Expliquer les erreurs de suppression de paquets dans l'ACI

Table des matières

- Introduction
- Informations générales
- Objets gérés
- Types de compteurs de pertes matérielles
  - Transférer
  - Erreur
  - Tampon
- Affichage des statistiques de rejet dans CLI
  - Objets gérés
  - Compteurs matériels
  - Feuille
  - Colonne Vertébrale
- Défauts
  - F112425 - Taux de paquets abandonnés en entrée (l2IngrPktsAg15min:dropRate)
  - F100264 - Taux de suppression de paquets en entrée dans la mémoire tampon (eqptIngrDropPkts5min:bufferRate)
  - F100696 - Transfert entrant et suppression de paquets (eqptIngrDropPkts5min:forwardingRate)
- Seuil de statistiques
  - Taux de paquets abandonnés en aval dans eqptIngrDropPkts
  - Taux de paquets abandonnés en entrée dans l2IngrPktsAg

Introduction

Ce document décrit chaque type de défaut et la procédure à suivre lorsque vous voyez ce défaut.

Informations générales

Pendant le fonctionnement normal d'un fabric Cisco ACI, l'administrateur peut voir les défaillances de certains types de paquets abandonnés.

Objets gérés

Dans l'ACI Cisco, toutes les pannes sont déclenchées sous Objets gérés (MO). Par exemple, une erreur F11245 - ingress drop packets rate(l2IngrPktsAg15min:dropRate) concerne le paramètre dropRate dans MO l2IngrPktsAg15min.

Cette section présente quelques exemples d'objets gérés (MO) liés aux erreurs de suppression de paquets.

	Exemple	Description	Exemples de paramètres	Échantillon MO Contre Quelles défaillances sont relevées
l2IngrPkts	l2IngrPkts5min l2PaquetsIngr15min l2PaquetsIngénieurs1h etc.	Cela représente les statistiques de paquets entrants par VLAN au cours de chaque période.	dropRate floodRate MulticastRate UnicastRate	vlanCktEp (VLAN)
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d etc.	Cela représente les statistiques de paquets en entrée par EPG, BD, VRF, etc. Par exemple, les statistiques EPG représentent l'agrégation des statistiques VLAN qui appartiennent à l'EPG.	dropRate floodRate MulticastRate UnicastRate	fvAEPg (EPG) fvAp (profil d'application) fvBD (BD) l3extOut (L3OUT)
EqptIngrDropPkts	EqptIngrDropPkts15 min EqptIngrDropPkts1h pqptIngrDropPkts1d etc.	Cela représente les statistiques de paquets de suppression en entrée par interface pendant chaque période.	*1 forwardingRate *1 taux d'erreur *1 bufferRate	l1PhysIf (port physique) pcAggrIf (port-channel)

*1 :Ces compteurs dans eqptIngrDropPkts peuvent être augmentés par erreur en raison d'une limitation ASIC dans plusieurs plates-formes Nexus 9000, parce que les paquets SUP_REDIRECT sont enregistrés comme abandons de transmission. Voir aussi ID de bogue

Cisco CSCvo68407 et ID de bogue Cisco CSCvn72699 pour plus de détails et les versions corrigées.

Types de compteurs de pertes matérielles

Sur les commutateurs Nexus 9000 s'exécutant en mode ACI, il y a 3 compteurs matériels principaux pour la raison de perte d'interface d'entrée sur l'ASIC.

Un dropRate dans l2IngrPkts, l2IngrPktsAg inclut ces compteurs. Trois paramètres (forwardingRate, errorRate, bufferRate) de la table pour eqptIngrDropPkts représentent chacun trois compteurs d'interface.

Transférer

Les abandons vers l'avant sont des paquets qui sont abandonnés sur le bloc de recherche (LU) de l'ASIC. Dans un bloc LU, une décision de transmission de paquet est prise sur la base des informations d'en-tête de paquet. Si la décision est d'abandonner le paquet, la fonction Forward Drop est comptabilisée. Il y a plusieurs raisons pour lesquelles cela peut se produire. Les principales sont les suivantes :

REFUS_GROUPE_SÉCURITÉ

Une perte en raison de contrats manquants pour autoriser la communication.

Lorsqu'un paquet entre dans le fabric, le commutateur examine l'EPG source et de destination pour voir s'il existe un contrat autorisant cette communication. Si la source et la destination se trouvent dans des groupes de terminaux différents et qu'aucun contrat n'autorise ce type de paquet entre eux, le commutateur abandonne le paquet et l'étiquette comme SECURITY_GROUP_DENY. Le compteur Forward Drop est incrémenté.

VLAN_XLATE_MISS

Une perte en raison d'un VLAN inapproprié.

Lorsqu'un paquet entre dans le fabric, le commutateur le consulte pour déterminer si la configuration du port autorise ce paquet. Par exemple, une trame entre dans le fabric avec une étiquette 802.1Q de 10. Si le commutateur a le VLAN 10 sur le port, il

inspecte le contenu et prend une décision de transfert basée sur l’adresse MAC de destination. Cependant, si le VLAN 10 n'est pas sur le port, il l'abandonne et l'étiquette comme VLAN_XLATE_MISS. Le compteur Forward Drop est incrémenté.

La raison pour XLATE ou Translate est que dans l'ACI, le commutateur leaf prend une trame avec un encapsulage 802.1Q et la traduit en un nouveau VLAN qui est utilisé pour VXLAN et d'autres normalisations à l'intérieur du fabric. Si la trame arrive avec un VLAN non déployé, la traduction échoue.

ACL_DROP

Une chute à cause de sup-tcam.

sup-tcam dans les commutateurs ACI contient des règles spéciales à appliquer en plus de la décision de transfert L2/L3 normale. Les règles de sup-tcam sont intégrées et ne sont pas configurables par l'utilisateur. L'objectif des règles sup-tcam est principalement de traiter certaines exceptions ou une partie du trafic du plan de contrôle et non destiné à être contrôlé ou surveillé par les utilisateurs. Lorsque le paquet atteint les règles sup-tcam et que la règle est d'abandonner le paquet, le paquet abandonné est compté comme ACL_DROP et il incrémente le compteur Forward Drop. Lorsque cela se produit, cela signifie généralement que le paquet est sur le point d'être transféré vers les principaux de transfert ACI de base.

