Coletar registros para problemas comuns do Firepower

Contents

Introdução

Este documento descreve os registros a serem coletados antes da abertura de um caso de TAC para solucionar problemas comuns do Firepower.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

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

Coletar registros para problemas comuns do Firepower

1. Problema de Failover Inesperado de FTD

As informações precisam ser coletadas antes da abertura do caso do TAC para solucionar o problema:

- Nome de host e endereço IP da unidade que falhou.
- Quaisquer alterações recentes feitas.
- Ocorrência do evento: A hora do evento e o fuso horário.
- Conectividade de cabo de failover: conectado diretamente com ambas as unidades ou qualquer dispositivo intermediário (switch) entre elas.
- Saída de comandos necessária de ambas as unidades:

show tech-support

show failover-history

show failover state

- Syslogs para 10 minutos antes e depois da ocorrência do evento.
- Coletar arquivo de solução de problemas de FTD.

Para gerar um arquivo de solução de problemas, consulte Solução de problemas de procedimentos de geração de arquivos do Firepower.

Para abrir um caso, consulte TAC SR.

Exemplo: Como executar comandos do FTDv.

Faça login no 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)

>
>
```

Execute os comandos a partir do 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. Questão inacessível da interface gráfica do CVP

As informações precisam ser coletadas antes da abertura do caso do TAC para solucionar o problema:

- Quaisquer alterações recentes feitas.
- Saída de comandos necessária do FMC SSH:

status de pmtool | grep -i gui

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

free -g

df -h

DBCheck.pl

superior

- Ao acessar a GUI do FMC, se houver alguma mensagem de erro, faça uma captura de tela da mensagem de erro.
- Ao acessar a GUI do FMC, é necessário coletar a saída dos comandos mencionados:

gui pigtail

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- Colete o arquivo de solução de problemas do FMC.

Para gerar um arquivo de solução de problemas, consulte Solução de problemas de procedimentos de geração de arquivos do Firepower.

Para abrir um caso, consulte TAC SR.

Exemplo: Como executar comandos do FMCv.

Faça login no 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:~#
```

Execute os comandos a partir da raiz:

```
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 interromper os logs, insira CTRL+C.

3. Problema de Falha de Backup do FMC

As informações precisam ser coletadas antes da abertura do caso do TAC para solucionar o problema:

- Quaisquer alterações recentes feitas.
- Captura de tela das mensagens de erro para falha de backup.
- O backup manual está falhando ou o backup programado/automático está falhando?

- Se o backup agendado falhar, colete a ocorrência do evento: Hora e Fuso Horário.
- Se o backup manual falhar, colete a saída do comando ao executar o backup manual:

tail -f /var/log/backup.log

- Colete o arquivo de solução de problemas do FMC.

Para gerar um arquivo de solução de problemas, consulte Solução de problemas de procedimentos de geração de arquivos do Firepower.

Para abrir um caso, consulte TAC SR.

Exemplo: Como executar comandos do FMCv.

Efetue login no FMC SSH e execute o comando a partir da raiz:

```
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 interromper os logs, insira CTRL+C.

4. Falha na Implantação da Política

- Quaisquer alterações recentes feitas.
- Em qual porcentagem a implantação da política está falhando.
- Na GUI do FMC, tire uma captura de tela das mensagens de erro para falha de implantação e transcrição para coletar a ID da transação:

Clique no ícone ao lado da guia Implantar e, em seguida, clique na guia Implantação e clique na guia Mostrar histórico.

- Ao executar a implantação da política, é necessário coletar a saída dos comandos mencionados:

Do CVP:

implantação de pigtail

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

Do FTD:

implantação de pigtail

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

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

- Colete o arquivo de solução de problemas do FMC e do FTD.

Para gerar um arquivo de solução de problemas, consulte Solução de problemas de procedimentos de geração de arquivos do Firepower.

Para abrir um caso, consulte TAC SR.

Exemplo: Como executar comandos do FMCv.

Faça login no 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:~#
```

Execute os comandos a partir da raiz:

```
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
```

Exemplo: Como executar comandos do FTDv.

Faça login no 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:~#
```

Execute os comandos a partir da raiz:

```
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 interromper os logs, insira CTRL+C.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.