Recopilar registros para problemas comunes de Firepower

Contenido

Introducción

Este documento describe los registros que se deben recopilar antes de abrir un caso TAC para la resolución de problemas comunes de Firepower.

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

Recopilar registros para problemas comunes de Firepower

1. FTD problema de falla inesperado

Información que se debe recopilar antes de abrir un caso del TAC para solucionar el problema:

- Nombre de host y dirección IP de la unidad que ha fallado.
- Cualquier cambio reciente realizado.
- Evento: Hora del evento y zona horaria.
- Conectividad con cable de conmutación por fallo: conectado directamente con ambas unidades o con cualquier dispositivo intermedio (switch) intermedio.
- Se requiere la salida de comandos de ambas unidades:

show tech-support

show failover-history

show failover state

- Registros del sistema durante 10 minutos antes y después de que se produzca el evento.
- Recopilar archivo de solución de problemas de FTD.

Para generar un archivo de solución de problemas, consulte Resolución de problemas de procedimientos de generación de archivos de Firepower.

Para abrir un caso, consulte TAC SR.

Ejemplo: Cómo ejecutar comandos desde FTDv.

Inicie sesión en 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)

>
>
```

Ejecute los comandos desde 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. Problema inaccesible de la GUI de FMC

Información que se debe recopilar antes de abrir un caso del TAC para solucionar el problema:

- Cualquier cambio reciente realizado.
- Salida de comandos requerida de FMC SSH:

estado de pmtool | grep -i gui

estado de pmtool | grep -E "Wait|down|disabled"

free -g

df -h

DBCheck.pl

arriba

- Al acceder a la GUI del FMC, si aparece algún mensaje de error, realice una captura de pantalla del mensaje.
- Al acceder a la GUI de FMC, es necesario recopilar la salida de los comandos mencionados:

GUI de coleta

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- Recopile el archivo de solución de problemas de FMC.

Para generar un archivo de solución de problemas, consulte Resolución de problemas de procedimientos de generación de archivos de Firepower.

Para abrir un caso, consulte TAC SR.

Ejemplo: Cómo ejecutar comandos desde FMCv.

Inicie sesión en 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:~#
```

Ejecute los comandos desde la raíz:

```
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
```

Para interrumpir los registros, escriba CTRL+C.

3. Problema de falla de respaldo de FMC

Información que se debe recopilar antes de abrir un caso del TAC para solucionar el problema:

- Cualquier cambio reciente realizado.
- Captura de pantalla de los mensajes de error de la copia de seguridad.
- ¿Falla la copia de seguridad manual o la copia de seguridad programada/automática?
- Si falla la copia de seguridad programada, recopile la aparición del evento: Hora y zona horaria.

- Si falla la copia de seguridad manual, recopile la salida del comando mientras realiza la copia de seguridad manual:

tail -f /var/log/backup.log

- Recopile el archivo de solución de problemas de FMC.

Para generar un archivo de solución de problemas, consulte Resolución de problemas de procedimientos de generación de archivos de Firepower.

Para abrir un caso, consulte TAC SR.

Ejemplo: Cómo ejecutar comandos desde FMCv.

Inicie sesión en FMC SSH y ejecute el comando desde 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
```

Para interrumpir los registros, escriba CTRL+C.

4. Fallo de implementación de políticas

- Cualquier cambio reciente realizado.
- Porcentaje de fallos en la implementación de políticas.
- En la GUI de FMC, realice una captura de pantalla de los mensajes de error de fallo de implementación y transcripción para recopilar la ID de transacción:

Haga clic en el icono situado junto a la ficha Desplegar y, a continuación, haga clic en la ficha Despliegue y, a continuación, haga clic en la ficha Mostrar historial.

- Mientras se realiza la implementación de políticas, es necesario recopilar los resultados de los comandos mencionados:

Desde el CSP:

implementación de coleta

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

Desde FTD:

implementación de coleta

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

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

- Recopile el archivo de solución de problemas de FMC y FTD.

Para generar un archivo de solución de problemas, consulte Resolución de problemas de procedimientos de generación de archivos de Firepower.

Para abrir un caso, consulte TAC SR.

Ejemplo: Cómo ejecutar comandos desde FMCv.

Inicie sesión en 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:~#
```

Ejecute los comandos desde la raíz:

```
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
```

Ejemplo: Cómo ejecutar comandos desde FTDv.

Inicie sesión en 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:~#
```

Ejecute los comandos desde la raíz:

```
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
```

Para interrumpir los registros, escriba CTRL+C.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).