Même si le nom d'abandon est ACL_DROP, cette liste de contrôle d'accès n'est pas la même que la liste de contrôle d'accès normale qui peut être configurée sur des périphériques NX-OS autonomes ou tout autre périphérique de routage/commutation.

SUP_REDIRECTION

Ce n'est pas une goutte.

Un paquet redirigé vers le sup (par exemple, CDP/LLDP/UDLD/BFD, etc.) peut être compté comme Forward Drop même si le paquet est correctement traité et transféré vers le CPU.

Cela est dû à la limitation de la mise en oeuvre de l'ASIC avec les commutateurs ACI N9k basés sur l'évolutivité du cloud (EX/FX/FX2/FX3/GX/GX2).

Erreur

Lorsque le commutateur reçoit une trame non valide sur l'une des interfaces du panneau avant, elle est abandonnée en tant qu'erreur. Les trames avec des erreurs FCS ou CRC en sont des exemples. Lorsque vous examinez les ports leaf de liaison ascendante/descendante ou les ports Spine, il est préférable de vérifier les erreurs FCS/CRC à l'aide de la commande show interface. Cependant, dans des conditions de fonctionnement normales, il est prévu que les paquets d'erreur s'incrémentent sur les ports de liaison ascendante/descendante des ports leaf ou Spine, car ce compteur inclut également les trames qui sont élaguées par le système et qui ne sont pas censées être envoyées hors de l'interface.

Exemple : Défaillances de durée de vie pour les paquets routés, même interface de diffusion/trames diffusées.

Tampon

Lorsque le commutateur reçoit une trame et qu'aucun crédit de mémoire tampon n'est disponible pour l'entrée ou la sortie, la trame peut être abandonnée avec la mémoire tampon. Cela indique généralement une congestion quelque part dans le réseau. La liaison qui affiche la défaillance peut être pleine ou la liaison contenant la destination peut être encombrée.

Affichage des statistiques de rejet dans CLI

Objets gérés

Secure Shell (SSH) à l'un des APIC et exécutez ces commandes.

```
apic1# moquery -c l2IngrPktsAg15min
```

Cela fournit toutes les instances d'objet pour cette classe l2IngrPktsAg15min.

Voici un exemple avec un filtre pour interroger un objet spécifique. Dans cet exemple, le filtre doit afficher uniquement un objet avec les attributs dn qui inclut tn-TENANT1/ap-APP1/epg-EPG1.

De plus, cet exemple utilise egrep pour afficher uniquement les attributs requis.

Exemple de sortie 1 : Objet compteur EPG (l2IngrPktsAg15min) du locataire TENANT1, profil d'application APP1, epg EPG1.

```
apic1# moquery -c l2IngrPktsAg15min -f 'l2.IngrPktsAg15min.dn*"tn-TENANT1/ap-APP1/epg-EPG1"' | egrep 'd

dn               : uni/tn-TENANT1/ap-APP1/epg-EPG1/CDl2IngrPktsAg15min
dropPer          : 30                              <--- number of drop packet in the current periodic i
dropRate         : 0.050000                        <--- drop packet rate = dropPer(30) / periodic inter
repIntvEnd       : 2017-03-03T15:39:59.181-08:00   <--- periodic interval = repIntvEnd - repIntvStart
repIntvStart     : 2017-03-03T15:29:58.016-08:00                          = 15:39 - 15:29
                                                                          = 10 min = 600 sec
```

Vous pouvez également utiliser une autre option -d au lieu de -c pour obtenir un objet spécifique si vous connaissez l'objet dn.

Exemple de sortie 2 : Objet compteur EPG (l2IngrPktsAg15min) du locataire TENANT1, profil d'application APP1, epg EPG2.

```
apic1# moquery -d uni/tn-TENANT1/ap-APP1/epg-EPG2/CDl2IngrPktsAg15min | egrep 'dn|drop[P,R]|rep'
dn               : uni/tn-jw1/BD-jw1/CDl2IngrPktsAg15min
dropPer          : 30
dropRate         : 0.050000
repIntvEnd       : 2017-03-03T15:54:58.021-08:00
repIntvStart     : 2017-03-03T15:44:58.020-08:00
```

Compteurs matériels

Si vous voyez des erreurs ou si vous souhaitez vérifier les pertes de paquets sur les ports de commutation à l'aide de l'interface de ligne de commande, la meilleure façon de le faire est d'afficher les compteurs de plate-forme dans le matériel. La plupart des compteurs, mais pas tous, sont affichés à l'aide de la commande show interface. Les 3 principales raisons de perte ne peuvent être visualisées qu'à l'aide des compteurs de la plate-forme. Pour les afficher, procédez comme suit :

Feuille

Établissez une connexion SSH avec le leaf et exécutez ces commandes.

ACI-LEAF# vsh_lc
module-1# show platform internal counters port <X>
* où X représente le numéro de port

Exemple de résultat pour ethernet 1/31 :

<#root>

```
ACI-LEAF#

vsh_lc

vsh_lc
module-1#
module-1#

show platform internal counters port 31

Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                         Output
                                Packets       Bytes           Packets    Bytes
eth-1/31    31  Total          400719   286628225      2302918    463380330
                Unicast        306610   269471065       453831     40294786
                Multicast           0           0      1849091    423087288
                Flood           56783     8427482            0            0
              Total Drops       37327                        0
                Buffer              0                        0
                Error               0                        0
                Forward         37327
                LB                  0
                AFD RED                                      0
                    ----- snip -----
```

Colonne Vertébrale

Pour une colonne vertébrale de type boîte (N9K-C9336PQ), elle est exactement identique à Leaf.

Pour les modules Spine (N9K-C9504 et ainsi de suite), vous devez d'abord fixer la carte de ligne spécifique avant de pouvoir afficher les compteurs de la plate-forme. Établissez une connexion SSH avec la colonne vertébrale et exécutez les commandes suivantes :

ACI-SPINE# vsh

ACI-SPINE# module de connexion <X>

module-2# show platform internal counters port <Y>.

