Caractéristique de tracé de paquets IOS-XE Datapath

Contenu

Introduction

Ce document décrit comment effectuer le suivi de paquet de datapath pour le Cisco IOS® - logiciel XE par l'intermédiaire de la caractéristique de tracé de paquets.

Afin d'identifier des questions telles que la mauvaise configuration, surcharge de capacité, ou même l'erreur de programmation ordinaire tout en dépannant, il est nécessaire de comprendre ce qui arrive à un paquet dans un système. La caractéristique de tracé de paquets de Cisco IOS XE satisfait ce besoin. Il fournit une méthode de champ-coffre-fort qui est utilisée pour rendre compte et afin de capturer le par-paquet traitant des détails basés sur une classe des conditions définies par l'utilisateur.

Conditions préalables

Exigences

Cisco recommande que vous ayez la connaissance de la caractéristique de tracé de paquets qui est disponible dans des versions 3.10 et ultérieures de Cisco IOS XE, aussi bien que dans des toutes les Plateformes qui exécutent le Logiciel Cisco IOS XE version 2, tel que les Routeurs de services d'agrégation de gamme Cisco 1000 (ASR1K), le routeur de services en nuage de gamme de Cisco 1000V (CSR1000v), et l'Integrated Services Router de gamme Cisco 4451-X (ISR4451-X).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 3.10S de Logiciel Cisco IOS XE version 2 (15.3(3)S) et plus tard
- ASR1K

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, veillez-vous pour comprendre l'impact potentiel de n'importe quelle commande utilisée.

Topologie de référence

Ce diagramme montre la topologie qui est utilisée pour les exemples qui sont décrits dans ce document :

Paquet traçant en service

Afin d'illustrer l'utilisation de la caractéristique de tracé de paquets, l'exemple qui est utilisé dans toute cette section décrit un suivi du trafic de Protocole ICMP (Internet Control Message Protocol) du poste de travail local 172.16.10.2 (derrière l'ASR1K) au serveur distant 172.16.20.2 (la direction d'entrée pour l'ASR1K à l'interface Gig0/0/1).

Vous pouvez tracer des paquets sur l'ASR1K avec ces deux étapes :

1. Activez la plate-forme conditionnelle met au point afin de sélectionner les paquets ou trafiquer que vous voulez tracer sur l'ASR1K.

2. Activez le tracé de paquets de plate-forme suivi de baie d'invocation de repère de conduit ou de caractéristique ((la FIA)).

Guide de démarrage rapide

Voici un guide de démarrage rapide si vous êtes déjà au courant du contenu du document, et

veulent une section pour un rapide regardent le CLI. Ce sont seulement quelques exemples pour illustrer l'utilisation de l'outil. Référez-vous aux sections postérieures qui discutent les syntaxes en détail, et assurez-vous l'utilisation la configuration qui est appropriée à votre condition requise.

1. Configurez les états de plate-forme :

```
debug platform condition ipv4 10.0.0.1/32 both --> matches in and out packets with source
or destination as 10.0.0.1/32

debug platform condition ipv4 access-list 198 egress --> (Ensure access-list 198 is
defined prior to configuring this command) - matches egress packets corresponding
to access-list 198

debug platform condition interface gig 0/0/0 ingress  --> matches all ingress packets
on interface gig 0/0/0

debug platform condition mpls 10 1 ingress --> matches MPLS packets with top ingress
label 10

debug platform condition ingress --> matches all ingress packets on all interfaces
(use cautiously)
```

   Après qu'un état de plate-forme soit configuré, commencez les conditions de plate-forme avec cette commande CLI :

```
debug platform condition start
```

2. Configurez le tracé de paquets :

```
debug platform packet-trace packet 1024  -> basic path-trace, and automatically stops
tracing packets after 1024 packets. You can use "circular" option if needed debug platform
packet-trace packet 1024 fia-trace -> enables detailed fia trace, stops
tracing packets after 1024 packets debug platform packet-trace drop [code <dropcode>]  ->
if you want to trace/capture only
packets that are dropped. Refer to Drop Trace section for more details.
```

   Note: Dans des releases plus tôt du Cisco IOS XE 3.x, la commande mettent au point l'enable de tracé de paquets de plate-forme est également exigée pour commencer la caractéristique de tracé de paquets. Ceci n'est plus exigé dans des releases du Cisco IOS XE 16.x.

