背景抓包工具

使用指导手册

版权声明与使用须知

版权声明

©2023 浙江宇视科技有限公司。保留一切权利。

未经浙江宇视科技有限公司（下称“本公司”）书面许可，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

本手册描述的产品中可能包含本公司及可能存在的许可人享有版权的软件。未经相关权利人许可，任何人不得以任何形式对前述软件进行包括但不限于复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件著作权的行为。

使用须知

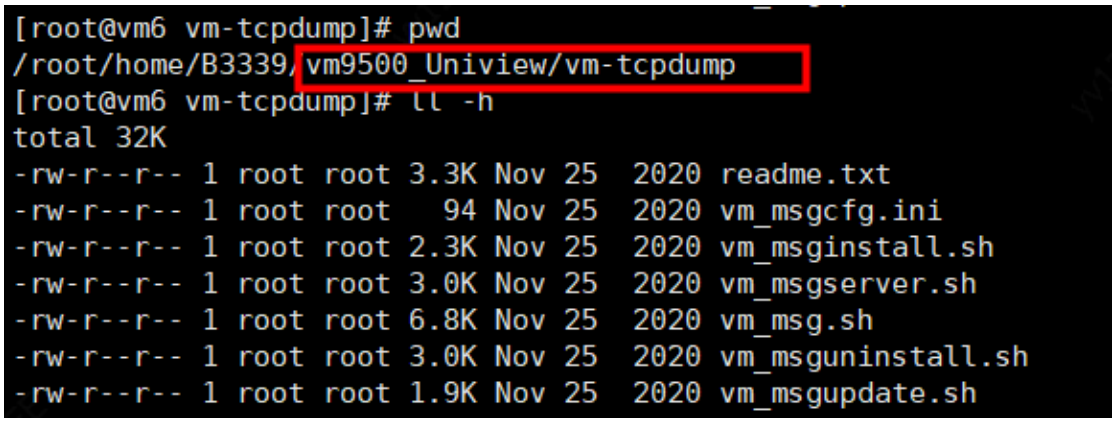
由于产品版本升级等原因，本手册内容会不定期更新。

本手册仅作为使用指导，其内所有陈述、信息和建议等均不构成任何明示或暗示的担保。本手册中的图形、图表或照片等仅用于说明示例，可能与实际产品存在差异，请以实物为准。

一． 工具概况

当遇到偶现性问题时，很难抓取到出现问题时的报文信息，为减轻收集信息的工作强度，可使用背景抓包工具，后台可根据背景抓包工具配置指定的端口一直进行抓包，待到问题复现即可获得有效信息；

在 B3331 及以上版本合入背景抓包脚本，安装目录为：/vm9500_Uniview/vm-tcpdump。



脚本信息如下：

vm_msginstall.sh------背景抓包安装脚本

vm_msgupdate.sh-----背景抓包升级脚本

vm_msguninstall.sh---背景抓包卸载脚本

vm_msgcfg.ini---------背景抓包配置文件

vm_msgserver.sh------控制脚本,可传入相关参数

二．工具使用方法

1. 查看此前是否安装过背景抓包工具：

sh /vm9500_Uniview/vm-tcpdump/vm_msgserver.sh status

```
[root@vm6 vm-tcpdump]# sh vm_msgserver.sh status
version: 2018-04-04
/var/vm_msg : 1651 M
[  running  ]
tcpdump 16964 S 8800 /var/vm_msg/2021-07-07-17-00-01_soi_8800.cap
tcpdump 17141 S 5060 /var/vm_msg/2021-07-07-17-00-01_sip_5060.cap
tcpdump 17162 S 5061 /var/vm_msg/2021-07-07-17-00-01_sg_5061.cap
root 11933 11912 vm_msg.sh defunct
root 15966 15957 vm_msg.sh defunct
[root@vm6 vm-tcpdump]# pwd
/root/home/B3337/vm9500_Uniview/vm-tcpdump
```

未安装如下图所示：

```
[root@localhost vm-tcpdump]# pwd
/home/B3352/vm9500_Uniview/vm-tcpdump
[root@localhost vm-tcpdump]# sh vm_msgserver.sh status
 server already uninstall
[root@localhost vm-tcpdump]#
```

2.判断环境中背景抓包工具是否为最新版本：cat vm_msgcfg.ini

其中 CReatTime=2018-04-04 表示抓包的版本号，以时间进行命名，若此配置文件中的版本号和实际版本号一致（实际版本号在上一步中的 version 可直接查看）则不需要对背景抓包工具进行更新，如果不一致则需进行更新或安装。

```
[root@vm6 vm-tcpdump]# cat vm_msgcfg.ini
[vm_msgcfg]
port=8800,5060,5061,5063,161
path=/var/vm_msg
limitSize=20000
creatTime=2018-04-04[root@vm6 vm-tcpdump]#
```

背景抓包的配置文件说明如下：

port：需要抓取报文的端口

path：抓取报文后的保存路径

limitSize：path 路径下的报文可占文件的最大值，超过该文件大小则会启动清理机制

creatTime：版本时间

3.安装命令：sh vm_msginstall.sh

安装时会有配置端口提示，可输入需要抓包的端口，默认为 8800.5060.5061

如果之前有安装过老版本的背景抓包工具，可以运行升级脚本升级：

sh vm_msgupdate.sh

4.安装之后会按照配置文件中的端口抓取报文，报文默认保存路径为：/var/vm_msg 下，抓包文件会根据配置文件中设置的容量限制做到自动清理。

5.问题复现后，收集报文分析

注：

- 抓包时要根据业务，过滤相应端口或 IP 去获取到想要的报文
- 以下给出几个常见业务的抓包过滤方法，实际如何抓包需要结合局点业务及环境情况灵活变动，如果业务压力不大建议抓全包

本域相机实况	过滤 5060/8800 端口
IMOS 相机跨域实况	过滤 5060/5061/8800 端口
GB 相机跨域实况	过滤 5060/5061/5063/8800 端口
SIP 告警上报	过滤 5060/5063 端口
回放下载	过滤 80/554/5060/5066/5061/8800 端口
本域设备注册	过滤 5060/5063 端口
外域注册、资源共享、外域资源查询	上下级域同时抓包过滤 5060/5061 端口
存在网闸/中间防火墙等网络转发设备	转发设备两侧同时抓包（确认是否抓发设备改变报文）
涉及跨域	加上 5061 端口，尽量上下级同时抓包
涉及 GB 相机	加上 5063 端口
通用情况	尽量抓全包

注：背景抓包工具不支持抓全包


uniview 宇视
视无界 智以恒