* où X représente le numéro de module de la carte de ligne que vous souhaitez afficher

Y représente le numéro de port

Exemple de résultat pour Ethernet 2/1 :

<#root>

```
ACI-SPINE#

vsh

Cisco iNX-OS Debug Shell
This shell can only be used for internal commands and exists
for legacy reasons. User can use ibash infrastructure as this
can be deprecated.
ACI-SPINE#
ACI-SPINE#

attach module 2

Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Last login: Mon Feb 27 18:47:13 UTC 2017 from sup01-ins on pts/1
No directory, logging in with HOME=/
Bad terminal type: "xterm-256color". can assume vt100.
module-2#
module-2#

show platform internal counters port 1

Stats for port 1
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-2/1      1  Total        85632884  32811563575     126611414   25868913406
                  Unicast   81449096  32273734109     104024872   23037696345
                  Multicast  3759719   487617769     22586542   2831217061
                  Flood            0           0            0            0
               Total Drops         0                        0


Buffer           0

                       0


Error            0

                       0


Forward          0

                  LB               0
                  AFD RED                                  0
                       ----- snip -----
```

Défauts

F112425 - Taux de paquets abandonnés en entrée (l2IngrPktsAg15min:dropRate)

Description:

Une des raisons courantes de cette erreur est que les paquets de couche 2 sont abandonnés avec la raison Forward Drop. Il y a plusieurs raisons, mais la plus courante est :

Sur certaines plates-formes (voir l'ID de bogue Cisco CSCvo68407), il y a une limitation où les paquets L2 qui doivent être redirigés vers le CPU (par exemple, CDP/LLDP/UDLD/BFD, etc.), sont enregistrés comme un Forward Drop et sont copiés vers le CPU. Cela est dû à une limitation de l'ASIC utilisé dans ces modèles.

Résolution :

Les gouttes décrites sont purement cosmétiques. La meilleure pratique consiste donc à augmenter le seuil de défaillance, comme indiqué dans la section Seuil d'état. Pour ce faire, reportez-vous aux instructions de la section Stats Threshold.

F100264 - Taux de suppression de paquets en entrée dans la mémoire tampon (eqptIngrDropPkts5min:bufferRate)

Description:

Cette erreur peut s'incrémenter lorsque des paquets sont abandonnés sur un port avec la raison Buffer. Comme mentionné précédemment, cela se produit généralement en cas d’encombrement sur une interface dans le sens de l’entrée ou de la sortie.

Résolution :

Cette erreur représente les paquets réellement abandonnés dans l'environnement en raison d'un encombrement. Les paquets abandonnés peuvent entraîner des problèmes avec les applications exécutées dans le fabric ACI. Les administrateurs réseau peuvent

isoler le flux de paquets et déterminer si l'encombrement est dû à des flux de trafic inattendus, à un équilibrage de charge inefficace, etc., ou à une utilisation attendue sur ces ports.

F100696 - Transfert entrant et suppression de paquets (eqptIngrDropPkts5min:forwardingRate)

Remarque : Une limitation ASIC telle que mentionnée précédemment pour F11245 peut également provoquer l'élévation de ces défauts. Veuillez consulter l'ID de bogue Cisco CSCvo68407 pour plus de détails.

Cette erreur est causée par quelques scénarios. Le plus courant est :

Description 1 - Gouttes vertébrales

Si cette erreur se produit sur une interface Spine, elle peut être due au trafic vers un point d'extrémité inconnu. Lorsqu'un paquet ARP ou IP est transféré au point d'extrémité pour une recherche de proxy et que le point d'extrémité est inconnu dans le fabric, un paquet de glanage spécial est généré et envoyé à toutes les leafs sur l'adresse de groupe de multidiffusion BD (interne) appropriée. Cela déclenche une requête ARP de chaque noeud leaf dans le domaine de pont (BD) pour découvrir le point de terminaison. En raison d'une limitation, le paquet glane reçu par le leaf est également réfléchi à nouveau dans le fabric et déclenche une perte de transmission sur la liaison spine connectée au leaf. Dans ce scénario, le transfert direct n'est incrémenté que sur le matériel Spine de génération 1.

Résolution 1

Comme il est connu que le problème est causé par un périphérique qui envoie une quantité inutile de trafic de monodiffusion inconnu dans le fabric ACI, il est nécessaire de déterminer quel périphérique est à l'origine de ce problème et de voir s'il peut être évité. Cela est généralement dû aux périphériques qui recherchent des adresses IP sur les sous-réseaux à des fins de surveillance. Afin de trouver quel IP envoie ce trafic, SSH sur le leaf qui est connecté à l'interface spine montrant la panne.

À partir de là, vous pouvez exécuter cette commande pour voir l'adresse IP source (sip) qui déclenche le paquet glane :

<#root>

```
ACI-LEAF# show ip arp internal event-history event | grep glean | grep sip | more
```

```
    [116] TID 11304:arp_handle_inband_glean:3035:
```

log_collect_arp_glean

```
;sip =
```

192.168.21.150

```
;dip =
```

192.168.20.100

```
;info = Received glean packet is an IP packet
    [116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip = 192.
```

Dans cet exemple de sortie, le paquet glane est déclenché par 192.168.21.150 et il est recommandé de voir si cela peut être atténué.

Description 2 - Gouttes de feuilles

Si cette erreur est détectée sur une interface leaf, la cause la plus probable est due aux abandons SECURITY_GROUP_DENY mentionnés.

Résolution 2

Le leaf ACI conserve un journal des paquets refusés en raison de violations. Ce journal ne les capture pas toutes pour protéger les ressources CPU, cependant, il vous fournit toujours une grande quantité de journaux.

Pour obtenir les journaux requis, si l'interface sur laquelle l'erreur est déclenchée fait partie d'un port-channel, il est nécessaire d'utiliser cette commande et grep pour le port-channel. Sinon, l'interface physique peut être saisie.

Ce journal peut être rapidement inversé en fonction de la quantité de pertes de contrat.

