

Überprüfung der Bereitschaft oder Upgrade auf Überwachung und Wiederaufnahme für FMC/FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[1. Status der Bereitschaftsprüfung überwachen](#)

[2. Upgrade-Status überwachen](#)

[3. Wiederaufnahme der Bereitschaftsprüfung im Fehlerfall](#)

[4. Upgrade im Fehlerfall fortsetzen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Bereitschaftsprüfung oder das Upgrade für FMC/FTD überwachen und fortsetzen.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

1. Status der Bereitschaftsprüfung überwachen

Nachdem die Bereitschaftsprüfung vom FMC zum FMC oder für das verwaltete Gerät initiiert wurde, können wir den Status der Prüfung über eine andere CLI als über die FMC-GUI validieren. Falls die Bereitschaftsprüfung fehlschlägt, können wir über die CLI im Expertenmodus die

relevanten Protokolle abrufen, um den Grund für den Ausfall zu ermitteln.

Navigieren Sie in den Expertenmodus, und nach der Eskalation in den Root-Account können diese Befehle verwendet werden.

Experte

```
sudo su - (Kennwort eingeben)
```

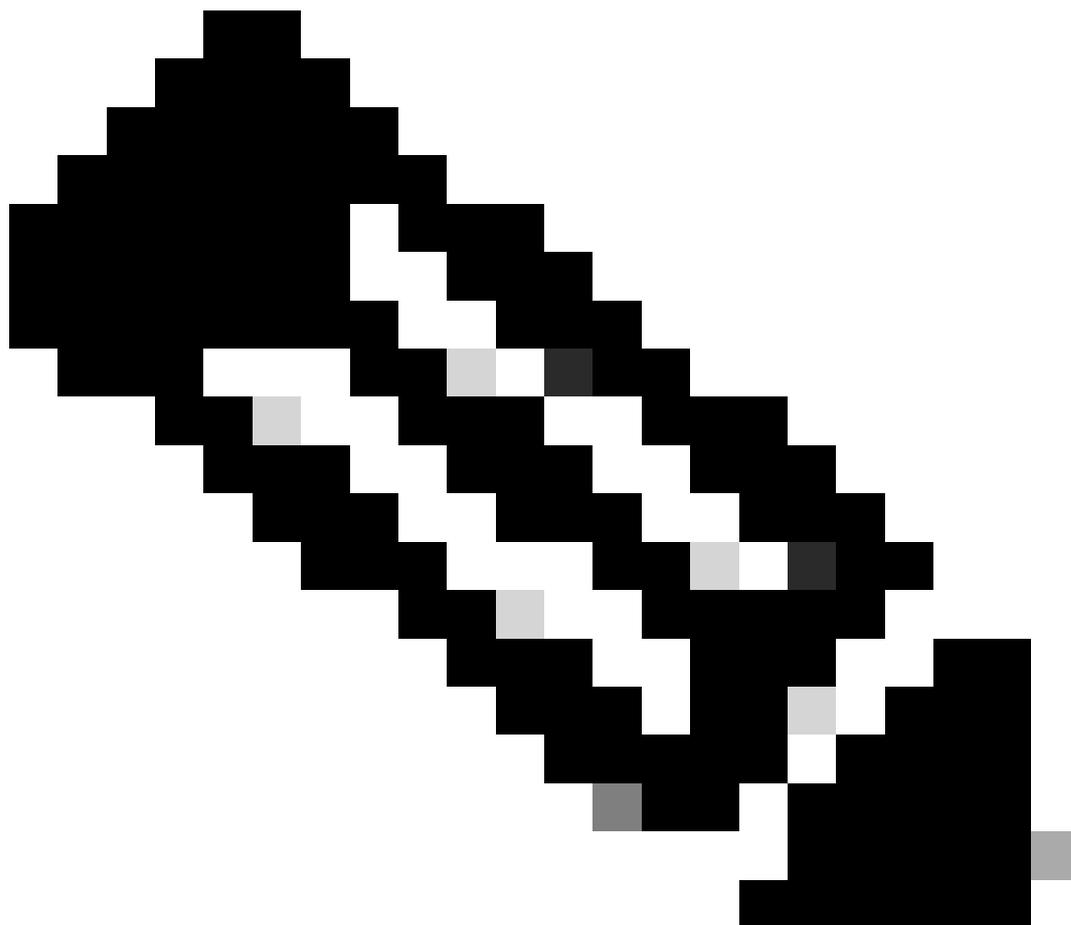
```
cd /var/log/sf
```

```
cd <Upgrade_Dateiname>
```

```
cd upgrade_readiness
```

```
tail -f main_upgrade_script.log
```

