Journalisation et surveillance de Punt-Policer ASR1000

Contenu

Introduction

Ce document décrit la fonction de contrôle de ponctualité et quelques modifications apportées à cette fonction pour les routeurs à services d'agrégation Cisco ASR 1000 et ISR G3. Punt-policer est activé par défaut et il règle tout le trafic pointé du plan de contrôle. Si vous voulez en savoir plus sur les suppressions de punt-policer et de punt, reportez-vous à Packet Drops sur les routeurs de service de la gamme Cisco ASR 1000. Récemment, quelques modifications ont été apportées à la journalisation et au fonctionnement de punt-policer, destinées à donner à l'utilisateur CLI commun un mécanisme de journalisation clair pour identifier la raison des abandons de paquets sur le périphérique.

Par interface Punt-Policer

Ceci a été introduit dans Polaris version 16.4.

Cela permet à l'administrateur réseau de configurer les limites de punt-policer par interface. Il est particulièrement utile lorsque vous voulez identifier l'interface qui génère un nombre important de trafic de données, ce qui réduit le temps de dépannage et donne une alternative à la capture de paquets. Avant cette fonctionnalité, si vous aviez besoin de connaître l'interface source du trafic ponctuel, vous deviez effectuer une capture de paquets qui a consommé beaucoup de temps et de ressources.

Configuration et vérification

```
Router(config)#platform punt-intf rate < packet per second>

Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#punt-control enable
```

Cette configuration active la surveillance de la régulation des points par interface. Par exemple, si vous configurez le taux de contrôle de point sur 1 000 globalement ainsi que sur une interface particulière, le périphérique gardera le suivi de la perte de point pour cette interface particulière

pendant 30 secondes. Après l'intervalle de 30 secondes, le routeur affiche un journal comme celui-ci pour alerter l'administrateur qu'il y a eu un événement de violation de punt.

```
*Jun 21 23:01:01.476: %IOSXE-5-PLATFORM:  F1: cpp_cp: QFP:0.1 Thread:076 TS:00000044123616602847
%PUNT_INJECT-5-DROP_PUNT_INTF: punt interface policer drop packet from GigabitEthernet0/0/0
```

30 secondes étant un intervalle important, une commande avec laquelle vous pouvez voir la dernière chute de point pour l'interface a été introduite.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop
latest
Punt Intf Drop Statistics (lastest 1000 dropped packets):

     Interface                         Packets
 ---------------------------------------------
     GigabitEthernet0/0/0              1000
```

Vous pouvez effacer les statistiques de perte afin de surveiller les pertes en temps réel.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop
latest clear
Punt Intf Drop Statistics (lastest 1000 dropped packets):

     Interface                         Packets
 ---------------------------------------------
Router#
```

Journalisation pour Punt-Policer par défaut

En fonction de l'interface, le pointeur de contrôle doit être explicitement configuré. Cependant, sur les périphériques ASR globalement, le punt-policer par cause est toujours actif. Récemment, dans l'image version 16.6.1, la journalisation a été implémentée pour chaque cause punt-policer. À partir de maintenant, un journal sera généré chaque fois qu'une violation de punt par cause se produit.

Àpartir du premier journal, le routeur surveillera la cause des incidents pendant 30 secondes. Si, après 30 secondes, il y a une autre activité de perte, un autre journal est généré.

Le message de journal ressemblerait à ceci et vous voyez donc la goutte pour la cause de punt 60.

```
F1: cpp_cp: QFP:0.1 Thread:035 TS:00000000089593031387 %PUNT_INJECT-5-DROP_PUNT_CAUSE: punt
cause policer drop packet cause 60
```

Vous pouvez vérifier les détails relatifs à la cause de la ponctuation à l'aide de cette commande.

```
BGL14.Q.20-ASR1006-1#show platform hardware qfp active infrastructure punt config cause 60
QFP Punt Table Configuration

Punt table base addr : 0x48F46010
 punt cause index     60
 punt cause name      IP subnet or broadcast packet
 maximum instances    1
 punt table address : 0x48F46100
 instance[0] ptr    : 0x48F46910
   QFP interface handle : 3
```

```
   Interface name       : internal1/0/rp:1
   instance address        : 0x48F46910
   fast failover address   : 0x48F2B884
   Low priority policer    : 70
   High priority policer   : 71
```

En dehors de ce journal, vous pouvez toujours utiliser les anciennes commandes afin de surveiller les pertes de punt.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-drop
Router#show platform hardware qfp active infrastructure punt statistics type per-cause
Router#show platform hardware qfp active infrastructure punt statistics type global-drop
```

Conclusion

Avec l'introduction de la journalisation ponctuelle par cause et de la surveillance ponctuelle par interface, il existe un meilleur outil pour isoler les problèmes liés aux punts. Chaque fois que vous voyez un pointeur tomber dans l'état QFP, vous devez utiliser les outils expliqués afin d'isoler davantage le problème.