<#root>

```
ACI-LEAF# show logging ip access-list internal packet-log deny | grep port-channel2 | more
[ Sun Feb 19 14:16:12 2017 503637 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-Id: 59,
```

SIP: 192.168.21.150, DIP: 192.168.20.3

```
, SPort: 0, DPort: 0,
```

Src Intf: port-channel2

,

Pr
oto: 1

, PktLen: 98
[Sun Feb 19 14:16:12 2017 502547 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-Id: 59,
oto: 1, PktLen: 98

Dans ce cas, 192.168.21.150 tente d'envoyer des messages ICMP (numéro de protocole IP 1) à 192.168.20.3. Cependant, il n'existe aucun contrat entre les 2 groupes de terminaux qui autorise le protocole ICMP, de sorte que le paquet est abandonné. Si le protocole ICMP est censé être autorisé, un contrat peut être ajouté entre les deux groupes de terminaux.

Seuil de statistiques

Cette section décrit comment modifier un seuil pour un objet de statistiques qui pourrait potentiellement déclencher une erreur par rapport à un compteur d'abandon.

Un seuil pour les statistiques de chaque objet (par exemple, l2IngrPkts, eqptIngrDropPkts) est configuré par le biais de la stratégie de surveillance par rapport à une variété d'objets.

Comme indiqué dans le tableau au début, eqptIngrDropPkts est surveillé sous, par exemple, les objets l1PhysIf via la stratégie de surveillance.

Taux de paquets abandonnés en aval dans eqptIngrDropPkts

Il y a deux parties pour cela.

+ Politiques d'accès (ports vers les périphériques externes). Également appelés ports du panneau avant).

+ Politiques de fabric (ports entre LEAF et SPINE. Également appelés ports de fabric).

Front Panel Ports (ports towards external devices)



Fabric Ports (ports between LEAF and SPINE)



Chaque objet de port (l1PhysIf, pcAggrIf) peut se voir attribuer sa propre stratégie de surveillance via le groupe de stratégies d'interface, comme illustré dans l'image précédente.

Par défaut, il existe une stratégie de surveillance par défaut sous Fabric > Access Policies et Fabric > Fabric Policies dans l'interface utilisateur graphique du contrôleur APIC. Ces stratégies de surveillance par défaut sont attribuées à tous les ports, respectivement. La stratégie de surveillance par défaut sous Stratégies d'accès est pour les ports du panneau avant et la stratégie de surveillance par défaut sous Stratégies de fabric est pour les ports de fabric.

À moins qu'il ne soit nécessaire de modifier les seuils par port, la stratégie de surveillance par défaut de chaque section peut être modifiée directement pour appliquer la modification à tous les ports du panneau avant et/ou à tous les ports de fabric.

Cet exemple montre comment modifier les seuils de l'abandon du transfert dans eqptIngrDropPkts sur les ports de fabric (stratégies de fabric). Effectuez la même opération sous Fabric > Access Policies pour les ports du panneau avant.

1. Accédez à Fabric > Politiques de fabric>Politiques de surveillance.

2. Cliquez avec le bouton droit et sélectionnez Créer une stratégie de surveillance.

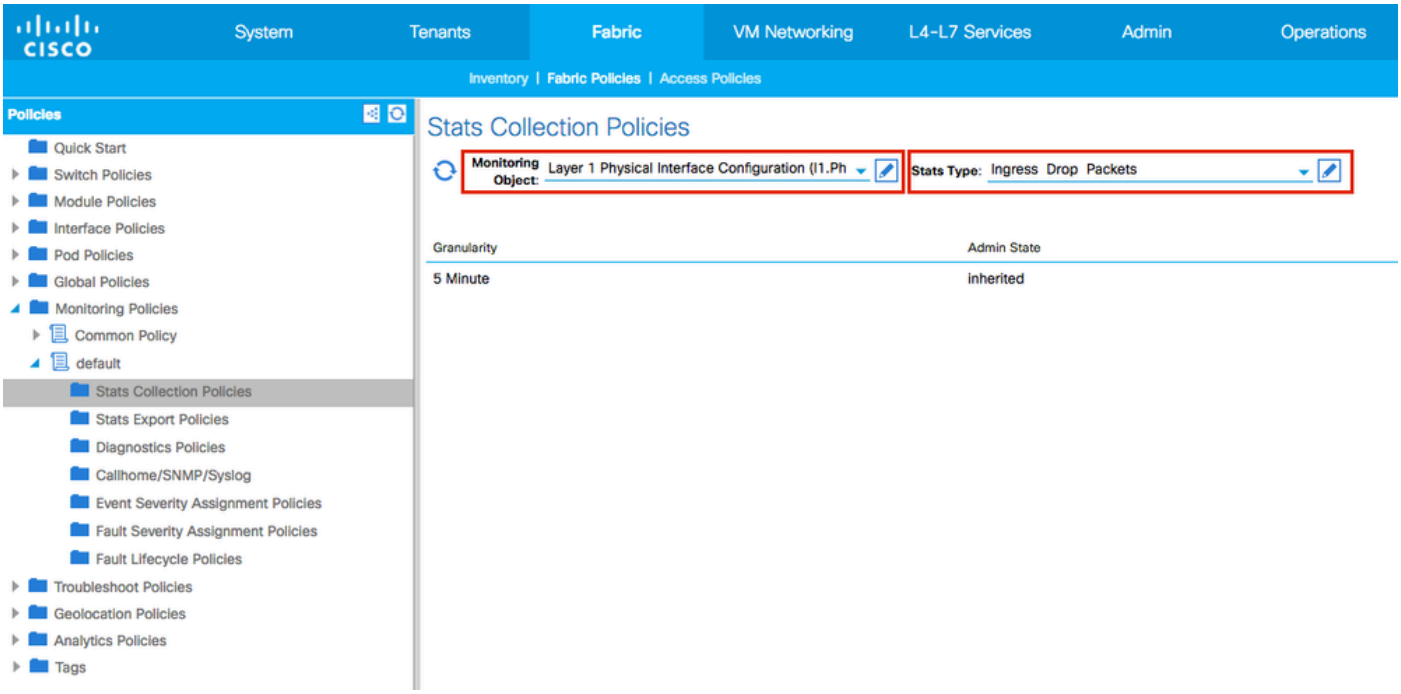
(Si le changement de seuil peut être appliqué à tous les ports du fabric, naviguez jusqu'à la valeur par défaut au lieu d'en créer un nouveau.)

