Monitor and Resume Readiness Check or Upgrade for FMC/FTD

Contents

Introduction

This document describes how to monitor and resume the readiness check or upgrade for FMC/FTD

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

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

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

1. Monitoring Readiness Check Status

Once the Readiness Check has been initiated from FMC to the FMC or for the managed device, we can validate the status of the check via CLI other than using FMC GUI. Also, in case if the readiness check fails, we can get the relevant logs to understand the reason for failure through CLI under expert mode.

Navigate to expert mode, and after escalating to root account, these commands can be used.

expert

sudo su - (enter password)

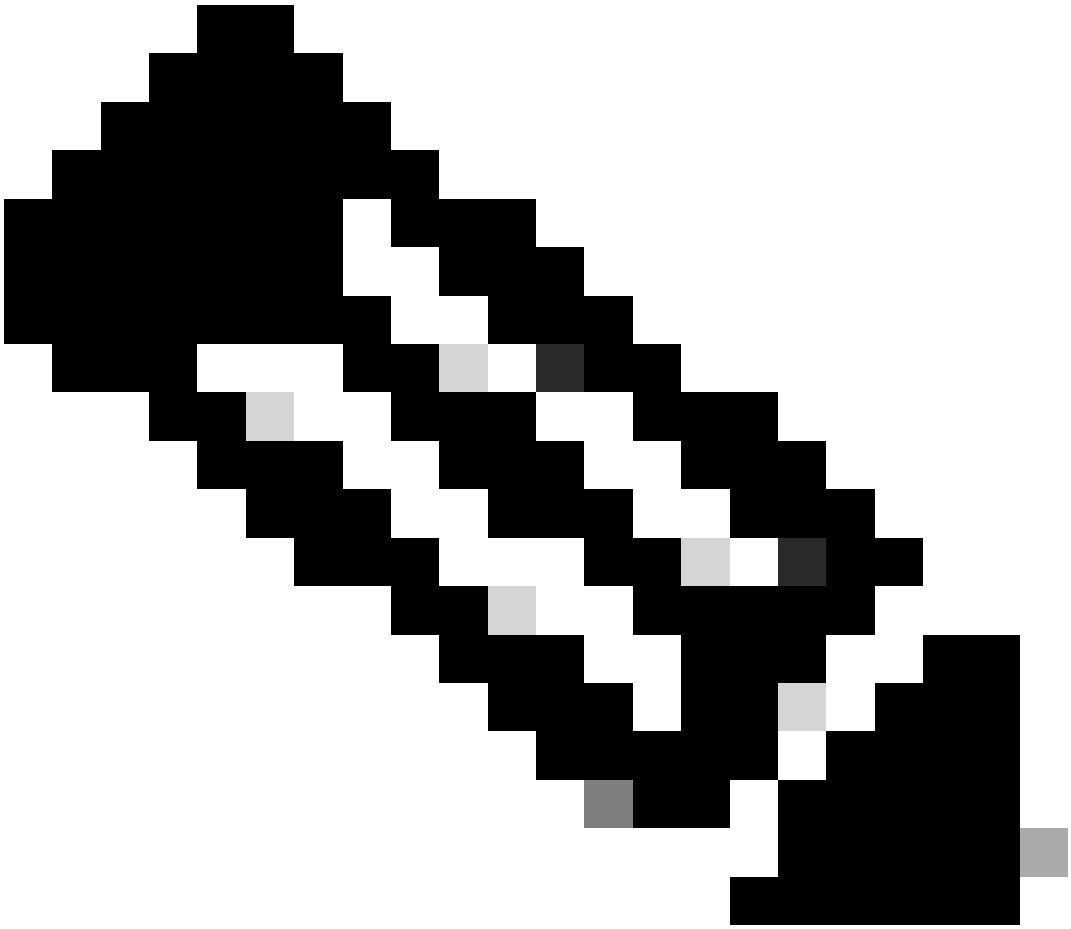
cd /var/log/sf

cd <upgrade_file_name>

cd upgrade_readiness

tail -f main_upgrade_script.log

Here is an example for the command output.