Sélectionnez cette commande afin d'effacer la mémoire tampon de suivi et remettre à l'état initial le tracé de paquets :

```
clear platform packet-trace statistics  --> clear the packet trace buffer
```

La commande d'effacer la plate-forme conditionne et la configuration de tracé de paquets est :

```
clear platform condition all  --> clears both platform conditions and the packet trace
configuration
```

Commandes show

Vérifiez l'état de plate-forme et la configuration de tracé de paquets après que vous appliquiez les commandes précédentes afin de vous assurer ont de ce que vous avez besoin.

```
show platform conditions --> shows the platform conditions configured

show platform packet-trace configuration --> shows the packet-trace configurations

show debugging --> this will show both platform conditions and platform packet-trace configured
```

Voici les commandes de vérifier paquets tracés/capturés :

```
show platform packet-trace statistics --> statistics of packets traced

show platform packet-trace summary  --> summary of all the packets traced, with input and
output interfaces, processing result and reason. show platform packet-trace packet 12 -> Tracing
the 12th packet, with complete path trace
or FIA trace details.
```

Debugs conditionnels de plate-forme d'enable

La caractéristique de tracé de paquets se fonde sur le conditionnel mettent au point l'infrastructure afin de déterminer les paquets à tracer. Les conditionnels mettent au point l'infrastructure fournissent la capacité de filtrer le trafic basé en fonction :

- Protocol
- Adresse IP et masque
- Liste de contrôle d'accès (ACL)
- Interface
- Direction du trafic (d'entrée ou de sortie)

Ces conditions définissent où et quand les filtres sont appliqués à un paquet.

Pour le trafic qui est utilisé dans cet exemple, la plate-forme d'enable conditionnelle met au point dans la direction d'entrée pour des paquets d'ICMP de 172.16.10.2 à 172.16.20.2. En d'autres termes, sélectionnez le trafic que vous voulez tracer. Il y a de diverses options que vous pouvez employer afin de sélectionner ce trafic.

```
ASR1000#debug platform condition ?
egress Egress only debug
feature For a specific feature
ingress Ingress only debug
interface Set interface for conditional debug
ipv4 Debug IPv4 conditions
ipv6 Debug IPv6 conditions
start Start conditional debug
stop Stop conditional debug
```

Dans cet exemple, une liste d'accès est utilisée afin de définir la condition, comme affiché ici :

```
ASR1000#show access-list 150
Extended IP access list 150
10 permit icmp host 172.16.10.2 host 172.16.20.2
ASR1000#debug platform condition interface gig 0/0/1 ipv4
 access-list 150 ingress
```

Afin de commencer l'élimination des imperfections conditionnelle, sélectionnez cette commande :

```
ASR1000#debug platform condition start
```

> **Note**: Afin d'arrêter ou désactiver l'infrastructure conditionnelle d'élimination des imperfections, sélectionnez la commande d'**arrêt d'état de plate-forme de débogage**.

Afin de visualiser le conditionnel mettez au point les filtres qui sont configurés, sélectionnent cette commande :

```
ASR1000#show platform conditions

Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------|---------
GigabitEthernet0/0/1 & IPV4 ACL [150] ingress

Feature Condition Format Value
----------------------|----------------------|-------------------------------

ASR1000#
```

En résumé, cette configuration a été appliquée jusqu'ici :

```
access-list 150 permit icmp host 172.16.10.2 host 172.16.20.2
debug platform condition interface gig 0/0/1 ipv4 access-list 150 ingress
debug platform condition start
```

Tracé de paquets d'enable

> **Note**: Cette section décrit les options de paquet et de copie en détail, et les autres options sont décrites plus tard dans le document.

Des tracés de paquets sont pris en charge sur l'examen médical et les interfaces logiques, telles que le tunnel ou les interfaces d'accès virtuel.

Voici la syntaxe CLI de tracé de paquets :

```
ASR1000#debug platform packet-trace ?
copy Copy packet data
drop Trace drops only
inject Trace injects only
packet Packet count
punt Trace punts only

debug platform packet-trace packet <pkt-size/pkt-num> [fia-trace | summary-only]
 [circular] [data-size <data-size>]
```

Voici les descriptions pour les mots clé de cette commande :

- **paquet-numérique** - Le nombre de paquet spécifie le nombre maximal de paquets qui sont mis à jour en même temps.
- **réservé au résumé** - Ceci spécifie que seulement les données récapitulatives sont capturées. Le par défaut est de capturer des données récapitulatives et des données de caractéristique-chemin.

