FTD Alertes de coeur de processeur élevé du processus Pruner.pl

Problème

FMC génère fréquemment des alertes d'utilisation élevée du CPU pour plusieurs périphériques FTD gérés, et soulève des préoccupations concernant les performances et la stabilité du pare-feu. Plus précisément, le moniteur d'état FMC montre des pics de coeur de processeur répétés sur des coeurs spécifiques sur des périodes prolongées, avec le processus d'arrière-plan interne Pruner.pl consommant constamment un CPU excessif pour les coeurs spécifiés. Malgré l'apparition de ces alertes CPU critiques dans FMC, aucun impact sur le trafic visible par l'utilisateur n'est observé et la stabilité globale du FTD n'est pas affectée.

Environnement

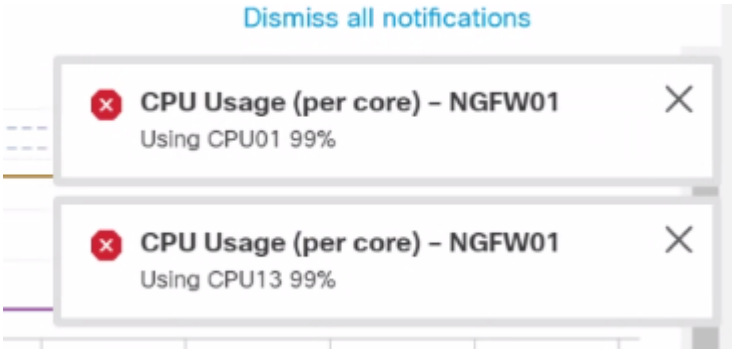
- Version du logiciel FTD : 7.2.5 (affecte les modèles virtuels et matériels dans toutes les versions antérieures à la version 7.2.6)
- Périphériques gérés par Firepower Management Center (FMC)

Résolution

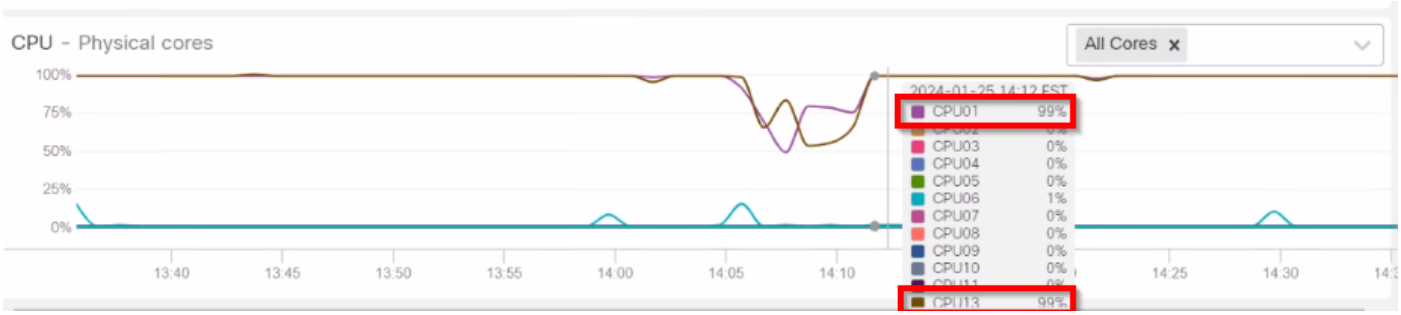
La résolution implique la mise à niveau des périphériques FTD concernés vers une version logicielle qui contient le correctif pour le défaut identifié.

Étapes de dépannage et d'analyse

1: Examinez les modèles d'utilisation du CPU dans les graphiques FTD Health Monitor au fil du temps pour identifier l'étendue et la durée du problème. L'analyse révèle des pics répétés de coeur de processeur sur des coeurs spécifiques se produisant, tandis que l'utilisation globale du processeur et de la mémoire est restée dans des plages de fonctionnement normales.



image_en_ligne_0.png



image_inline_1.png

```
Health Monitor Alert | Time: Mon Jul 24 06:34:20 2023 UTC | Severity: critical | Module: CPU Usage (per
Health Monitor Alert | Time: Mon Jul 24 04:24:20 2023 UTC | Severity: critical | Module: CPU Usage (per
```

2: Analysez l'interface de ligne de commande du FTD et dépannez les offres groupées du FTD affecté pour identifier la cause première d'une utilisation CPU élevée.

