MikroTik最佳实践


2018年成都MUM
MikroTik STAFF
MikroTik STAFF
routerboard
ROUTING THE WORLD

主要内容

一. MikroTik 日志痛点

二. 安装Splunk

三. 日志接收设置

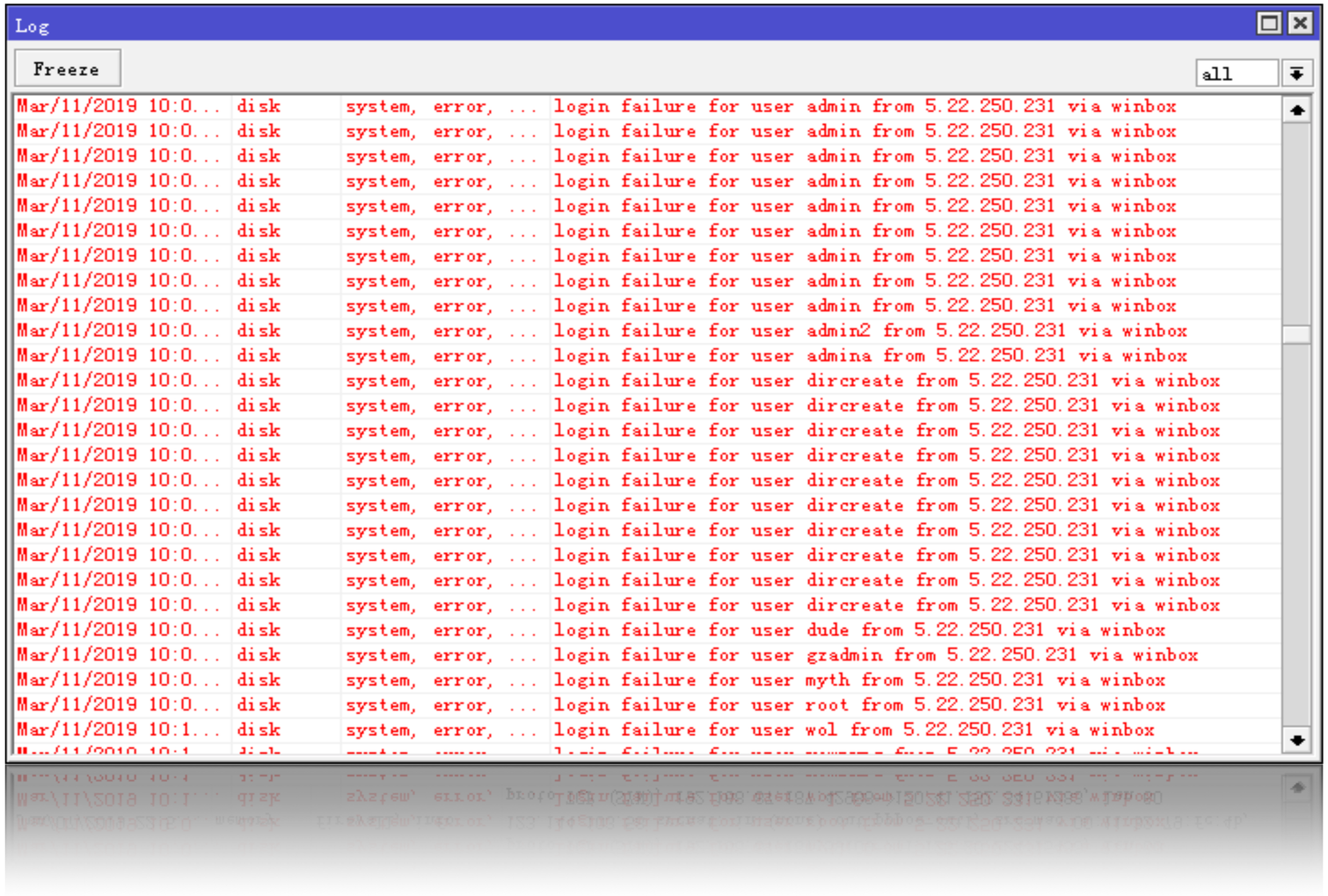
四. MikroTik 脚本分享

五. Live Dome

MikroTik日志痛点

1.设备重启后日志被清空。
2.无法查询日志历史记录。
3.设备节点多，日志分散，收集日志方式繁琐。
4.日志不能可视化。

日志查询困难

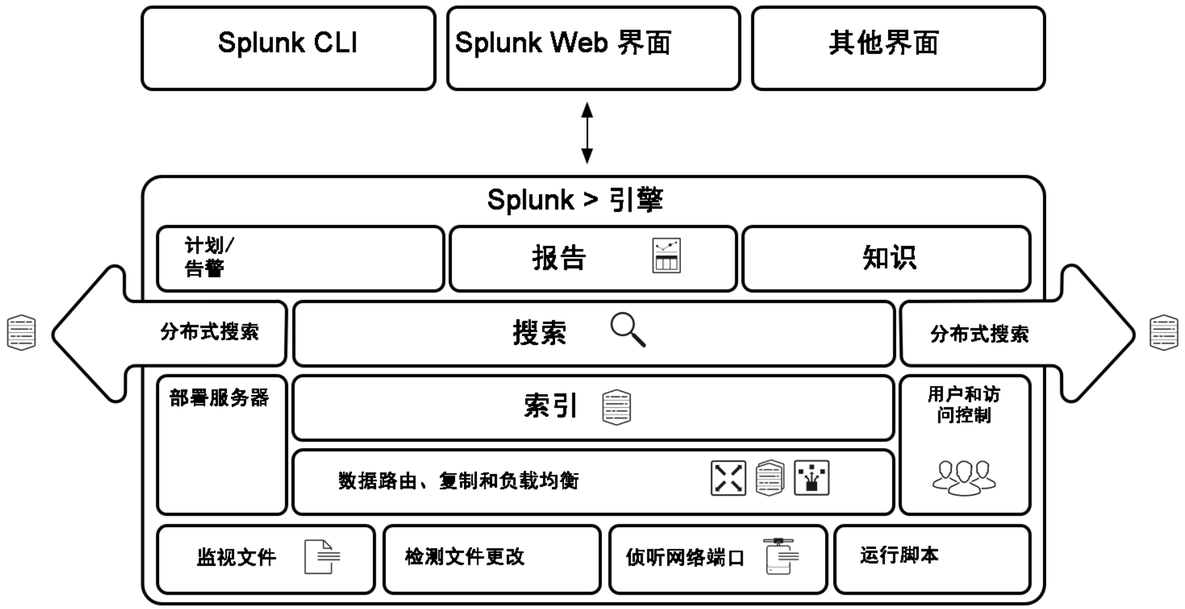


分布在全国各地的设备

如何解决?

什么是Splunk

Splunk 是一款软件产品，允许您搜索、分析和可视化从 IT 基础设施或业务组件收集的数据。Splunk可从网站、应用程序、传感器、设备等处获取数据。您定义完数据源后，Splunk对数据 流建立索引并将其解析至一系列您可以查看和搜索的单独事件中。