Note: Use /ngfw/var/log/sf directory while checking the status for the FTD. The output file shows the status “Success”.

```
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] ##################################################
```

Readiness check status

2. Monitoring Upgrade Status

When the upgrade has been initiated from FMC to the FMC or for the managed device, we can validate the status of the upgrade via CLI other than using FMC GUI. Also, in case if the upgrade fails, we can get the relevant logs to understand the reason for failure through CLI under expert mode.

Navigate to expert mode, and after escalating to root account, these commands can be used.

expert sudo su - (enter password)

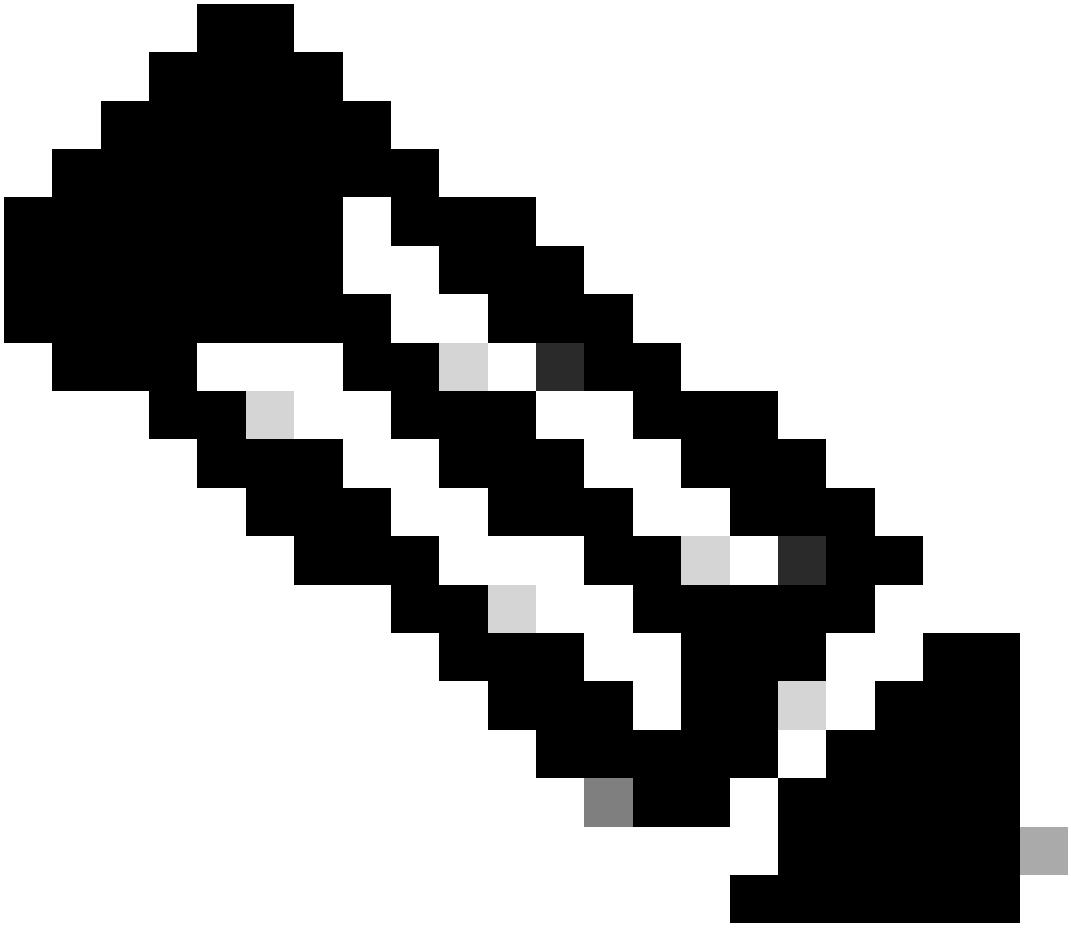
cd /var/log/sf

cd <upgrade_file_name>

tail -f main_upgrade_script.log

tail -f status.log

Here is an example for the command output.



