Collect Logs for Firepower Common Issues

Contents

Introduction

This document describes about what logs to collect before opening a TAC case for troubleshooting Firepower common issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

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

Collect Logs for Firepower Common Issues

1. FTD Unexpected Failover Issue

Information need to collect before opening TAC case to troubleshoot the issue:

- Hostname and IP address of the unit which failed.
- Any recent changes done.
- Event occurrence: Time of the event and Timezone.
- Failover cable connectivity: Directly connected with both units or any intermediate device (switch) in between.
- Commands output required from both units:

show tech-support

show failover-history

show failover state

- Syslogs for 10 minutes before and after event occurrence.
- Collect FTD troubleshoot file.

To generate a troubleshoot file, refer to Troubleshoot Firepower File Generation Procedures.

To open a case, refer to TAC SR.

Example: How to run commands from FTDv.

Log into 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)

>
>
```

Run the commands from clish:

```
> 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 Inaccessible Issue

Information need to collect before opening TAC case to troubleshoot the issue:

- Any recent changes done.
- Commands output required from FMC SSH:

pmtool status | grep -i gui

pmtool status | grep -E "Wait|down|disabled"

free -g

df -h

DBCheck.pl

top

- While accessing the FMC GUI, if there is any error message, then take a screenshot of the error

message.

- While accessing the FMC GUI, need to collect mentioned commands output:

pigtail gui

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- Collect FMC troubleshoot file.

To generate a troubleshoot file, refer to Troubleshoot Firepower File Generation Procedures.

To open a case, refer to TAC SR.

Example: How to run commands from FMCv**.**

Log into 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:~#
```

Run the commands from root:

```
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
```

To interrupt the logs enter **CTRL+C**.

3. FMC Backup Failed Issue

Information need to collect before opening TAC case to troubleshoot the issue:

- Any recent changes done.
- Screenshot of the error messages for backup failure.
- Is Manual backup failing or Scheduled/Automatic backup failing?
- If scheduled backup failing, collect event occurrence: Time and Timezone.
- If manual backup failing, collect command output, while performing manual backup:

tail -f /var/log/backup.log

- Collect FMC troubleshoot file.

To generate a troubleshoot file, refer to Troubleshoot Firepower File Generation Procedures.

To open a case, refer to TAC SR.

Example: How to run commands from FMCv.

Log into FMC SSH and run the command from root:

```
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
```

To interrupt the logs enter **CTRL+C**.

4. Policy Deployment Failure

- Any recent changes done.
- At what percentage policy deployment is failing.
- From FMC GUI, take a screenshot of the error messages for deployment failure and transcript to collect the transaction ID:

Click on icon next to Deploy tab, then click on Deployment tab, and click on Show History tab.

- While performing the policy deployment, need to collect mentioned commands output:

From FMC:

pigtail deploy

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

From FTD:

pigtail deploy

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

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

- Collect FMC and FTD troubleshoot file.

To generate a troubleshoot file, refer to Troubleshoot Firepower File Generation Procedures.

To open a case, refer to TAC SR.

Example: How to run commands from FMCv.

Log into 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:~#
```

Run the commands from root:

```
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
```

Example: How to run commands from FTDv.

Log into 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:~#
```

Run the commands from root:

```
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
```

To interrupt the logs enter **CTRL+C.**