- **FIA-suivi** - Ceci exécute sur option un suivi FIA en plus des informations de données de chemin.

- **taille de données** - Ceci te permet pour spécifier la taille de la mémoire tampon de données de chemin, de 2,048 à 16,384 octets. Le par défaut est de **2,048** octets.

```
debug platform packet-trace copy packet {in | out | both} [L2 | L3 | L4]
 [size <num-bytes>]
```

Voici les descriptions pour les mots clé de cette commande :

- **entrée/sortie** - Ceci spécifie la direction de l'écoulement de paquet à copier - d'entrée et/ou de sortie.

- **L2/L3/L4** - Ceci te permet pour spécifier l'emplacement que la copie du paquet commence. La couche 2 (L2) est l'emplacement par défaut.

- **taille** - Ceci te permet pour spécifier le nombre maximal d'octets qui sont copiés. Le par défaut est 64 octets.

Pour cet exemple, c'est la commande utilisée afin d'activer le tracé de paquets pour le trafic qui est sélectionné avec le conditionnel mettent au point l'infrastructure :

```
ASR1000#debug platform packet-trace packet 16
```

Afin de passer en revue la configuration de tracé de paquets, sélectionnez cette commande :

```
ASR1000#show platform packet-trace configuration
debug platform packet-trace packet 16 data-size 2048
```

Vous pouvez également sélectionner la commande de **show debugging** afin de visualiser la plate-forme conditionnelle met au point et les configurations de tracé de paquets :

```
ASR1000# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Start

Conditions
Direction
------------------------------------------------------------------------|---------
GigabitEthernet0/0/1 & IPV4 ACL [150] ingress
...
IOSXE Packet Tracing Configs:

Feature Condition Format Value
----------------------|----------------------|-------------------------------

Feature Type Submode Level
-------|--------------|---------------------------------------------|----------

IOSXE Packet Tracing Configs:
debug platform packet-trace packet 16 data-size 2048
```

> **Note**: Écrivez l'**état clair de plate-forme toute la** commande afin d'effacer tous les debugs condition de plate-forme et les configurations et les données de tracé de paquets.

En résumé, ces données de configuration ont été utilisées jusqu'ici afin d'activer le tracé de paquets :

```
debug platform packet-trace packet 16
```

Limite d'état de sortie avec des tracés de paquets

Les conditions définissent les filtres conditionnels et quand elles sont appliquées à un paquet. Par exemple, **mettez au point le de sortie de l'interface g0/0/0 d'état de plate-forme** signifie qu'un paquet est identifié comme correspondance quand il atteint la FIA de sortie sur l'interface g0/0/0, tellement n'importe quel traitement de paquets qui a lieu du d'entrée jusqu'à ce que ce point soit manqué.

> **Note**: Cisco recommande fortement que vous employiez des conditions d'entrée pour des tracés de paquets afin d'obtenir les la plupart complètes et des données signicatives possibles. Les conditions de sortie peuvent être utilisés, mais se rendent compte des limites.

Affichez les résultats de tracé de paquets

> **Note**: Cette section suppose que le repère de conduit est activé.

Trois niveaux spécifiques d'inspection sont fournis par le tracé de paquets :

- Comptabilité
- résumé de Par-paquet
- données de chemin de Par-paquet

Quand cinq paquets de demandes d'ICMP sont envoyés de 172.16.10.2 à 172.16.20.2, ces commandes peuvent être utilisées afin de visualiser les résultats de tracé de paquets :

```
ASR1000#show platform packet-trace statistics
Packets Traced: 5
Ingress 5
Inject 0
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/1          Gi0/0/0          FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace packet 0

Packet: 0           CBUG ID: 4
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
```

```
State : FWD
Timestamp
   Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
   Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)

ASR1000#
```

> **Note**: La troisième commande fournit un exemple qui montre comment visualiser le tracé de paquets pour chaque paquet. Dans cet exemple, le premier paquet tracé est affiché.

De ces sorties, vous pouvez voir que cinq paquets sont tracés et que vous pouvez visualiser l'interface d'entrée, l'interface de sortie, l'état, et le repère de conduit.