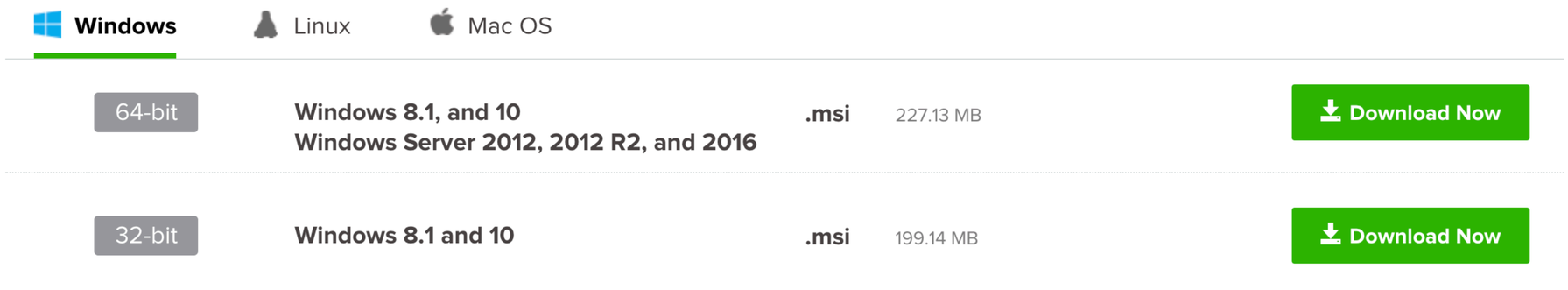
安装Splunk

下载Splunk 安装包：https://www.splunk.com/en_us/download/splunk-enterprise.html
试用60天每天数据索引量限制为500MB/天

Splunk Enterprise 7.2.6

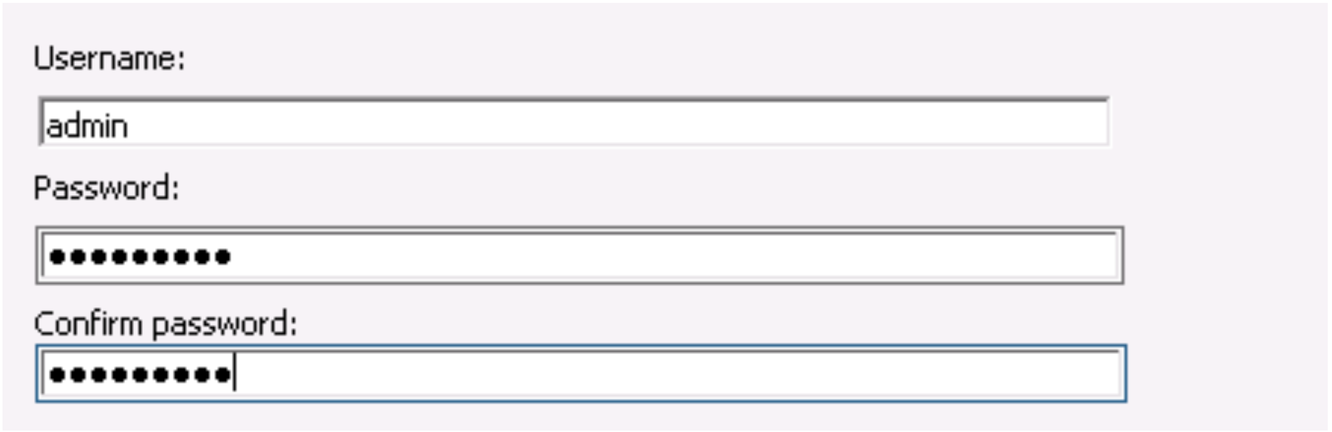
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