3. Développez la nouvelle stratégie de surveillance ou par défaut et accédez à Stratégies de collecte de statistiques.

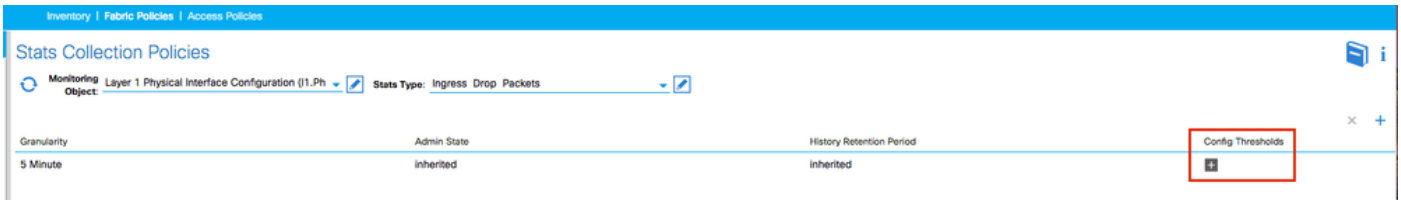
4. Cliquez sur l'icône en forme de crayon pour l'objet de surveillance dans le volet droit, puis sélectionnez Configuration de l'interface physique de couche 1 (l1.PhysIf).

(L'étape 4 peut être ignorée lorsque la stratégie par défaut est utilisée.)

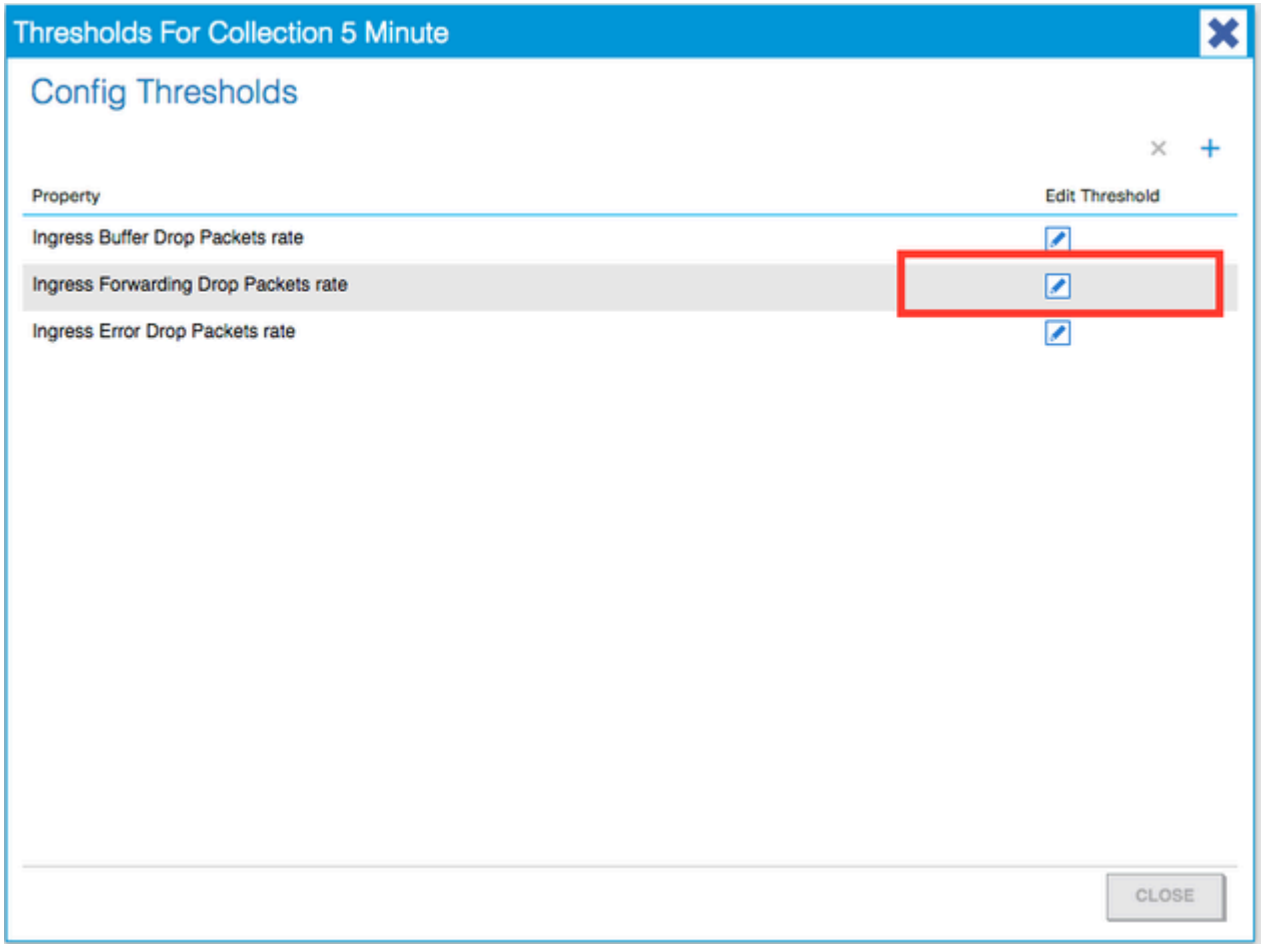
5. Dans la liste déroulante Objet de surveillance du volet de droite, sélectionnez Configuration de l'interface physique de couche 1 (l1.PhysIf) et Type d'état, sélectionnez Abandonner les paquets entrants.