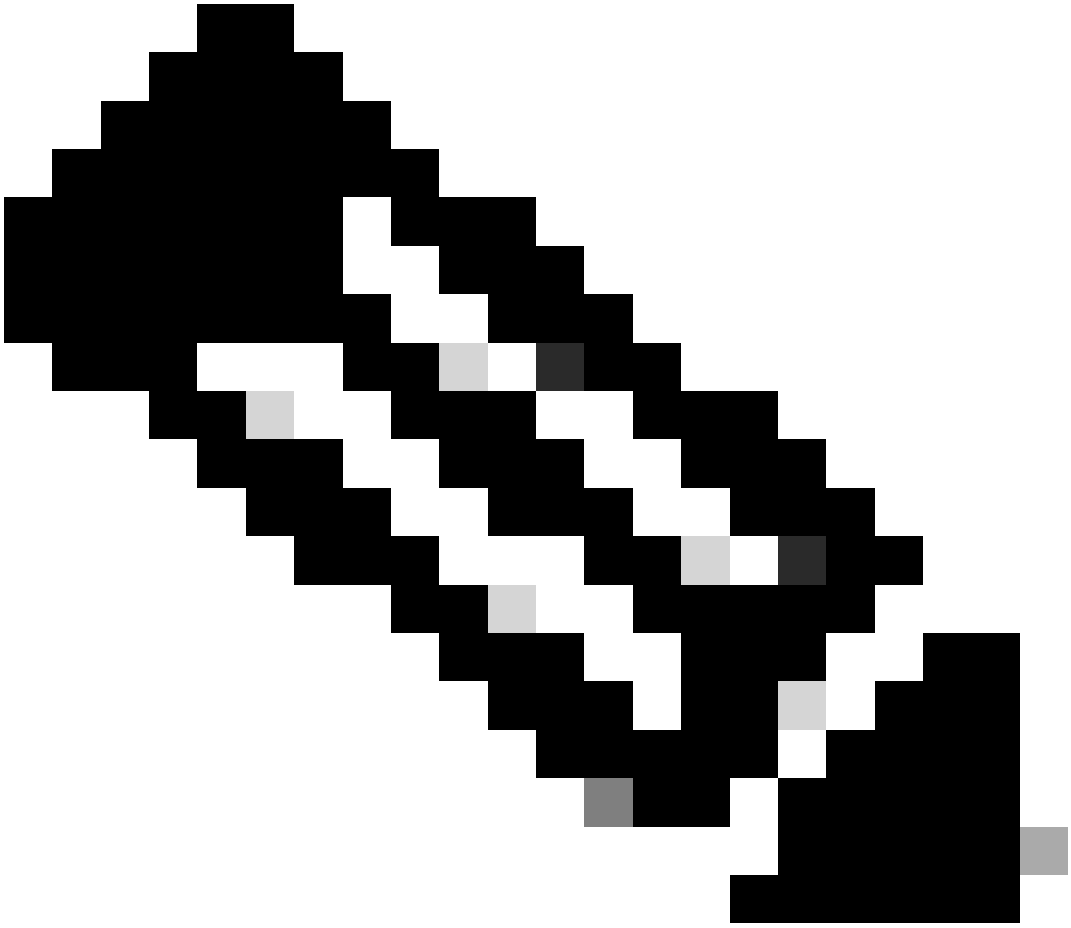
Note: Use /ngfw/var/log/sf directory while checking the status for the FTD. The output file shows the status “Completed”.

```
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_pth_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
```

Upgrade status

3. Resuming Readiness Check In-Case of Failure

This is the command used for resuming upgrade for FMC/FTD.