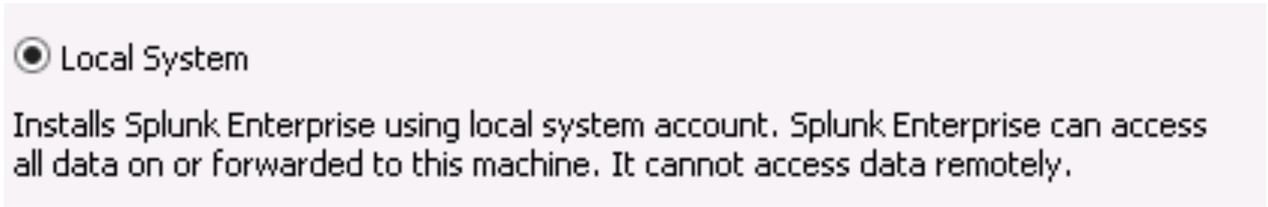
Choose Your Installation Package

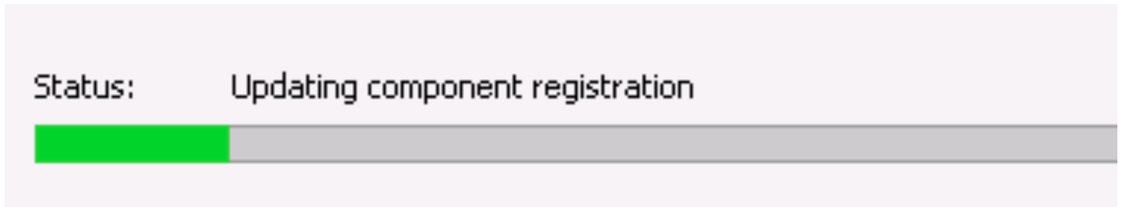


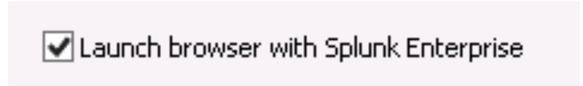
安装Splunk


Folder name:
D:\Program Files\Splunk\


Username:
admin
Password:
Confirm password:


Local System
Installs Splunk Enterprise using local system account. Splunk Enterprise can access all data on or forwarded to this machine. It cannot access data remotely.