Hier ist ein Beispiel für die Befehlsausgabe.



Hinweis: Verwenden Sie das Verzeichnis /ngfw/var/log/sf, während Sie den Status des FTD überprüfen. Die Ausgabedatei zeigt den Status "Success" an.

```
root@fmc:/# cd /var/log/sf
root@fmc:/var/log/sf# cd Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5/
root@fmc:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5#
root@fmc:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5# cd upgrade_readiness/
root@fmc:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5/upgrade_readiness#
root@fmc:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5/upgrade_readiness# tail -f main_upgrade_script.log
[231002 08:06:49:445] SKIP 200_pre/610_lamplighter_010_artifacts_export.sh
[231002 08:06:49:485] SKIP 200_pre/999_enable_sync.sh
[231002 08:06:49:519] MAIN_UPGRADE_SCRIPT_END
[231002 08:06:49:535] Readiness check completed...
[231002 08:06:49:542] Attempting to remove upgrade lock
[231002 08:06:49:543] Success, removed upgrade lock
[231002 08:06:49:545]
[231002 08:06:49:546] #####
[231002 08:06:49:547] # UPGRADE READINESS CHECK COMPLETE status : PASS #
[231002 08:06:49:548] #####
```

Stand der Bereitschaftsprüfung

2. Überwachung des Upgrade-Status

Wenn das Upgrade von FMC auf das FMC oder auf das verwaltete Gerät initiiert wurde, können wir den Status des Upgrades über die CLI validieren. Dies ist nicht mit der FMC-GUI möglich. Falls das Upgrade fehlschlägt, können wir über die CLI im Expertenmodus die relevanten Protokolle abrufen, um den Grund für den Ausfall zu ermitteln.

Navigieren Sie in den Expertenmodus, und nach der Eskalation in den Root-Account können diese Befehle verwendet werden.

expert sudo su - (enter password)

cd /var/log/sf

cd <Upgrade_Dateiname>

tail -f main_upgrade_script.log

tail -f status.log

Hier ist ein Beispiel für die Befehlsausgabe.