Note: If an update fails, only resume when the underlying cause of the failure has been identified; otherwise, the same error possibly occurs again.

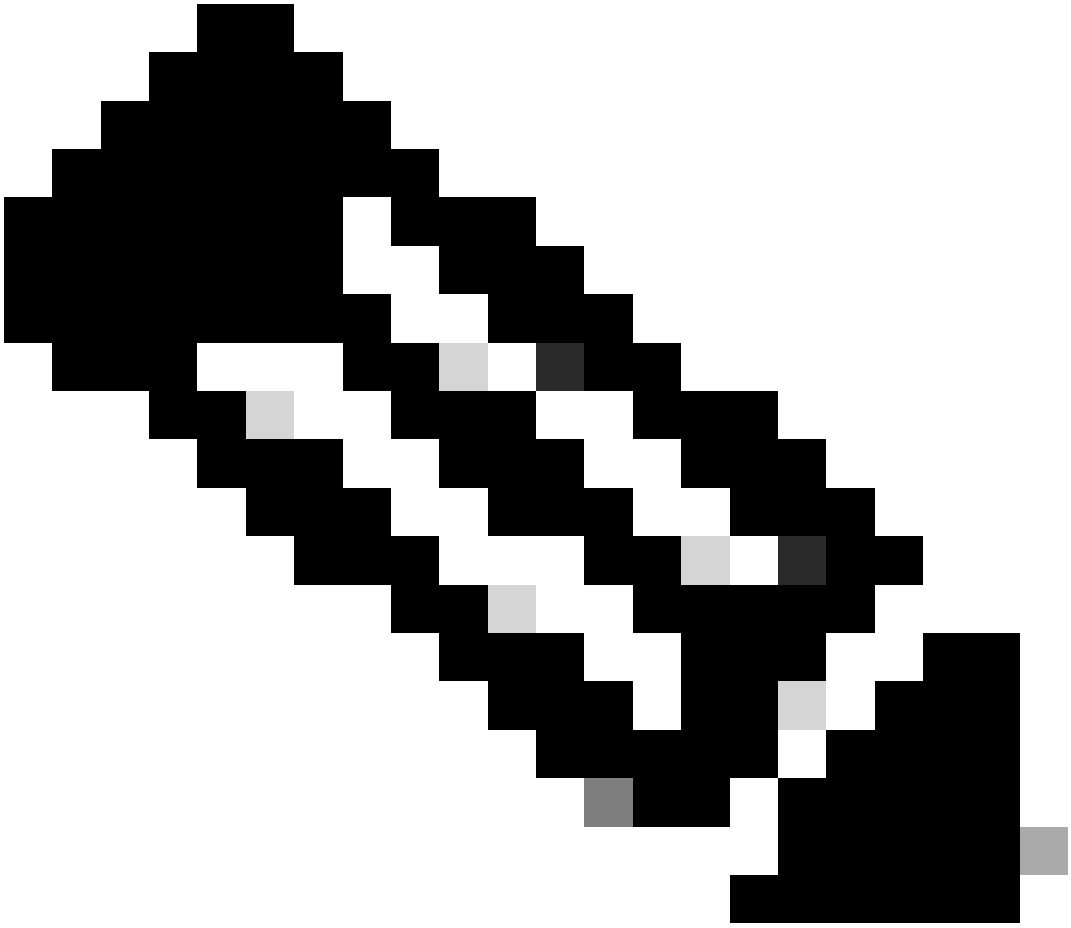
install_update.pl --detach --readiness-check /var/sf/update/<upgrade_file_name>

Here is an example for the command output.

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

4. Resuming Upgrade In-Case of Failure

This is the command used for resuming upgrade for FMC/FTD.



Note: If the readiness check fails, only resume when the underlying cause of the failure has been identified; otherwise, the same error possibly occurs again.

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

Here is an example for the command output.

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

By combining these methods, you can get a comprehensive understanding of how the readiness check and upgrade can be monitored or troubleshoot.