État	Remarque
TRANS.	Le paquet est programmé/aligné pour la livraison, pour être expédié au prochain saut l'intermédiaire d'une interface de sortie.
COUP DE VOLÉE	Le paquet est donné un coup de volée du processeur d'expédition (point de gel) au processeur d'artère (RP) (avion de contrôle).
BAISSE	Le paquet est lâché sur le point de gel. Exécutez le suivi FIA, utilisez les compteurs gl de baisse, ou le datapath d'utilisation met au point afin de trouver plus de détails pour raisons de baisse.
INCONVÉNIENTS	Le paquet est consommé pendant un processus de paquet, comme pendant la requêt ping d'ICMP ou les cryptos paquets.

Le d'entrée et **injectent des** compteurs dans la sortie de statistiques de tracé de paquets correspondent aux paquets qui entrent par l'intermédiaire d'une interface externe et des paquets qui sont vus comme injectés de l'avion de contrôle, respectivement.

Suivi FIA

La FIA tient la liste de fonctionnalités qui sont exécutés séquentiellement en les moteurs de traitement de paquet (PPE) dans le processeur d'écoulement de Quantum (QFP) quand un paquet est expédié le d'entrée ou le de sortie. Les caractéristiques sont basées sur les données de configuration qui sont appliquées sur l'ordinateur. Ainsi, une FIA tracent des aides pour comprendre l'écoulement du paquet par le système pendant que le paquet est traité.

Vous devez appliquer ces données de configuration afin d'activer le tracé de paquets avec la FIA :

```
ASR1000#debug platform packet-trace packet 16 fia-trace
```

Affichez les résultats de tracé de paquets

> **Note**: Cette section suppose que la FIA tracent est activée. En outre, quand vous ajoutez ou modifiez les commandes en cours de tracé de paquets, les détails mis en mémoire tampon de tracé de paquets sont effacés, ainsi vous devez envoyer du trafic de nouveau de sorte que vous puissiez le tracer.

Envoyez cinq paquets d'ICMP de 172.16.10.2 à 172.16.20.2 après que vous sélectionniez la

commande qui est utilisée afin d'activer la FIA tracent, comme décrit dans la section précédente.

```
ASR1000#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/1          Gi0/0/0          FWD
1     Gi0/0/1          Gi0/0/0          FWD
2     Gi0/0/1          Gi0/0/0          FWD
3     Gi0/0/1          Gi0/0/0          FWD
4     Gi0/0/1          Gi0/0/0          FWD

ASR1000#show platform packet-trace packet 0
Packet: 0           CBUG ID: 9
Summary
 Input     : GigabitEthernet0/0/1
 Output    : GigabitEthernet0/0/0
 State     : FWD
 Timestamp
   Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
   Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
 Feature: IPV4
   Source      : 172.16.10.2
   Destination : 172.16.20.2
   Protocol    : 1 (ICMP)
 Feature: FIA_TRACE
   Entry     : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
   Timestamp : 3685243309297
 Feature: FIA_TRACE
   Entry     : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
   Timestamp : 3685243311450
 Feature: FIA_TRACE
   Entry     : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
   Timestamp : 3685243312427
 Feature: FIA_TRACE
   Entry     : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
   Timestamp : 3685243313230
 Feature: FIA_TRACE
   Entry     : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
   Timestamp : 3685243315033
 Feature: FIA_TRACE
   Entry     : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
   Timestamp : 3685243315787
 Feature: FIA_TRACE
   Entry     : 0x80321450 - IPV4_VFR_REFRAG
   Timestamp : 3685243316980
 Feature: FIA_TRACE
   Entry     : 0x82014700 - IPV6_INPUT_L2_REWRITE
   Timestamp : 3685243317713
 Feature: FIA_TRACE
   Entry     : 0x82000080 - IPV4_OUTPUT_FRAG
   Timestamp : 3685243319223
 Feature: FIA_TRACE
   Entry     : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
   Timestamp : 3685243319950
 Feature: FIA_TRACE
   Entry     : 0x8059aff4 - PACTRAC_OUTPUT_STATS
   Timestamp : 3685243323603
 Feature: FIA_TRACE
   Entry     : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
   Timestamp : 3685243326183

ASR1000#
```

Vérifiez la FIA associée avec une interface

Quand vous activez la plate-forme conditionnelle met au point, il est ajoutée à la FIA comme caractéristique. Selon l'emplacement qu'on l'ajoute à la liste, vous pourriez devoir ajuster vos conditions de plate-forme, comme quand vous tracez des paquets de pré-encap et de POST-encap.