Status:
Updating component registration

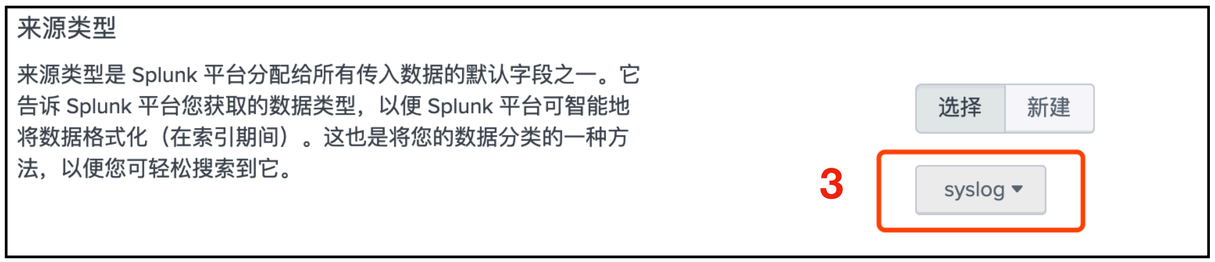

Launch browser with Splunk Enterprise

设置Splunk

本机访问：http://localhost:8000

输入我们前面安装时设置的账号密码登录系统

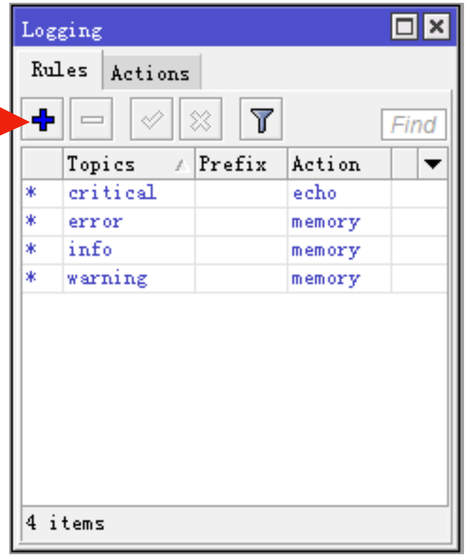
设置Splunk日志接收

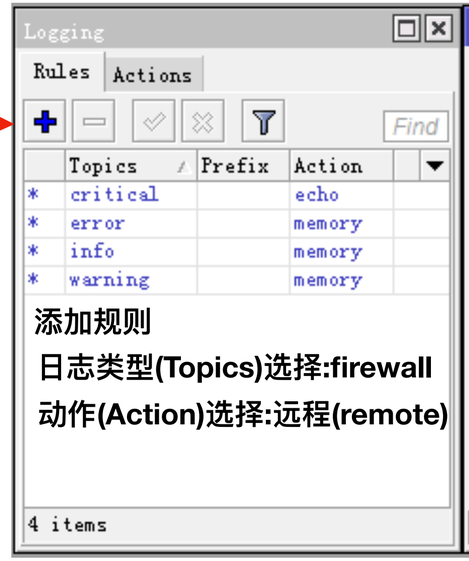


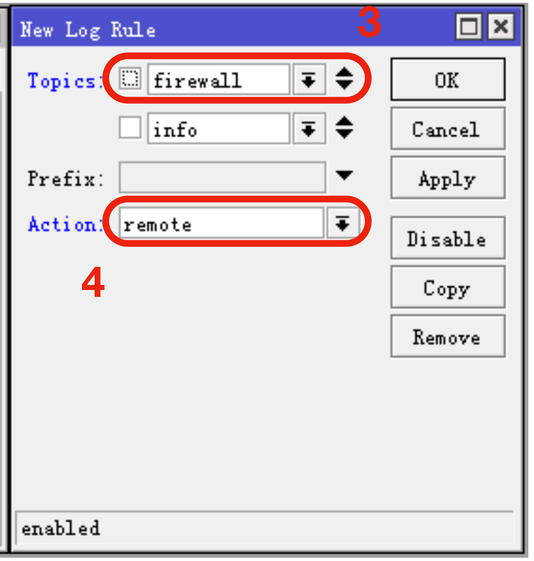
查询Log数据

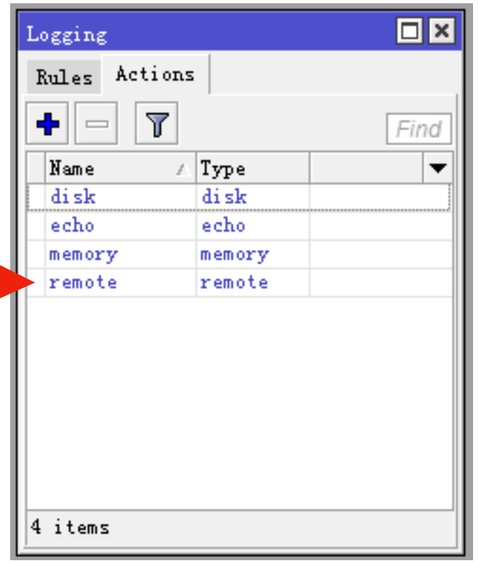

搜索或输入网站名称
splunk>enterprise
应用: S...
Admini...
消息
设置
活动
帮助
查找
搜索
数据集
报表
告警
仪表板
Search & Reporting
搜索
在此输入搜索...
前 24 小时
无事件采样
快速模式
如何搜索
如果不熟悉搜索功能或想要了解更多，请查看以下资源之一。
文档
教程
如何搜索
1,881,602,118 事件
已编入索引
3个月前
最早的事件
几秒前
最晚的事件
数据摘要
搜索历史

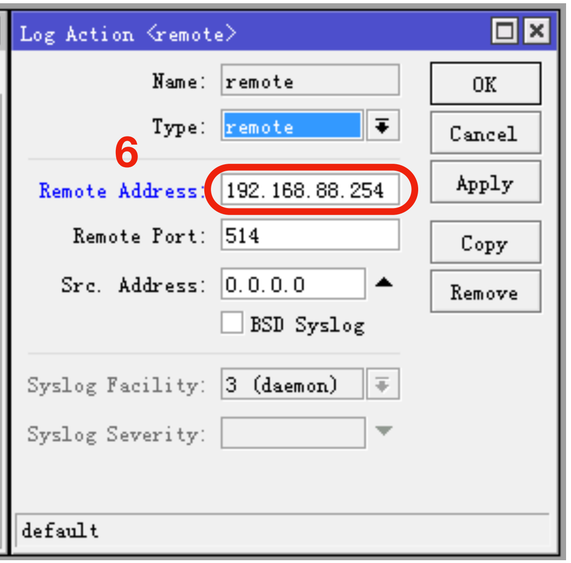
设置MikroTIK











设置脚本

```
# 添加远程服务器IP和接收端口
/system logging action add name=Server1 remote=x.x.x.x remote-port=514
target=remote
# 添加日志服务器
/system logging add action=Server1 topics=firewall,info
```

Mikrotik 支持多种类型的日志输出

```
[admin@AC] > system logging add topics=
account   certificate  e-mail    igmp-proxy  l2tp     ospf     pptp    rsvp       sstp       tr069      wireless
async     critical     error     info        ldp      ovpn     radius  script     state      upnp       write
backup    ddns         event     interface   lte      packet   radvd   sertcp     store      ups        !
bfd       debug        firewall  ipsec       manager  pim      raw     simulator  system     vrrp
bgp       dhcp         gps       iscsi       mme      poe-out  read    smb        telephony  warning
calc      dns          gsm       isdn        mpls     ppp      rip     snmp       tftp       watchdog
caps      dude         hotspot   kvm         ntp      pppoe    route   ssh        timer      web-proxy
```

生成NAT图表

MikroTik

编辑 导出 ...

