收集Firepower常见问题的日志

目录

简介

本文档介绍在打开TAC案例之前要收集哪些日志以排除Firepower常见问题。

先决条件

要求

思科建议您了解以下产品：

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

收集Firepower常见问题的日志

1. FTD意外的故障转移问题

在打开TAC案例之前需要收集的信息来排查问题：

- 发生故障的单元的主机名和IP地址。
- 最近所做的任何更改。
- 事件发生：事件的时间和时区。
- 故障切换电缆连接：直接与两台设备或设备之间的任何中间设备（交换机）连接。
- 两台设备所需的命令输出：

show tech-support

show failover-history

show failover state

- 事件发生前后10分钟的系统日志。
- 收集FTD故障排除文件。

要生成故障排除文件，请参阅Firepower文件生成过程故障排除。

要提交案例，请参阅TAC SR。

示例：如何从FTDv运行命令。

登录FTD SSH:

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.6.5 (build 13)
Cisco Firepower Threat Defense for VMWare v6.6.5 (build 81)

>
>
```

从clish运行命令：

```
> show tech-support                 <- - To display configuration of the device.
```

```
> show failover history             <- - To display failover Date/Time, what was the failover state an
```

```
> show failover state               <- - To display Last Failure Reason and Date/Time.
```

2. FMC GUI不可访问的问题

在打开TAC案例之前需要收集的信息来排查问题：

- 最近所做的任何更改。
- FMC SSH所需的命令输出：

pmtool状态 | grep -i gui

pmtool状态 | grep -E "等待|关闭|禁用"

free -g

df -h

DBCheck.pl

顶部

- 访问FMC GUI时，如果出现任何错误消息，则获取该错误消息的截图。
- 访问FMC GUI时，需要收集提到的命令输出：

pigtail gui

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- 收集FMC故障排除文件。

要生成故障排除文件，请参阅Firepower文件生成过程故障排除。

要提交案例，请参阅TAC SR。

示例：如何从FMCv运行命令。

登录FMC SSH:

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

从根目录运行命令：

```
root@firepower:~# pmtool status | grep -i gui                  <- - To display all GUI services status.
```

```
root@firepower:~# pmtool status | grep -E "Wait|down|disabled" <- - To display services that are in wai
```

```
root@firepower:~# free -g                                    <- - To display Used and Free memory in

root@firepower:~# df -h                                      <- - To display Used and Free disk.

root@firepower:~# DBCheck.pl          <- - To display any error or warning in database.(Database Integri

root@firepower:~# top                 <- - To display which processes cpu & memory utilisation.

root@firepower:~# pigtail gui         <- - To display GUI logs in real time.

root@firepower:~# cd /var/log/httpd/
root@firepower:/var/log/httpd# tail -f httpsd_access_log <- - To display GUI web server access logs in

root@firepower:~# cd /var/log/httpd/
root@firepower:/var/log/httpd# tail -f httpsd_error_log  <- - To display GUI web server error logs in r
```

要中断日志，请输入CTRL+C。

3. FMC备份失败问题

在打开TAC案例之前需要收集的信息来排查问题：

- 最近所做的任何更改。
- 备份失败的错误消息的截图。
- 手动备份失败还是计划/自动备份失败？
- 如果计划备份失败，请收集事件发生情况：时间和时区。
- 如果手动备份失败，请在执行手动备份时收集命令输出：

tail -f /var/log/backup.log

- 收集FMC故障排除文件。

要生成故障排除文件，请参阅Firepower文件生成过程故障排除。

要提交案例，请参阅TAC SR。

示例：如何从FMCv运行命令。

登录FMC SSH并从根目录运行命令：

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
Last login: Wed Sep  6 21:38:20 UTC 2023 on pts/0
root@firepower:~#
root@firepower:~# cd /var/log/
root@firepower:/var/log# tail -f backup.log                    <- - To display backup logs in real tim
```

要中断日志，请输入CTRL+C。

4.策略部署失败

- 最近所做的任何更改。
- 策略部署失败的百分比是多少。
- 从FMC GUI中，截取部署失败的错误消息的屏幕截图，并记录以收集事务ID:

点击Deploy选项卡旁边的图标，然后点击Deployment选项卡，然后点击Show History选项卡。

- 执行策略部署时，需要收集提到的命令输出：

从FMC:

尾部部署

tail -f /var/log/sf/policy_deployment.log

从FTD:

尾部部署

tail -f /ngfw/var/log/ngfwManager.log

tail -f /ngfw/var/log/sf/policy_deployment.log

- 收集FMC和FTD故障排除文件。

要生成故障排除文件，请参阅Firepower文件生成过程故障排除。

要提交案例，请参阅TAC SR。

示例：如何从FMCv运行命令。

登录FMC SSH:

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.10.1 (build 175)
Cisco Firepower Management Center for VMware v7.0.1 (build 84)

>
> expert
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~#
```

从根目录运行命令：

```
root@firepower:~# pigtail deploy                              <- - To display deployment logs in real tim
```

```
root@firepower:/# cd /var/log/sf
root@firepower:/var/log/sf# tail -f policy_deployment.log   <- - To display policy deployment logs in r
```

示例：如何从FTDv运行命令。

登录FTD SSH:

```
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.6.5 (build 13)
Cisco Firepower Threat Defense for VMWare v6.6.5 (build 81)

>
> expert
admin@FTDA:~$ sudo su -
Password:
root@FTDA:~#
```

从根目录运行命令：

```
root@FTDA:~# pigtail deploy                  <- - To display deployment related logs in real time.
```

```
root@FTDA:~# cd /ngfw/var/log
root@FTDA:log# tail -f ngfwManager.log       <- - To display FTD to FMC communication related logs in r
```

```
root@firepower:/# cd /var/log/sf
root@firepower:/var/log/sf# tail -f policy_deployment.log   <- - To display policy deployment logs in r
```

要中断日志，请输入CTRL+C。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。