3: Passez en revue les données collectées pour identifier les processus qui consomment des ressources CPU excessives. L'analyse des fichiers top.log a confirmé que le processus Pruner.pl utilisait systématiquement un CPU élevé sur certains coeurs, le modèle de problème commençant autour d'un délai spécifique.

```
root@FTDdevice:/home/admin# cd /ngfw/var/log/
root@FTDdevice:/ngfw/var/log# grep "Pruner.pl --persistent" top.log | grep -v "S   0.0"
 12341 root      20   0  458920 437816  10056 R 100.0   0.2   9452:10 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9453:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9454:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R  94.1   0.2   9455:15 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9456:18 /usr/bin/perl /ngfw/usr/local/sf/
```

Les journaux affichent également un nombre élevé de fichiers vides de 0 octet "*snort-unified.log" qui sont la principale raison de l'exécution si fréquente de Pruner.pl.

```
root@FTDdevice:/home/admin# cd /ngfw/var/sf/detection_engines/FTD-UUID/
root@FTDdevice:/ngfw/var/sf/detection_engines/FTD-UUID# ls -l instance-* | grep -ri "root       0.snor
-rw-r--r--  1 root    root        0 Nov 12 19:47 snort-unified.log.1699818430
-rw-r--r--  1 root    root        0 Nov 12 19:41 snort-unified.log.1699818093
-rw-r--r--  1 root    root        0 Nov 12 19:35 snort-unified.log.1699817758
-rw-r--r--  1 root    root        0 Nov 12 17:13 snort-unified.log.1699809226
-rw-r--r--  1 root    root        0 Nov 12 17:08 snort-unified.log.1699808890
-rw-r--r--  1 root    root        0 Nov 12 17:02 snort-unified.log.1699808554
```

Solution de mise à niveau logicielle

1: Mettez à niveau tous les périphériques FTD concernés vers une version logicielle contenant le correctif pour CSCwh79095. Les versions minimales recommandées sont les suivantes :

- FTD 7.2.7 (version de correction minimale dans le train 7.2.x)
- FTD 7.4.1 ou version ultérieure (chemin de mise à niveau recommandé)

2: Après la mise à niveau, surveillez les alertes d'intégrité FMC pour confirmer que :

- L'utilisation du processeur par coeur reste stable
- Aucune nouvelle alarme critique n'est déclenchée pour Pruner.pl ou des processus similaires en arrière-plan
- Les alertes de CPU élevées pour le processus Pruner.pl ne se produisent plus

Prévention et meilleures pratiques

Mettez en oeuvre ces recommandations pour éviter des problèmes similaires :

- Évitez d'exécuter des trains de codes plus anciens à long terme et planifiez des mises à niveau périodiques vers les versions recommandées pour bénéficier des correctifs de bogues et des mises à jour de sécurité
- Avant toute mise à niveau majeure, consultez les notes de version de Cisco et recherchez les bogues sur les versions actuelles et cibles
- Continuer à surveiller les alertes d'état FMC après les mises à niveau pour assurer la stabilité du système
- Examiner toute considération spéciale de mise à niveau documentée dans les notes de version

Motif

Les alertes de CPU élevées sont causées par un défaut logiciel dans FTD 7.2.5 identifié comme ID de bogue Cisco CSCwh79095. Ce défaut est dû à des fichiers snort-unified.log vides de 0 octet, ce qui entraîne la consommation excessive de CPU par le processus d'arrière-plan interne de Pruner.pl sur des coeurs spécifiques. Cela déclenche des alarmes persistantes de CPU élevé dans FMC. Il est important de noter que cette condition n'affecte pas le transfert du trafic du plan de données ou la stabilité globale du périphérique ; il génère uniquement des alertes de CPU critiques dans l'interface de gestion. Le problème est lié à des bogues dupliqués, y compris CSCwe66384 (Pruner.pl et gestionnaire de disque CPU élevé sans problèmes évidents de disque) et CSCwf80946 (FTD : Processus d'élagage utilisant un nombre excessif de coeurs de CPU système et générant des alertes FMC HM).

Autres informations utiles

- ID de bogue Cisco CSCwh79095 - Snort générant un nombre excessif de fichiers journaux unifiés snort avec zéro octet (Correction : 7.2.7, 7.4.1, 7.6.0)
- ID de bogue Cisco CSCwf77994 - Fausses alertes critiques de CPU élevé pour les coeurs de système de périphérique FTD exécutant une utilisation élevée instantanée (Corrigé dans : 7.2.9, 7.4.1, 7.6.0)
- Notes de version FTD/FMC et documentation sur les versions recommandées
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.