# Tests et dépannage

Ce chapitre décrit comment dépanner l'ASA et tester la connectivité de base.



# Récupérer les mots de passe d'activation et Telnet

Si vous oubliez les mots de passe d'activation ou Telnet, vous pouvez les récupérer pour les modèles ASA virtuel et ISA 3000. Vous devez effectuer la tâche à l'aide de l'interface de ligne de commande.

**Remarque** Pour les autres plateformes, vous ne pouvez pas récupérer les mots de passe perdus. Vous pouvez uniquement restaurer la configuration d'usine par défaut et réinitialiser les mots de passe par défaut. Pour Firepower 4100/9300, consultez le Guide de configuration de FXOS. Pour les autres modèles, consultez le Guide de dépannage de FXOS.

## Récupérer les mots de passe sur l'ISA 3000

Pour récupérer les mots de passe des ISA 3000, procédez comme suit :

**Procédure**

**Étape 1** Connectez-vous au port de console de l'ASA.

**Étape 2** Mettez l'ASA hors tension, puis rallumez-le.

**Étape 3** Après le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

**Étape 4** Pour mettre à jour la valeur du registre de configuration, entrez la commande suivante :

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

L'ASA affiche la valeur actuelle du registre de configuration et une liste d'options de configuration. Enregistrez la valeur actuelle du registre de configuration afin de pouvoir la restaurer ultérieurement.

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

**Étape 5** Rechargez l'ASA en saisissant la commande suivante :

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

L'ASA charge la configuration par défaut au lieu de la configuration de démarrage.

**Étape 6** Accédez au mode d'exécution privilégié en saisissant la commande suivante :

```
ciscoasa# enable
```

**Étape 7** Lorsque le mot de passe vous est demandé, appuyez sur **Entrée**.

Le mot de passe est une valeur vide.

**Étape 8** Chargez la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa# copy startup-config running-config
```

**Étape 9** Accédez au mode de configuration globale en saisissant la commande suivante :

```
ciscoasa# configure terminal
```

**Étape 10** Modifiez les mots de passe, au besoin, dans la configuration par défaut en saisissant les commandes suivantes :

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

**Étape 11** Chargez la configuration par défaut en saisissant la commande suivante :

```
ciscoasa(config)# no config-register
```

La valeur par défaut du registre de configuration est 0x1. Voir la référence des commandes pour en savoir plus sur le registre de configuration.

**Étape 12** Enregistrez les nouveaux mots de passe dans la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa(config)# copy running-config startup-config
```

# Récupérer les mots de passe ou les images sur l'ASA virtuel

Pour récupérer les mots de passe ou les images sur l'ASA virtuel, procédez comme suit :

**Procédure**

**Étape 1** Copiez la configuration en cours d'exécution dans un fichier de sauvegarde sur l'ASA virtuel :

**copy running-config** *nom de fichier*

**Exemple :**

```
ciscoasa# copy running-config backup.cfg
```

**Étape 2** Redémarrez l'ASA virtuel :

**reload**

**Étape 3** Dans le menu GNU GRUB, appuyez sur la flèche vers le bas, choisissez <**filename**> **sans option de chargement de configuration**, puis appuyez sur **Enter** (Entrée). Le nom de fichier est le nom de fichier d'image de démarrage par défaut sur l'ASA virtuel. L'image de démarrage par défaut n'est jamais démarrée automatiquement par la commande **fallback**. Chargez ensuite l'image de démarrage sélectionnée.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

**Exemple :**

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

**Étape 4** Copiez le fichier de configuration de sauvegarde vers la configuration en cours d'exécution.

**copy** *nom_de_fichier* **running-config**

**Exemple :**

```
ciscoasa (config)# copy backup.cfg running-config
```

**Étape 5** Réinitialisez le mot de passe.

**enable password** *password*

**Exemple :**

```
ciscoasa(config)# enable password cisco123
```

**Étape 6** Enregistrez la nouvelle configuration.

**write memory**

**Exemple :**

```
ciscoasa(config)# write memory
```

# Désactiver la récupération du mot de passe pour le matériel ISA 3000

**Remarque** Vous ne pouvez pas désactiver la récupération du mot de passe sur les modèles ASA virtuel, Secure Firewall.

Pour désactiver la récupération du mot de passe et vous assurer que les utilisateurs non autorisés ne peuvent pas utiliser le mécanisme de récupération du mot de passe pour compromettre l'ASA, procédez comme suit.

### Avant de commencer

Sur l'ASA, la commande **no service password-recovery** vous empêche de passer en mode ROMMON avec la configuration intacte. Lorsque vous passez en mode ROMMON, l'ASA vous invite à effacer tous les systèmes de fichiers flash. Vous ne pouvez pas passer en mode ROMMON sans effectuer au préalable cet effacement. Si vous choisissez de ne pas effacer le système de fichiers flash, l'ASA se recharge. Étant donné que la récupération du mot de passe dépend de l'utilisation du mode ROMMON et du maintien de la configuration existante, cet effacement vous empêche de récupérer un mot de passe. Cependant, la désactivation de la récupération du mot de passe empêche les utilisateurs non autorisés d'afficher la configuration ou d'insérer des mots de passe différents. Dans ce cas, pour restaurer le système à un état de fonctionnement, chargez une nouvelle image et un fichier de configuration de sauvegarde, le cas échéant.