Cette sortie affiche la commande des caractéristiques à la FIA pour l'élimination des imperfections conditionnelle de plate-forme qui est activée dans la direction d'entrée :

```
ASR1000#show platform hardware qfp active interface if-name GigabitEthernet 0/0/1

General interface information
Interface Name: GigabitEthernet0/0/1
Interface state: VALID
Platform interface handle: 10
QFP interface handle: 8
Rx uidb: 1021
Tx uidb: 131064
Channel: 16
Interface Relationships

BGPPA/QPPB interface configuration information
Ingress: BGPPA/QPPB not configured. flags: 0000
Egress : BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
48 PUNT INJECT DB
39 SPA/Marmot server
40 ethernet
1 IFM
31 icmp_svr
33 ipfrag_svr
34 ipreass_svr
36 ipvfr_svr
37 ipv6vfr_svr
12 CPP IPSEC
Protocol 0 - ipv4_input
FIA handle - CP:0x108d99cc DP:0x8070f400
IPV4_INPUT_DST_LOOKUP_ISSUE (M)
IPV4_INPUT_ARL_SANITY (M)
  CBUG_INPUT_FIA
  DEBUG_COND_INPUT_PKT
IPV4_INPUT_DST_LOOKUP_CONSUME (M)
IPV4_INPUT_FOR_US_MARTIAN (M)
IPV4_INPUT_IPSEC_CLASSIFY
IPV4_INPUT_IPSEC_COPROC_PROCESS
IPV4_INPUT_IPSEC_RERUN_JUMP
IPV4_INPUT_LOOKUP_PROCESS (M)
IPV4_INPUT_IPOPTIONS_PROCESS (M)
IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x108d9a34 DP:0x8070eb00
```

```
IPV4_OUTPUT_VFR
MC_OUTPUT_GEN_RECYCLE (D)
IPV4_VFR_REFRAG (M)
IPV4_OUTPUT_IPSEC_CLASSIFY
IPV4_OUTPUT_IPSEC_COPROC_PROCESS
IPV4_OUTPUT_IPSEC_RERUN_JUMP
IPV4_OUTPUT_L2_REWRITE (M)
IPV4_OUTPUT_FRAG (M)
IPV4_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x108d9bd4 DP:0x8070c700
LAYER2_INPUT_SIA (M)
CBUG_INPUT_FIA
DEBUG_COND_INPUT_PKT
LAYER2_INPUT_LOOKUP_PROCESS (M)
LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x108d9658 DP:0x80714080
LAYER2_OUTPUT_SERVICEWIRE (M)
LAYER2_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 14 - ess_ac_input
FIA handle - CP:0x108d9ba0 DP:0x8070cb80
PPPOE_GET_SESSION
ESS_ENTER_SWITCHING
PPPOE_HANDLE_UNCLASSIFIED_SESSION
DEF_IF_DROP_FIA (M)

QfpEth Physical Information
DPS Addr: 0x11215eb8
Submap Table Addr: 0x00000000
VLAN Ethertype: 0x8100
QOS Mode: Per Link

ASR1000#
```

> **Note**: Les CBUG_INPUT_FIA et les DEBUG_COND_INPUT_PKT correspondent au conditionnel mettent au point les caractéristiques qui sont configurées sur le routeur.

Videz les paquets tracés

Vous pouvez copier et vider les paquets pendant qu'ils sont tracés, pendant que cette section décrit. Cet exemple affiche comment copier un maximum de 2,048 octets des paquets dans la direction d'entrée (172.16.10.2 à 172.16.20.2).

Voici la commande supplémentaire qui est nécessaire :

```
ASR1000#debug platform packet-trace copy packet input size 2048
```

> **Note**: La taille du paquet qui est copié est de l'ordre de 16 à 2,048 octets.

