Sammeln von Protokollen für häufige Probleme mit Firepower

Inhalt

Einleitung

In diesem Dokument wird beschrieben, welche Protokolle gesammelt werden müssen, bevor ein TAC-Ticket zur Fehlerbehebung bei häufigen FirePOWER-Problemen geöffnet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

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

Sammeln von Protokollen für häufige Probleme mit Firepower

1. Unerwartetes FTD-Failover-Problem

Zur Fehlerbehebung müssen Informationen gesammelt werden, bevor ein TAC-Serviceticket geöffnet wird:

- Hostname und IP-Adresse der fehlerhaften Einheit.
- Alle kürzlich vorgenommenen Änderungen
- Ereignis: Zeit des Ereignisses und Zeitzone.
- Failover-Kabelverbindung: Direkter Anschluss an beide Einheiten oder ein zwischengeschaltetes Gerät (Switch).
- Von beiden Einheiten erforderliche Befehlsausgabe:

show tech-support

Failover-Verlauf anzeigen

Failover-Status anzeigen

- Syslogs für 10 Minuten vor und nach dem Auftreten des Ereignisses.
- Sammeln Sie die FTD-Fehlerbehebungsdatei.

Informationen zum Generieren einer Fehlerbehebungsdatei finden Sie unter Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung.

Informationen zum Öffnen eines Tickets finden Sie im TAC SR.

Beispiel: Ausführung von Befehlen aus FTDv.

Bei FTD SSH anmelden:

```
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)

>
>
```

Führen Sie die Befehle aus 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 unzugänglich

Zur Fehlerbehebung müssen Informationen gesammelt werden, bevor ein TAC-Serviceticket geöffnet wird:

- Alle kürzlich vorgenommenen Änderungen
- Von FMC SSH erforderliche Befehlsausgabe:

pmtool-Status | grep -i gui

pmtool-Status | grep -E "Wait|down|disabled" (Warten|deaktiviert)

frei -g

df -h

DBCheck.pl

oberste

- Wenn beim Zugriff auf die FMC-GUI eine Fehlermeldung angezeigt wird, erstellen Sie einen Screenshot der Fehlermeldung.
- Beim Zugriff auf die FMC-GUI müssen die genannten Befehle gesammelt werden:

Huckepackgui

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- FMC-Fehlerbehebungsdatei sammeln.

Informationen zum Generieren einer Fehlerbehebungsdatei finden Sie unter Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung.

Informationen zum Öffnen eines Tickets finden Sie im TAC SR.

Beispiel: Ausführung von Befehlen über FMCv.

Bei FMC SSH anmelden:

```
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:~#
```

Führen Sie die Befehle von root aus:

```
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
```

Um die Protokolle zu unterbrechen, drücken Sie STRG+C.

3. Fehler bei FMC-Sicherung

Zur Fehlerbehebung müssen Informationen gesammelt werden, bevor ein TAC-Serviceticket geöffnet wird:

- Alle kürzlich vorgenommenen Änderungen
- Screenshot der Fehlermeldungen für einen Backup-Fehler.
- Schlägt die manuelle Sicherung fehl oder schlägt die zeitgesteuerte/automatische

Sicherung fehl?

- Wenn die geplante Sicherung fehlschlägt, erfassen Sie das Ereignis: Zeit und Zeitzone.
- Wenn die manuelle Sicherung fehlschlägt, erfassen Sie die Befehlsausgabe, während Sie eine manuelle Sicherung durchführen:

tail -f /var/log/backup.log

- FMC-Fehlerbehebungsdatei sammeln.

Informationen zum Generieren einer Fehlerbehebungsdatei finden Sie unter Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung.

Informationen zum Öffnen eines Tickets finden Sie im TAC SR.

Beispiel: Ausführung von Befehlen über FMCv.

Melden Sie sich bei FMC SSH an, und führen Sie den Befehl vom Root aus:

```
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
```

Um die Protokolle zu unterbrechen, drücken Sie STRG+C.

4. Fehler bei der Richtlinienbereitstellung

- Alle kürzlich vorgenommenen Änderungen
- Wie hoch ist der Prozentsatz der fehlgeschlagenen Richtlinienbereitstellung?
- Screenshot der FMC-GUI mit den Fehlermeldungen für Bereitstellungsfehler und Transkript zum Erfassen der Transaktions-ID:

Klicken Sie auf das Symbol neben der Registerkarte "Bereitstellen", dann auf die Registerkarte "Bereitstellung" und dann auf die Registerkarte "Versionsverlauf anzeigen".

- Bei der Richtlinienbereitstellung müssen die oben genannten Befehlsausgaben gesammelt werden:

Von FMC:

Spitzendruck

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

Von FTD:

Spitzendruck

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

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

- Sammeln Sie eine Fehlerbehebungsdatei für FMC und FTD.

Informationen zum Generieren einer Fehlerbehebungsdatei finden Sie unter Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung.

Informationen zum Öffnen eines Tickets finden Sie im TAC SR.

Beispiel: Ausführung von Befehlen über FMCv.

Bei FMC SSH anmelden:

```
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:~#
```

Führen Sie die Befehle von root aus:

```
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
```

Beispiel: Ausführung von Befehlen aus FTDv.

Bei FTD SSH anmelden:

```
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:~#
```

Führen Sie die Befehle von root aus:

```
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
```

Um die Protokolle zu unterbrechen, drücken Sie STRG+C.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.