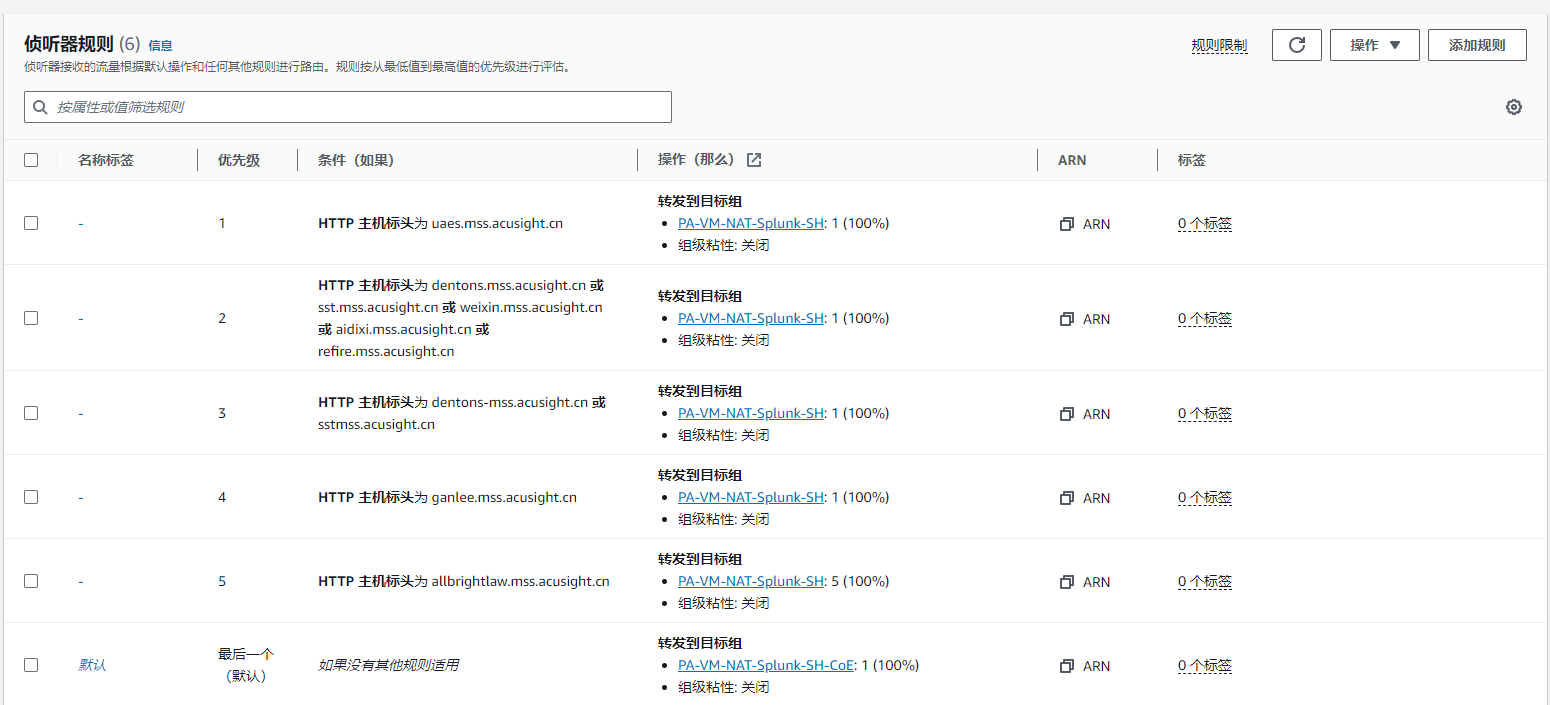
## 创建标准仪表板

从当前已有的标准的客户app中复制六个标准仪表板到新客户的应用中，并进行适配。

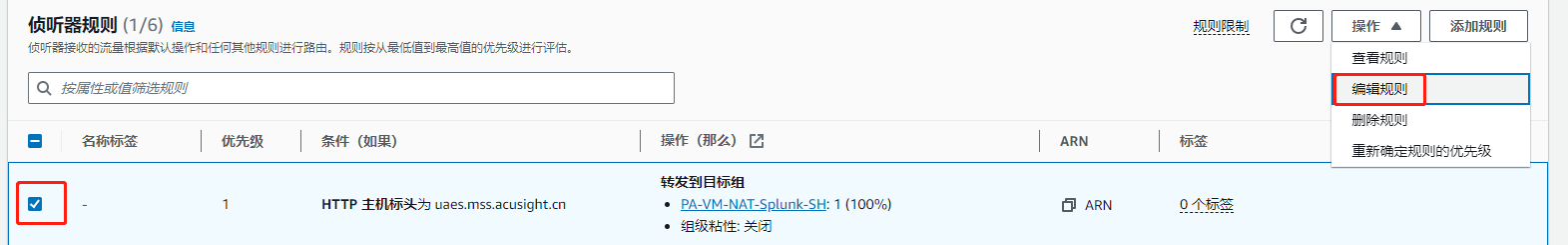
# 新建域名转发规则

进入MSS AWS控制台<https://cn-northwest-1.console.amazonaws.cn/>

依次点击ec2🡪负载均衡器🡪Security-demo-Splunk-ALB🡪HTTPS:8000进入如下界面：



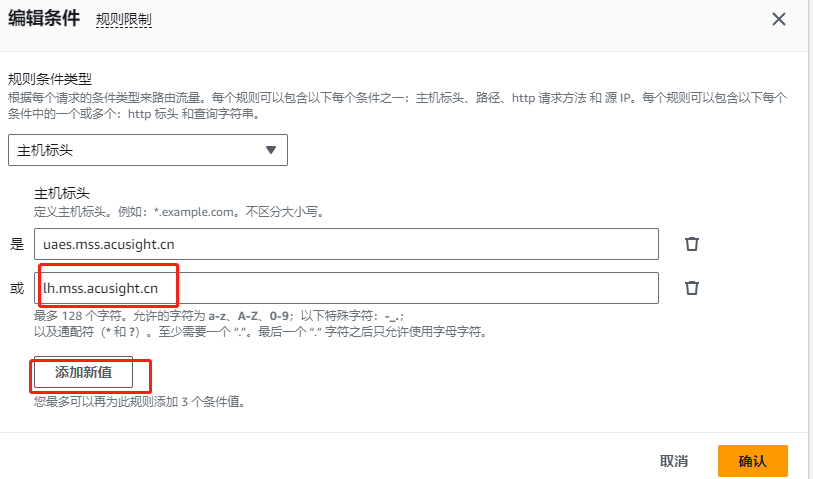
添加或编辑规则(每个规则中最多可包含5个条件，在有规则条件不足5个的情况下可优先选择编辑该规则)



勾选“主机标头”进行编辑



点击添加新值，输入新客户的域名，命名规则：$客户简称$.mss.acusight.cn



完成之后点击确认，随后一直点击“下一步”，并保存更改