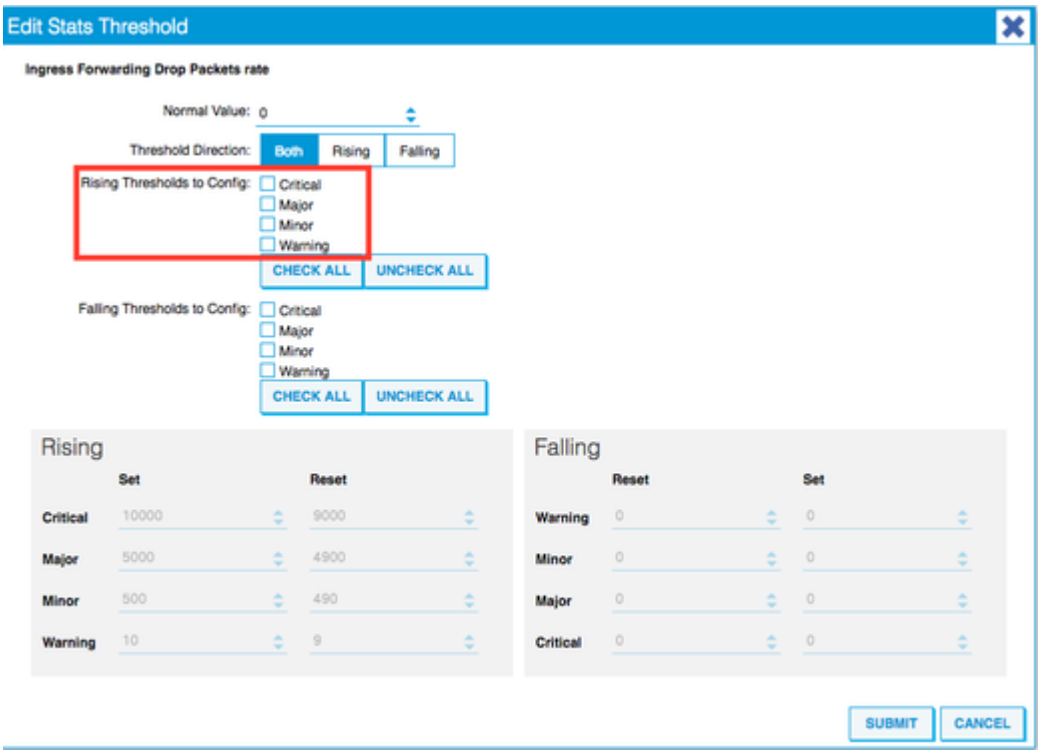
6. Cliquez sur le signe + en regard de Seuils de configuration.



7. Modifiez le seuil de perte de transfert.

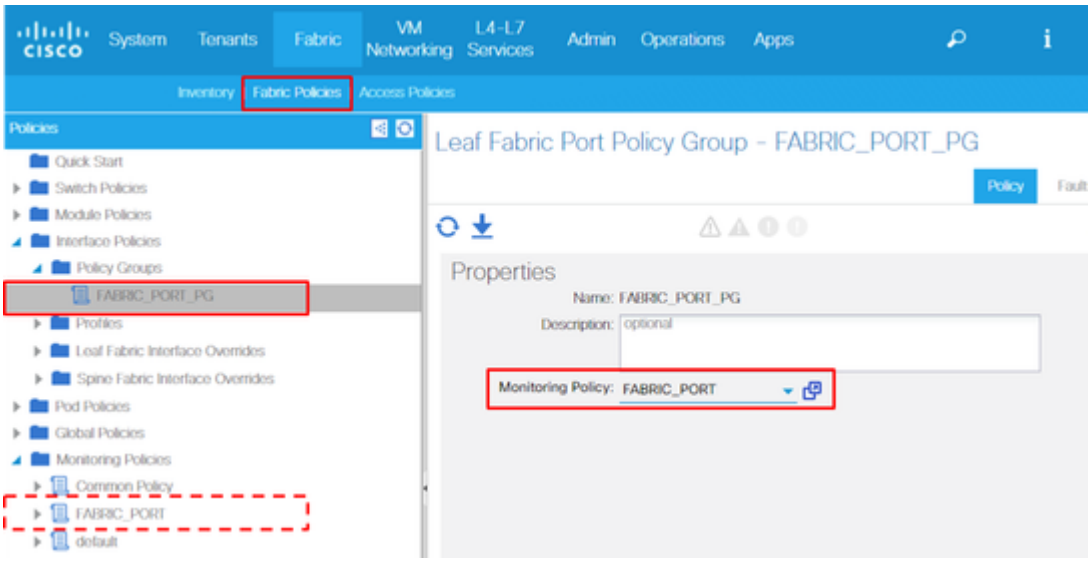


8. Il est recommandé de désactiver les seuils croissants à configurer pour le taux de perte critique, majeur, mineur et d'avertissement pour le transfert.



9. Appliquez cette nouvelle stratégie de surveillance au groupe de stratégies d'interface pour les ports requis. N'oubliez pas de configurer le profil d'interface, le profil de commutateur, etc. dans les politiques de fabric en conséquence.

(L'étape 9 peut être ignorée lorsque la stratégie par défaut est utilisée.)

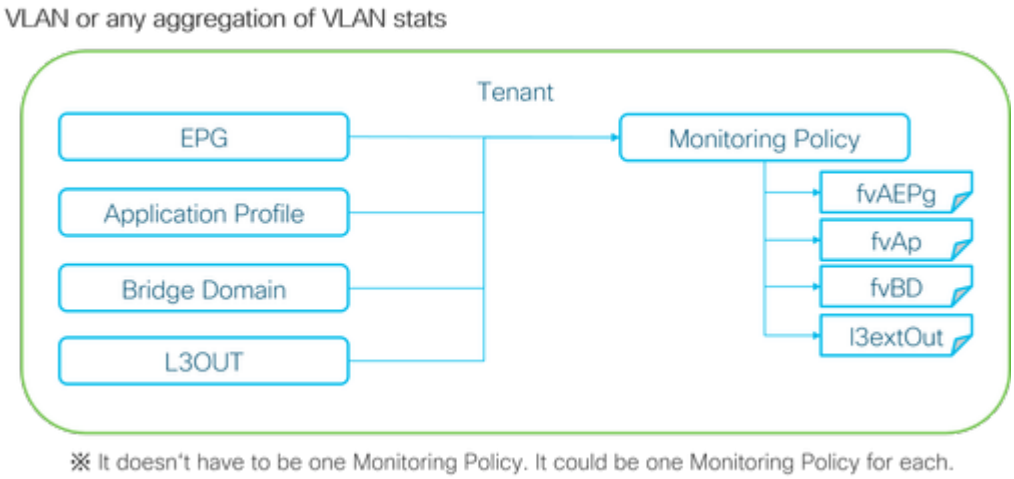


10. Si c'est le cas pour les ports du panneau avant (stratégies d'accès), effectuez la même chose pour l'interface agrégée (pc.Aggrlf) que pour la configuration d'interface physique de couche 1 (l1.Physlf) afin que cette nouvelle stratégie de surveillance puisse être appliquée au port-channel ainsi qu'au port physique.