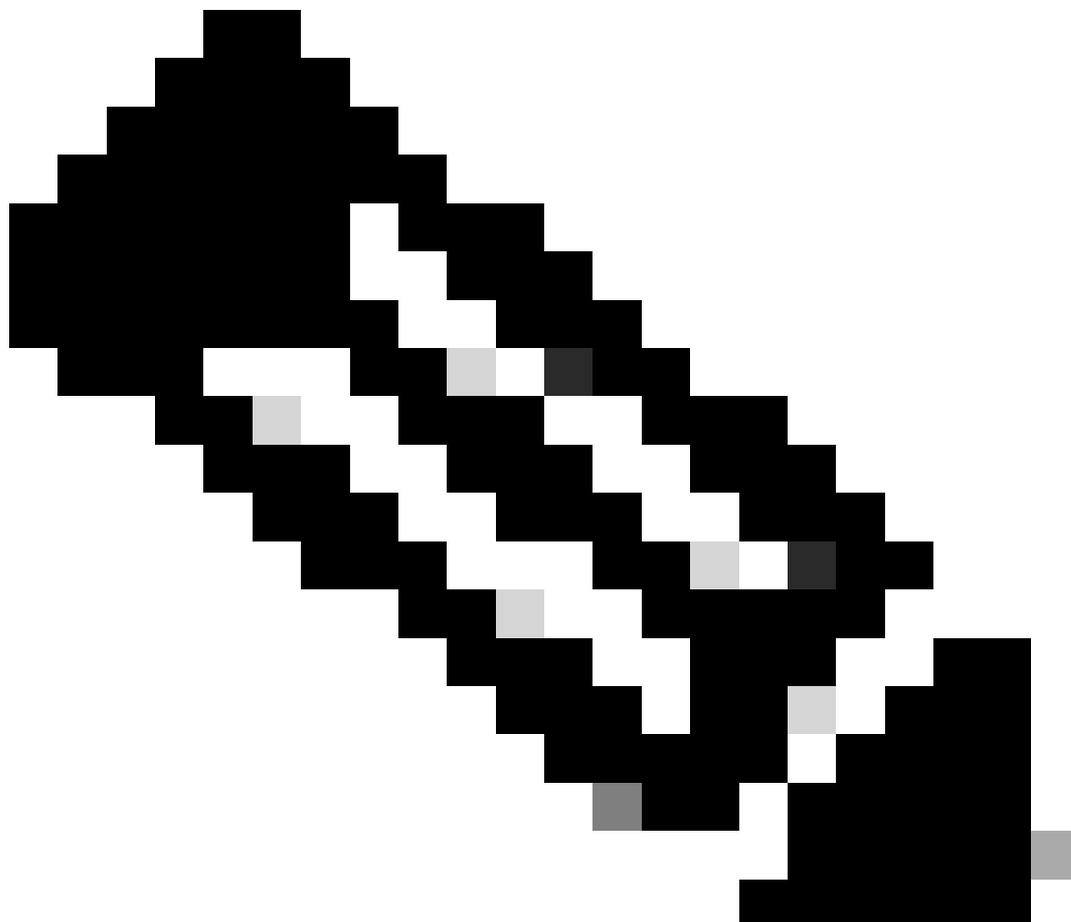
Hinweis: Verwenden Sie das Verzeichnis /ngfw/var/log/sf, während Sie den Status des FTD überprüfen. Die Ausgabedatei zeigt den Status "Abgeschlossen" an.

```
root@fmc:/var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2.5# tail -f status.log
ui:[99%] [1 mins to go for reboot] Running script 999_finish/999_y02_python2_ptn_clean.sh ...
TIMESTAMP:Mon Oct  2 08:55:15 UTC 2023 upgrade exceeded estimated time by 11 minutes
ui:[99%] [1 mins to go for reboot] Running script 999_finish/999_z_must_remain_last_finalize_boot.sh ...
ui:[100%] [1 mins to go for reboot] Running script 999_finish/999_zzz_complete_upgrade_message.sh ...
ui:[100%] [1 mins to go for reboot] Upgrade complete
ui:[100%] [1 mins to go for reboot] The system will now reboot.
ui:System will now reboot.
ui:[100%] [1 mins to go for reboot] Installation completed successfully.
ui:Upgrade has completed.
state:finished
```

Aktualisierungsstatus

3. Wiederaufnahme der Bereitschaftsprüfung im Fehlerfall

Mit diesem Befehl kann das Upgrade für FMC/FTD fortgesetzt werden.



Hinweis: Wenn ein Update fehlschlägt, fahren Sie erst fort, wenn die zugrunde liegende Fehlerursache ermittelt wurde. Andernfalls tritt der Fehler möglicherweise erneut auf.