Sélectionnez cette commande afin de vider les paquets copiés :

```
ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 14
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
    Start   : 1819281992118 ns (05/17/2014 06:40:01.207240 UTC)
    Stop    : 1819282095121 ns (05/17/2014 06:40:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
Timestamp : 4458180580929

<some content excluded>

Feature: FIA_TRACE
Entry : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
Timestamp : 4458180593896
Packet Copy In
a4934c8e 33020023 33231379 08004500 00640160 0000ff01 5f16ac10 0201ac10
01010800 1fd40024 00000000 000184d0 d980abcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcd

ASR1000#
```

Suivi de baisse

Le suivi de baisse est disponible dans la version 3.11 et ultérieures de Logiciel Cisco IOS XE version 2. Il active le tracé de paquets seulement pour les paquets relâchés. Voici quelques points culminants de la caractéristique :

- Il te permet sur option pour spécifier la conservation des paquets pour un code spécifique de baisse.
- Il peut être utilisé sans états globaux ou d'interface afin de capturer des événements de baisse.
- Une capture d'événement de baisse veut dire que seulement la baisse elle-même est tracée, pas la vie du paquet. Cependant, il te permet toujours pour capturer des données récapitulatives, des données de tuple, et le paquet afin d'aider à affiner des conditions ou à fournir des indices au prochain mettent au point l'étape.

Voici la syntaxe de commande qui est utilisée afin d'activer des tracés de paquets de baisse-type :

```
debug platform packet-trace drop [code <code-num>]
```

Le code de baisse est identique que l'ID de baisse, comme signalé dans la sortie de commande de **détail de baisse de statistiques actives de qfp de matériel de show platform** :

```
ASR1000#show platform hardware qfp active statistics drop detail
```

```
-------------------------------------------------------------------------------
   ID  Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------------
   60  IpTtlExceeded                                  3                    126
    8  Ipv4Acl                                       32                   3432
```

Scénario de suivi de baisse d'exemple

Appliquez cet ACL sur l'interface de la yole 0/0/0 de l'ASR1K afin de relâcher le trafic de 172.16.10.2 à 172.16.20.2 :

```
ASR1000#show platform hardware qfp active statistics drop detail
-------------------------------------------------------------------------------
   ID  Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------------
   60  IpTtlExceeded                                  3                    126
    8  Ipv4Acl                                       32                   3432
```

Avec l'ACL en place, qui relâche le trafic de l'hôte local au serveur distant, appliquez cette configuration de baisse-suivi :

```
debug platform condition interface Gig 0/0/1 ingress
debug platform condition start
debug platform packet-trace packet 1024 fia-trace
debug platform packet-trace drop
```

Envoyez cinq paquets de demandes d'ICMP de 172.16.10.2 à 172.16.20.2. Le suivi de baisse capture ces paquets qui sont lâchés par l'ACL, comme affiché :

```
ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 0
Punt 0
Drop     5
Count Code Cause
5 8 Ipv4Acl
Consume 0
```

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
1 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
2 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
3 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
4 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
```

```
ASR1K#debug platform condition stop

ASR1K#show platform packet-trace packet 0
Packet: 0 CBUG ID: 140
Summary
Input : GigabitEthernet0/0/1
```

```
Output : GigabitEthernet0/0/0
State     : DROP 8   (Ipv4Acl)
Timestamp
Start : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
Stop : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 657 ns
Feature: FIA_TRACE
Entry : 0x806a2698 - IPV4_INPUT_ACL
Lapsed time: 2773 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 1013 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 2951 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 2097 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry : 0x806db148 - OUTPUT_DROP
Lapsed time: 1297 ns
Feature: FIA_TRACE
Entry : 0x806a0c98 - IPV4_OUTPUT_ACL
Lapsed time: 78382 ns

ASR1000#
```

Injectez et donnez un coup de volée les suivis

La caractéristique de tracé de paquets d'injection et de coup de volée a été ajoutée dans la version 3.12 et ultérieures de Logiciel Cisco IOS XE version 2 afin de tracer le coup de volée (les paquets qui sont reçus sur le point de gel qui sont donnés un coup de volée à l'avion de contrôle) et injecter (les paquets qui sont injectés au point de gel de l'avion de contrôle) des paquets.

> **Note**: Le suivi de coup de volée peut fonctionner sans global ou relie des conditions, juste comme un suivi de baisse. Cependant, les conditions doivent être définies pour qu'un suivi d'injection fonctionne.

Être un exemple d'un coup de volée et voici injectent le tracé de paquets quand vous cinglez de l'ASR1K à un routeur contigu :

```
 ASR1000#debug platform condition ipv4 172.16.10.2/32 both
ASR1000#debug platform condition start
```