今日数据量

19,826,847 条

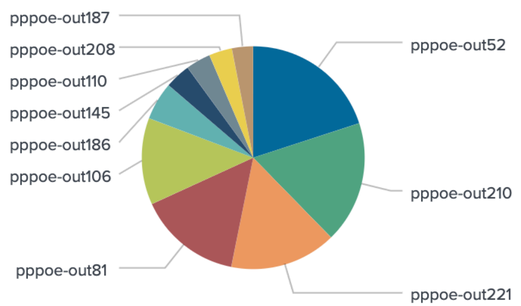
本月公网IP数量

516 个

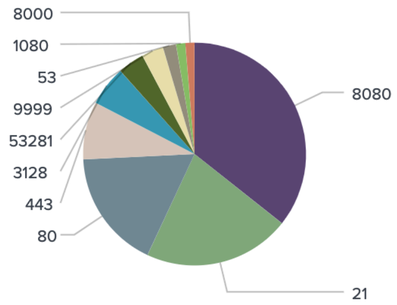
今日来源IP

127 个

今日PPPoE账号TOP 10



今日IP访问目的端口TOP 10



今日远程访问IP TOP 10

源IP地址	计数	占比
192.162.103.84	11931	37.990766
193.188.22.137	7338	23.365706
185.222.211.22	3943	12.555326
202.55.17.75	1649	5.250756
40.135.239.2	1030	3.279733
183.66.235.182	1000	3.184206
193.188.22.13	726	2.311734
123.157.78.171	711	2.263971
59.173.19.66	419	1.334182
85.93.20.238	414	1.318261

今日尝试登陆失败

IP地址	web
119.86..	1

今日登陆成功的用户

IP地址	admin
14.110.	2

脚本分享

下载文本并读取文本内容

#下载文本
/tool fetch mode=https url="https://ros.ac/mum/ps.txt" dst-path=/ps.txt
#读取文本内容并赋值给password变量
:global password [/file get ps.txt contents];
#打印变量
:put $password

```
[admin@AC] > /tool fetch mode=https url=https://ros.ac/mum/ps.txt dst-path=/ps.txt
      status: finished
  downloaded: 0KiBC-z pause]
       total: 0KiB
    duration: 1s

[admin@AC] > :global password [/file get ps.txt contents];
[admin@AC] > :put  $password
mum20191019
[admin@AC] >
```

脚本分享

封HTTPS网站

/ip firewall address-list
#添加要屏蔽的网站到地址里面
add address=www.baidu.com list=BaiDu
/ip firewall filter
添加防火墙规则
add action=reject chain=forward comment="Drop Baidu" disabled=yes dst-address-list=BaiDu protocol=tcp reject-with=tcp-reset

操作小技巧

Ctrl + C 中断操作

Ctrl + X 进入安全模式

```
[admin@AC] >
[Safe Mode taken]
[admin@AC] <SAFE>
```

```
[admin@AC] >
[Safe Mode taken]
[Safe Mode released]
[admin@AC] >
```

Ctrl + V 进入Hotlock 模式（命令将自动完成）

```
[admin@AC] >
[admin@AC] >>
```

Ctrl + D 注销会话同时也会撤消所有安全模式更改

Ctrl + K 删除光标后面所有字符

Log在线演示

Live Dome

参考资料

- MikroTik 维基百科：http://wiki.mikrotik.com
- Spunk官网:htttps://www.splunk.com
- Mikrotik Log：https://wiki.mikrotik.com/wiki/.../Log
- Splunk文档：https://docs.splunk.com/Documentation

Ali

Jiangbei, Chongqing

Scan the QR code to add me on WeChat

感谢聆听

ali@rosm.cn

https://t.me/MTEngineer