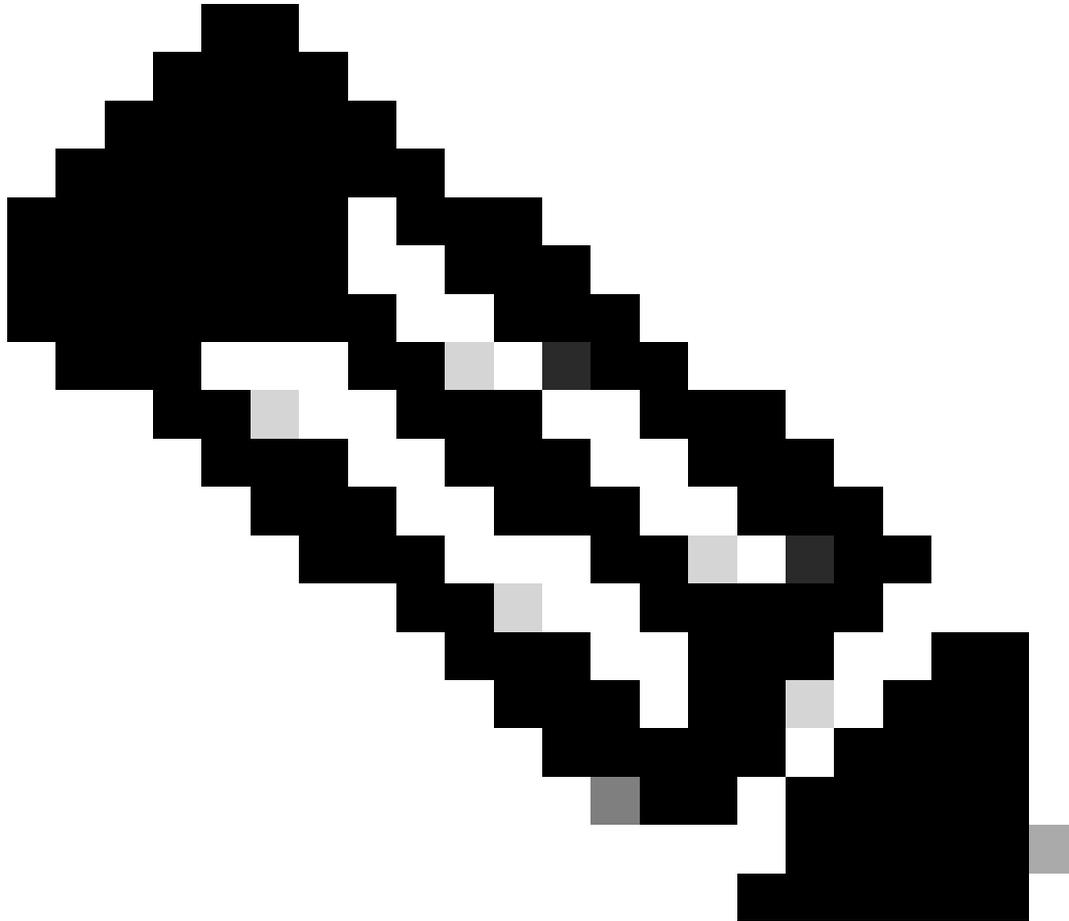
`install_update.pl --detach --readiness-check /var/sf/update/<Name der Upgrade-Datei>`

Hier ist ein Beispiel für die Befehlsausgabe.

`install_update.pl --detach --readiness-check /var/sf/update/ Cisco_FTD_Upgrade-7.0.4-55.sh.REL.tar`

4. Upgrade im Fehlerfall fortsetzen

Mit diesem Befehl kann das Upgrade für FMC/FTD fortgesetzt werden.



Hinweis: Wenn die Bereitschaftsprüfung fehlschlägt, fahren Sie erst fort, wenn die zugrunde liegende Fehlerursache ermittelt wurde. Andernfalls tritt der Fehler möglicherweise erneut auf.

```
install_update.pl --detach --resume /var/sf/updates/<Upgrade_Dateiname>
```

Hier ist ein Beispiel für die Befehlsausgabe.

```
install_update.pl --detach --resume /var/sf/updates/Cisco_FTD_Upgrade-7.0.4-55.sh.REL.tar
```

Durch die Kombination dieser Methoden erhalten Sie einen umfassenden Einblick, wie die Bereitschaftsprüfung und das Upgrade überwacht oder Fehler behoben werden können.

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.