```
ASR1000#debug platform packet-trace punt
ASR1000#debug platform packet-trace inject
ASR1000#debug platform packet-trace packet 16
ASR1000#
ASR1000#ping 172.16.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/14/15 ms
ASR1000#
```

Maintenant vous pouvez vérifier le coup de volée et injecter des résultats de suivi :

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 INJ.2 Gi0/0/1 FWD
1 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
2 INJ.2 Gi0/0/1 FWD
3 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
4 INJ.2 Gi0/0/1 FWD
5 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
6 INJ.2 Gi0/0/1 FWD
7 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
8 INJ.2 Gi0/0/1 FWD
9 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 120
Summary
Input     : INJ.2
Output : GigabitEthernet0/0/1
State : FWD
Timestamp
Start : 115612780360228 ns (05/29/2014 15:02:55.467987 UTC)
Stop : 115612780380931 ns (05/29/2014 15:02:55.468008 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.1
Destination : 172.16.10.2
Protocol : 1 (ICMP)

ASR1000#
ASR1000#show platform packet-trace packet 1
Packet: 1 CBUG ID: 121
Summary
Input : GigabitEthernet0/0/1
Output : internal0/0/rp:0
State     : PUNT 11  (For-us data)
Timestamp
Start : 115612781060418 ns (05/29/2014 15:02:55.468687 UTC)
Stop : 115612781120041 ns (05/29/2014 15:02:55.468747 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.10.1
Protocol : 1 (ICMP)
```

Exemples de tracé de paquets

Cette section fournit quelques exemples où la caractéristique de tracé de paquets est utile pour dépanner des buts.

Exemple de tracé de paquets - NAT

Avec cet exemple, un Traduction d'adresses de réseau (NAT) de source d'interface est configuré sur l'interface WAN d'un ASR1K (Gig0/0/0) pour le sous-réseau local (172.16.10.0/24).

Voici la configuration d'état et de tracé de paquets de plate-forme qui est utilisée afin de tracer le trafic de 172.16.10.2 à 172.16.20.2, qui devient traduit (NAT) sur l'interface Gig0/0/0 :

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 INJ.2 Gi0/0/1 FWD
1 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
2 INJ.2 Gi0/0/1 FWD
3 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
4 INJ.2 Gi0/0/1 FWD
5 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
6 INJ.2 Gi0/0/1 FWD
7 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
8 INJ.2 Gi0/0/1 FWD
9 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 120
Summary
Input     : INJ.2
Output : GigabitEthernet0/0/1
State : FWD
Timestamp
Start : 115612780360228 ns (05/29/2014 15:02:55.467987 UTC)
Stop : 115612780380931 ns (05/29/2014 15:02:55.468008 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.1
Destination : 172.16.10.2
Protocol : 1 (ICMP)

ASR1000#
ASR1000#show platform packet-trace packet 1
Packet: 1 CBUG ID: 121
Summary
Input : GigabitEthernet0/0/1
Output : internal0/0/rp:0
State     : PUNT 11  (For-us data)
Timestamp
Start : 115612781060418 ns (05/29/2014 15:02:55.468687 UTC)
Stop : 115612781120041 ns (05/29/2014 15:02:55.468747 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.10.1
Protocol : 1 (ICMP)
```

Quand cinq paquets d'ICMP sont envoyés de 172.16.10.2 à 172.16.20.2 avec une configuration NAT de source d'interface, ce sont les résultats de tracé de paquets :

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
1 Gi0/0/1 Gi0/0/0 FWD
```

```
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 146
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 3010217805313 ns (05/17/2014 07:01:52.227836 UTC)
Stop : 3010217892847 ns (05/17/2014 07:01:52.227923 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 355 ns
Feature: FIA_TRACE
Entry : 0x803c6af4 - IPV4_INPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 942 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 568 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: NAT
Direction : IN to OUT
Action : Translate Source
Old Address : 172.16.10.2 00028
New Address : 192.168.10.1 00002
Feature: FIA_TRACE
Entry : 0x8031c248 - IPV4_NAT_OUTPUT_FIA
Lapsed time: 55697 ns
Feature: FIA_TRACE
```

```
Entry : 0x801424f8 - IPV4_OUTPUT_THREAT_DEFENSE
Lapsed time: 693 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 444 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1457 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 7431 ns
ASR1000#
```

Exemple de tracé de paquets - VPN

Avec cet exemple, un tunnel VPN de site à site est utilisé entre l'ASR1K et le routeur Cisco IOS afin de protéger le trafic qui circule entre 172.16.10.0/24 et 172.16.20.0/24 (des sous-réseaux locaux et distants).

