Raccolta dei log per i problemi comuni di Firepower

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Raccolta dei log per i problemi comuni di Firepower](#)
[1. Problema di failover imprevisto FTD](#)
[2. Problema inaccessibile nell'interfaccia utente grafica del CCP](#)
[3. Problema di backup FMC non riuscito](#)
[4. Errore di distribuzione dei criteri](#)

Introduzione

Questo documento descrive i log da raccogliere prima di aprire una richiesta TAC per risolvere i problemi comuni di Firepower.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

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

Raccolta dei log per i problemi comuni di Firepower

1. Problema di failover imprevisto FTD

Informazioni da raccogliere prima di aprire la richiesta TAC per risolvere il problema:

- Nome host e indirizzo IP dell'unità in cui si è verificato l'errore.
- Tutte le modifiche recenti apportate.
- Occorrenza evento: ora dell'evento e fuso orario.
- Connettività del cavo di failover: collegato direttamente a entrambe le unità o a qualsiasi dispositivo intermedio (switch).
- Output comandi richiesti da entrambe le unità:

show tech-support

show failover-history

mostra stato failover

- Registri di sistema per 10 minuti prima e dopo il verificarsi dell'evento.
- Raccogli file di risoluzione dei problemi FTD.

Per generare un file di risoluzione dei problemi, consultare Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower.

Per aprire una richiesta, fare riferimento a TAC SR.

Esempio: come eseguire i comandi da FTDv.

Accedere a 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)

>
>
```

Eseguire i comandi da 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 inaccessibile nell'interfaccia utente grafica del CCP

Informazioni da raccogliere prima di aprire la richiesta TAC per risolvere il problema:

- Tutte le modifiche recenti apportate.
- Output comandi richiesti da FMC SSH:

stato di pmtool | grep-i gui

stato di pmtool | grep -E "Attendi|giù|disabilitato"

free -g

df -h

DBCheck.pl

in alto

- Durante l'accesso all'interfaccia utente di FMC, se viene visualizzato un messaggio di errore, catturare una schermata di tale messaggio.
- Durante l'accesso all'interfaccia utente di FMC, è necessario raccogliere l'output dei comandi indicati:

gui

tail -f /var/log/httpd/httpsd_access_log

tail -f /var/log/httpd/httpsd_error_log

- Raccogli file di risoluzione dei problemi di FMC.

Per generare un file di risoluzione dei problemi, consultare Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower.

Per aprire una richiesta, fare riferimento a TAC SR.

Esempio: come eseguire i comandi da FMCv.

Accedere a 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:~#
```

Eseguire i comandi dalla directory principale:

```
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
```

Per interrompere i registri, immettere CTRL+C.

3. Problema di backup FMC non riuscito

Informazioni da raccogliere prima di aprire la richiesta TAC per risolvere il problema:

- Tutte le modifiche recenti apportate.
- Schermata dei messaggi di errore per l'errore di backup.
- Il backup manuale non riesce o il backup pianificato/automatico non riesce?
- Se il backup pianificato ha esito negativo, raccogliere l'occorrenza dell'evento: Ora e Fuso orario.

- Se il backup manuale non riesce, raccogliere l'output del comando durante il backup manuale:

tail -f /var/log/backup.log

- Raccogli file di risoluzione dei problemi di FMC.

Per generare un file di risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower.

Per aprire una richiesta, fare riferimento a TAC SR.

Esempio: come eseguire i comandi da FMCv.

Accedere a FMC SSH ed eseguire il comando dalla directory principale:

```
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
```

Per interrompere i registri, immettere CTRL+C.

4. Errore di distribuzione dei criteri

- Tutte le modifiche recenti apportate.
- Percentuale di errori di distribuzione dei criteri.
- Dall'interfaccia utente di FMC, acquisire uno screenshot dei messaggi di errore relativi all'errore di distribuzione e trascriverli per raccogliere l'ID della transazione:

Fare clic sull'icona accanto alla scheda Distribuzione, quindi sulla scheda Distribuzione e fare clic sulla scheda Mostra cronologia.

- Durante l'esecuzione della distribuzione dei criteri, è necessario raccogliere l'output dei comandi indicati:

Dal CCP:

distribuzione a spirale

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

Da FTD:

distribuzione a spirale

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

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

- Raccogliere file di risoluzione dei problemi FMC e FTD.

Per generare un file di risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower.

Per aprire una richiesta, fare riferimento a TAC SR.

Esempio: come eseguire i comandi da FMCv.

Accedere a 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:~#
```

Eseguire i comandi dalla directory principale:

```
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
```

Esempio: come eseguire i comandi da FTDv.

Accedere a 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:~#
```

Eseguire i comandi dalla directory principale:

```
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
```

Per interrompere i registri, immettere CTRL+C.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).