(L'étape 10 peut être ignorée lorsque la stratégie par défaut est utilisée.)

Taux de paquets abandonnés en entrée dans l2IngrPktsAg

Il y a plusieurs parties pour cela.



Comme le montre l'image précédente, l2IngrPktsAg est surveillé sous de nombreux objets. Cette image ne montre que quelques exemples, mais pas tous les objets pour l2IngrPktsAg. Cependant, le seuil des statistiques est configuré via la stratégie de surveillance ainsi que par eqptIngrDropPkts sous l1PhysIf ou pcAggrIf.

Chaque objet (EPG(fvAEPg), domaine de pont(fvBD), etc.) peut se voir attribuer sa propre stratégie de surveillance, comme illustré ci-dessus.

Par défaut, tous ces objets sous le locataire utilisent la stratégie de surveillance par défaut sous Locataire > commun > Stratégies de surveillance > par défaut, sauf s'ils sont configurés autrement.

À moins qu'il ne soit nécessaire de modifier les seuils pour chaque composant, la stratégie de surveillance par défaut sous locataire commun peut être directement modifiée pour appliquer la modification à tous les composants associés.

Cet exemple permet de modifier les seuils du taux de paquets abandonnés en entrée dans l2IngrPktsAg15min sur le domaine Bridge.

1. Accédez à Locant > (nom du locataire) > Monitoring Policies.

(le locataire doit être commun si la stratégie de surveillance par défaut est utilisée ou si la

nouvelle stratégie de surveillance doit être appliquée entre les locataires)

2. Cliquez avec le bouton droit et sélectionnez Créer une stratégie de surveillance.

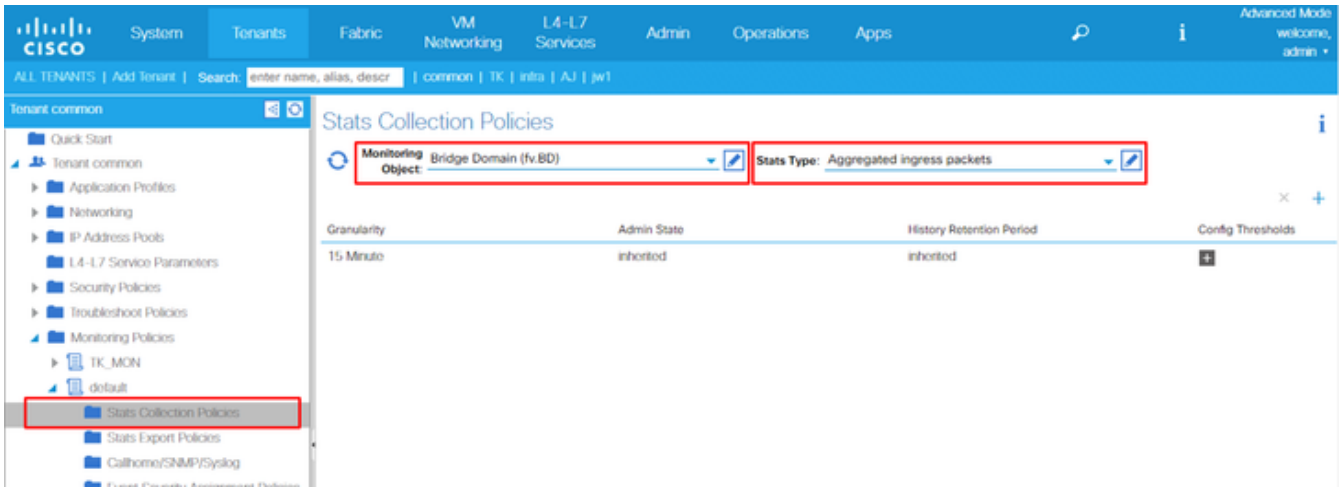
(Si le changement de seuil peut être appliqué à tous les composants, naviguez jusqu'à la valeur par défaut au lieu d'en créer un nouveau.)

3. Développez la nouvelle stratégie de surveillance ou par défaut et accédez à Stratégies de collecte de statistiques.

4. Cliquez sur l'icône en forme de crayon pour l'objet de surveillance sur le volet droit, sélectionnez Domaine Bridge (fv.BD).

(L'étape 4 peut être ignorée lorsque la stratégie par défaut est utilisée.)

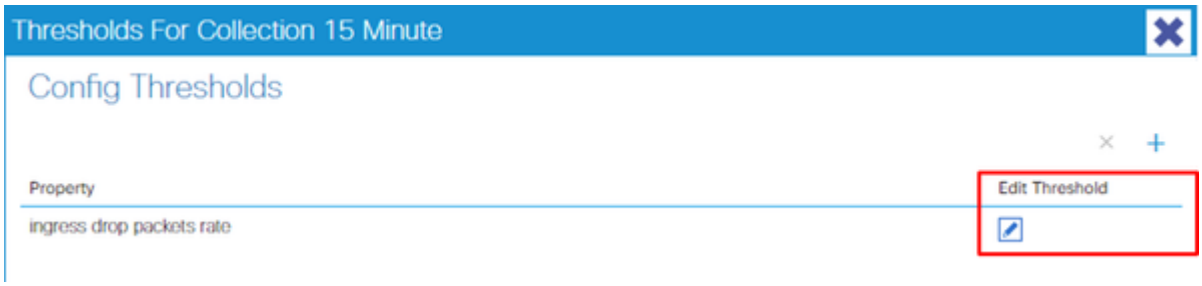
5. Dans la liste déroulante Objet de surveillance sur le volet droit, choisissez Domaine de pont (fv.BD) et Type de statistiques, choisissez Paquets d'entrée agrégés.