Voici la configuration d'état et de tracé de paquets de plate-forme qui est utilisée afin de tracer le trafic VPN qui découle de 172.16.10.2 à 172.16.20.2 sur l'interface de la yole 0/0/1 :

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 146
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 3010217805313 ns (05/17/2014 07:01:52.227836 UTC)
Stop : 3010217892847 ns (05/17/2014 07:01:52.227923 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
```

```
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 355 ns
Feature: FIA_TRACE
Entry : 0x803c6af4 - IPV4_INPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 942 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 568 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: NAT
Direction : IN to OUT
Action : Translate Source
Old Address : 172.16.10.2 00028
New Address : 192.168.10.1 00002
Feature: FIA_TRACE
Entry : 0x8031c248 - IPV4_NAT_OUTPUT_FIA
Lapsed time: 55697 ns
Feature: FIA_TRACE
Entry : 0x801424f8 - IPV4_OUTPUT_THREAT_DEFENSE
Lapsed time: 693 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 444 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1457 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 7431 ns
ASR1000#
```

Quand cinq paquets d'ICMP sont envoyés de 172.16.10.2 à 172.16.20.2, qui sont chiffrés par le tunnel VPN entre l'ASR1K et le routeur Cisco IOS dans cet exemple, ce sont les informations de suivi de tracé de paquets :

> **Note**: Les tracés de paquets affichent le traitement de l'association de sécurité QFP (SA) dans le suivi qui est utilisé afin de chiffrer le paquet, qui est utile quand vous dépannez des questions d'IPsec VPN afin de vérifier que SA correcte est utilisée pour le cryptage.

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 211
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 4636921551459 ns (05/17/2014 07:28:59.211375 UTC)
Stop : 4636921668739 ns (05/17/2014 07:28:59.211493 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 622 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 320 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 1102 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 586 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x80757914 - MC_OUTPUT_GEN_RECYCLE
Lapsed time: 195 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: IPSec
Result : IPSEC_RESULT_SA
Action : ENCRYPT
SA Handle : 6
Peer Addr : 192.168.20.1
Local Addr: 192.168.10.1
Feature: FIA_TRACE
Entry : 0x8043caec - IPV4_OUTPUT_IPSEC_CLASSIFY
Lapsed time: 9528 ns
Feature: FIA_TRACE
Entry : 0x8043915c - IPV4_OUTPUT_IPSEC_DOUBLE_ACL
Lapsed time: 355 ns
Feature: FIA_TRACE
```

```
Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN
Lapsed time: 657 ns
Feature: FIA_TRACE
Entry : 0x8043ae28 - IPV4_OUTPUT_IPSEC_RERUN_JUMP
Lapsed time: 888 ns
Feature: FIA_TRACE
Entry : 0x80436f10 - IPV4_OUTPUT_IPSEC_POST_PROCESS
Lapsed time: 2186 ns
Feature: FIA_TRACE
Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN
Lapsed time: 675 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 1902 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 71 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1582 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 3964 ns
ASR1000#
```

Impact sur les performances

Les mémoires tampons de tracé de paquets consomment la mémoire vive dynamique QFP, soient ainsi conscientes de la quantité de mémoire qu'une configuration exige et de la quantité de mémoire qui est disponible.

L'incidence des performances varie, dépendant sur les options de tracé de paquets qui sont activées. Le tracé de paquets affecte seulement la représentation d'expédition des paquets qui sont tracés, comme ces paquets qui apparient les conditions utilisateur-configurées. Le plus granulaire et les informations détaillées que vous configurez le tracé de paquets pour capturer, plus il affectera des ressources considérablement.

Comme avec n'importe quel dépannage, il est le meilleur d'adopter une approche itérative et d'activer seulement les options plus-détaillées de suivi quand une situation de débogage la justifie.

L'utilisation de mémoire vive dynamique QFP peut être estimée avec cette formule :

la mémoire a eu besoin = (des stats au-dessus) + numérique des paquets * (taille récapitulative + taille de données de chemin + taille de copie)

> **Note**: Là où les **stats temps système** et la **taille de résumé** sont réparés à 2 KO et 128 B, respectivement, les **données de chemin classent** et la **taille de copie** sont utilisateur-configurable.

Informations connexes

- Guide de configuration du logiciel de routeurs de la gamme d'agrégation de gamme Cisco ASR1000 - Tracé de paquets
- Pertes de paquets sur des routeurs de service de gamme Cisco ASR1000

- Support et documentation techniques - Cisco Systems