

Limitations de la banque TCAM Nexus 7000 et configuration de la chaîne bancaire

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Restrictions](#)

[Configuration](#)

[Informations connexes](#)

Introduction

Ce document décrit la programmation par défaut des fonctionnalités ACL (Access Control List) pour les banques TCAM (Ternary Content Addressable Memory) Nexus 7000, et comment mettre en commun des ressources à l'aide de la fonction de chaînage bancaire.

Problème

Avec la mise en oeuvre initiale, les fonctions ACL ne sont pas programmées sur différentes banques TCAM. Cela limite les entrées disponibles pour chaque fonction à 16 000. Pour les clients qui ont de grandes listes de contrôle d'accès, cela devient un problème. L'utilisation de la fonction de chaîne bancaire résout ce problème en supprimant la restriction bancaire. Lorsque la chaîne bancaire est activée, les fonctions basées sur les listes de contrôle d'accès peuvent être programmées sur plusieurs banques.

Exemples de messages d'erreur :

```
ACLQOS-SLOT3-4-ACLQOS_OVER_THRESHOLD Tcam 0 Bank 0's usage has reached its threshold
```

```
ACLMGR-3-ACLMGR_VERIFY_FAIL Verify failed: client 8200016E, Sufficient free entries are not available in TCAM bank
```

Solution

- Lorsque la chaîne bancaire est activée, elle n'affecte que les configurations futures. Les entrées TCAM actuelles ne sont pas reprogrammées. Lorsqu'une nouvelle liste de contrôle d'accès est appliquée à une interface, cette nouvelle liste de contrôle d'accès est programmée sur plusieurs banques.
- Lorsque la chaîne bancaire est activée, la liste de contrôle d'accès est programmée sur plusieurs banques (sauf Tunnel Decap and Control Plane Protection (CoPP)). (Reportez-vous à la section Restrictions.) S'il y a suffisamment d'entrées dans deux banques TCAM 0, la liste de contrôle d'accès est divisée et programmée en ces deux banques.
- Si les deux 0 de la banque TCAM n'ont pas assez d'entrées libres, la règle ACL est

programmée sur les quatre banques.

- Lorsque la fonction de chaîne bancaire est activée, même si la liste de contrôle d'accès a un nombre de règles inférieur à celui des entrées libres d'une seule banque, elle est programmée sur les deux 0 de la banque TCAM.
- Lorsque la chaîne bancaire est désactivée, les entrées TCAM actuelles sont reprogrammées. Si la liste de contrôle d'accès actuelle ne correspond pas à une seule banque, un message d'erreur est renvoyé et la chaîne bancaire ne peut pas être désactivée.
- Lors de la mise à niveau logicielle en service (ISSU), la chaîne bancaire doit être désactivée ; dans le cas contraire, la mise à niveau ISSU échouera.

Restrictions

- Lorsque la fonction de chaîne bancaire est activée, les stratégies appliquées à une interface et à un répertoire peuvent être fusionnées. Aucune des stratégies dont les statistiques sont activées ne peut être fusionnée. Lorsque la chaîne bancaire est activée, la fonctionnalité avec statistiques activées ne peut pas coexister avec d'autres fonctionnalités sur la même interface, dans la même direction. **Exemple** : Lorsque les statistiques sont activées sur la liste de contrôle d'accès au routeur d'entrée (RAACL) sur Ethernet2/1, le routage basé sur des politiques (PBR) ne peut pas être configuré sous cette interface.
- Deux stratégies, dont les types de résultats sont différents, ne peuvent pas être fusionnées. Il existe trois types de résultats : ACL, comptabilité et qualité de service (QoS). Ces trois types de résultats ne peuvent pas être fusionnés. Fonctionnalités sous le type de résultat ACL : Liste de contrôle d'accès aux ports (PAACL), RAACL, liste de contrôle d'accès aux VLAN (VAACL), PBR, DHCP, protocole de résolution d'adresse (ARP), Netflow. Fonctionnalités sous le type de résultat Comptabilité : Échantillon Netflow. Fonctionnalités sous le type de résultat QoS : QoS
Exemple : RAACL et QoS ne peuvent pas coexister dans la même direction sous une interface avec la chaîne bancaire activée.
- Le décodage de tunnel et le CoPP sont programmés sous une interface logique (LIF) et ne peuvent pas être fusionnés car leurs types de résultats sont différents. Afin d'éviter les restrictions dans lesquelles ils ne peuvent coexister, ils sont conservés dans une seule banque, même lorsque la chaîne bancaire est activée. Lorsque la liste RBACL (Role-Based Access Control List) est activée, la balise SGT/DGT (Source Security Group Tag/Destination Security Group Tag) sera utilisée afin de créer la clé de recherche TCAM. La liste RBACL ne peut pas fusionner avec d'autres stratégies de sortie, car l'étiquette est programmée pour récupérer les adresses de destination source SGT/DGT au lieu des adresses de destination source IPv4. Lorsque la chaîne bancaire est activée, les règles suivantes s'appliquent :
 1. Si la RBACL est activée sous Virtual Routing and Forwarding (VRF), aucune autre stratégie de sortie ne peut être configurée sous ces interfaces sur ce VRF.
 2. Si la liste RBACL est activée sous VLAN, aucune stratégie de sortie VLAN ne peut être configurée.
- Politique Port + Vlan : dans le matériel (matériel), les étiquettes de stratégie de port et de politique VLAN sont programmées sous une seule entrée ILM (Information Lifecycle Management). Il ne peut avoir qu'une seule étiquette pour la politique de port et une étiquette pour la politique de VLAN. Lorsque la chaîne bancaire est activée, les stratégies Port + VLAN

ne peuvent pas être prises en charge : Lorsqu'une stratégie de port est configurée, aucune stratégie ne peut être configurée sous le VLAN/SVI auquel le port appartient. Lorsqu'une stratégie VLAN/SVI est configurée, aucune stratégie ne peut être configurée sur le port qui appartient au VLAN.

Exemple de message d'erreur :

```
ERROR: Resource-pooling is not supported with certain feature combinations
```

Configuration

config t

le regroupement de ressources de liste d'accès matériel !peut uniquement être émis à partir du VDC par défaut

show hardware access-list resource pool
show system internal access-list status

```
SITE1-AGG1(config)# hardware access-list resource pooling mod ?  
  <1-9> Specify module number  
SITE1-AGG1(config)# hardware access-list resource pooling mod 3  
SITE1-AGG1(config)# show hardware access-list resource pooling  
  Module 3 enabled  
SITE1-AGG1# show system internal access-list status  
Atomic ACL updates Enabled.  
TCAM Default Result is Deny.  
ACL Logging enabled.  
Current LOU resource threshold: 5
```

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)