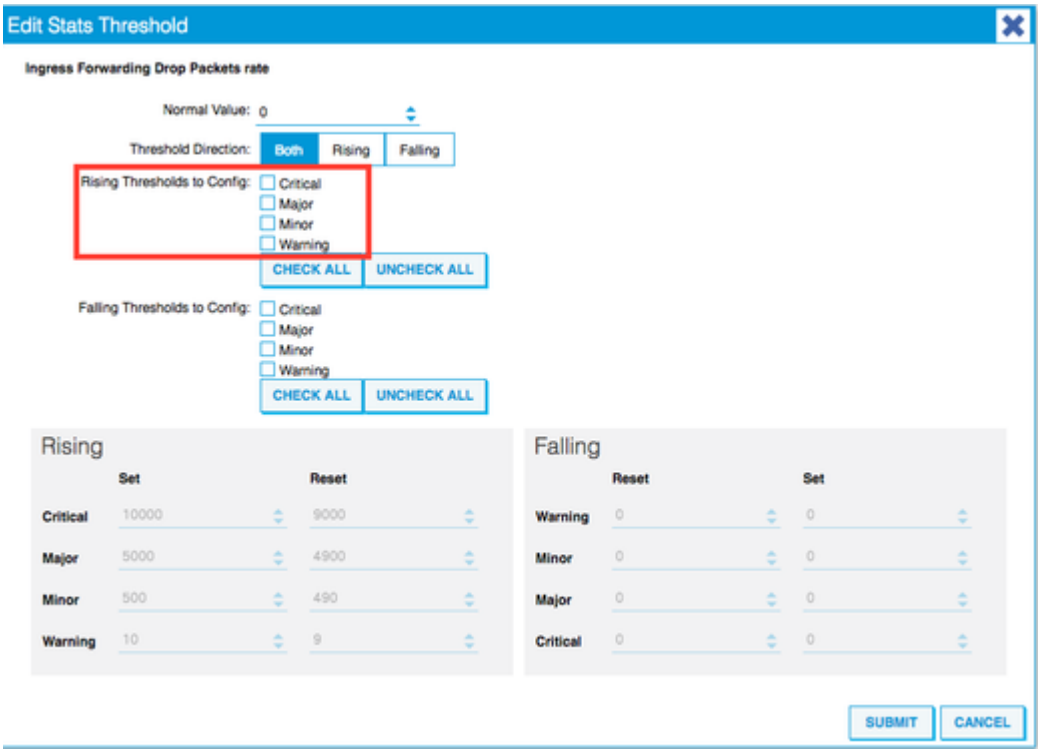
6. Cliquez sur le signe + en regard de Seuils de configuration.



7. Modifiez le seuil de perte de transfert.

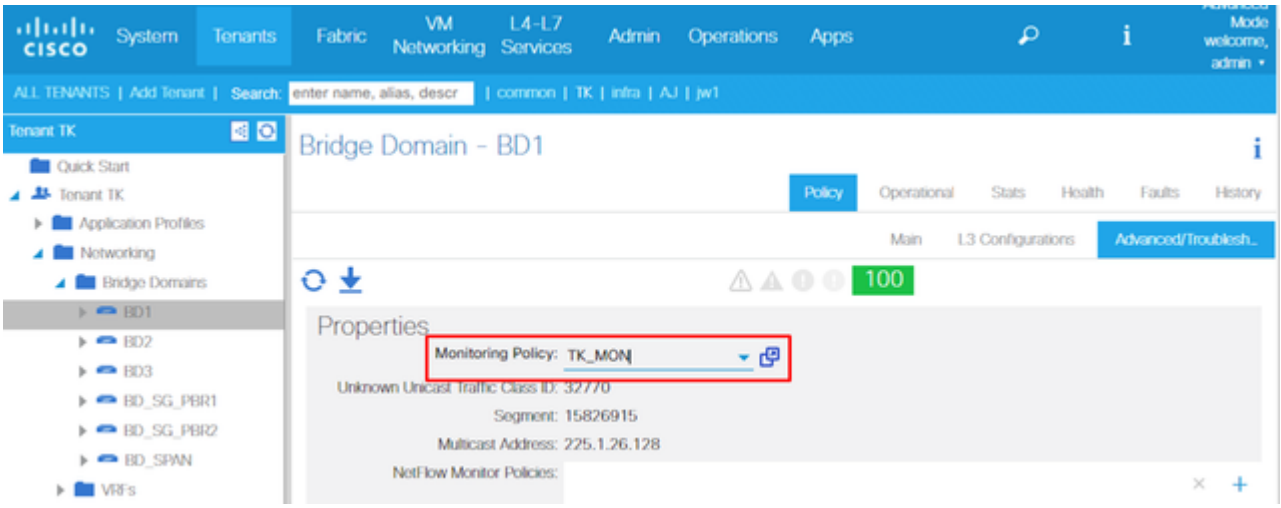


8. Il est recommandé de désactiver les seuils croissants à configurer pour le taux de perte critique, majeur, mineur et d'avertissement pour le transfert.



9. Appliquez cette nouvelle stratégie de surveillance au domaine Bridge qui nécessite une modification du seuil.

(L'étape 9 peut être ignorée lorsque la stratégie par défaut est utilisée.)



NOTE:
La stratégie de surveillance non par défaut ne peut pas avoir de configurations présentes sur la stratégie de surveillance par défaut. S'il est nécessaire de conserver ces configurations identiques à la stratégie de surveillance par défaut, les utilisateurs doivent vérifier la configuration de la stratégie de surveillance par défaut et configurer manuellement les mêmes stratégies sur une stratégie de surveillance autre que la stratégie par défaut.

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.