La commande **service password-recovery** apparaît dans le fichier de configuration pour information uniquement. Lorsque vous saisissez la commande à l'invite de l'interface de ligne de commande, le paramètre est enregistré dans la NVRAM. La seule façon de modifier le paramètre est d'entrer la commande à l'invite de l'interface de ligne de commande. Le chargement d'une nouvelle configuration avec une version différente de la commande ne modifie pas le paramètre. Si vous désactivez la récupération du mot de passe lorsque l'ASA est configuré pour ignorer la configuration de démarrage au démarrage (en préparation de la récupération du mot de passe), l'ASA modifie le paramètre pour charger la configuration de démarrage comme d'habitude. Si vous utilisez le basculement et que l'unité de secours est configurée pour ignorer la configuration de démarrage, la même modification est apportée au registre de configuration lorsque la commande **no service password- recovery** est dupliquée sur l'unité de secours.

**Procédure**

Désactivez la récupération du mot de passe.

**no service password-recovery**

**Exemple :**

```
ciscoasa (config)# no service password-recovery
```

# Afficher les messages de débogage

Comme les résultats du débogage obéissent à un niveau de priorité élevé dans le processus du CPU, ils sont susceptibles de rendre le système inutilisable. Par conséquent, les commandes **debug** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le personnel d'assistance technique de Cisco. De plus, il est préférable d'utiliser les commandes **debug** en dehors des périodes d'affluence de trafic et lorsque peu d'utilisateurs sont connectés au réseau. En effectuant le débogage pendant ces périodes, il y moins de chance que des frais généraux d'administration accrus associés à l'exécution de la commande **debug** aient des répercussions sur l'utilisation du système. Pour activer les messages de débogage, consultez les commandes **debug** dans la référence de commande.

# Capture de paquets

La capture de paquets peut être utile lors du dépannage de problèmes de connectivité ou de la surveillance d'activités suspectes. Nous vous conseillons de communiquer avec le TAC de Cisco si vous souhaitez utiliser le service de capture de paquets.

## Lignes directrices pour la capture des paquets

### Mode contextuel

- Vous pouvez configurer les captures sur la liaison de commande de grappe dans un contexte; seul le paquet associé au contexte envoyé dans la liaison de commande de grappe est capturé.
- Vous ne pouvez configurer qu'une seule capture pour un VLAN partagé; si vous configurez une capture dans plusieurs contextes sur le VLAN partagé, seule la dernière capture configurée est utilisée.
- Si vous supprimez la dernière capture configurée (active), aucune capture ne devient active, même si vous avez déjà configuré une capture dans un autre contexte; vous devez supprimer la capture et l'ajouter à nouveau pour la rendre active.
- Tout le trafic qui entre dans l'interface à laquelle la capture est connectée est capturé, y compris le trafic vers d'autres contextes sur le VLAN partagé. Par conséquent, si vous activez une capture dans le contexte A pour un VLAN qui est également utilisé par le contexte B, le trafic entrant du contexte A et du contexte B est capturé.

- Pour le trafic de sortie, seul le trafic du contexte avec la capture active est capturé. La seule exception est lorsque vous n'activez pas l'inspection ICMP (par conséquent, le trafic ICMP n'a pas de session dans le chemin accéléré). Dans ce cas, le trafic ICMP d'entrée et de sortie pour tous les contextes sur le VLAN partagé est capturé.

### Directives supplémentaires

- Si l'ASA reçoit des paquets avec un en-tête TCP mal formaté et les abandonne du fait de la raison d'abandon ASP *invalid-tcp-hdr-length*, la sortie de la commande **show capture** sur l'interface où ces paquets sont reçus n'affiche pas ces paquets.
- Vous pouvez uniquement capturer le trafic IP; vous ne pouvez pas capturer des paquets non IP tels que les ARP.
- Pour les paquets marqués SGT en ligne, les paquets capturés contiennent un en-tête CMD supplémentaire que votre visualiseur PCAP pourrait ne pas comprendre.
- Les captures de paquets comprennent les paquets que le système modifie ou injecte dans la connexion en raison de l'inspection, de la normalisation de la NAT, du TCP ou d'autres fonctionnalités qui ajustent le contenu d'un paquet.
- La trace de la durée de vie d'un paquet virtuel injecté dans un chemin de données ne reflète pas exactement la façon dont le chemin de données gère les paquets physiques. Cette différence dépend de la version du logiciel, de la configuration et du type de paquets virtuels injectés. Voici les paramètres de configuration qui pourraient entraîner cette disparité :
  - Il existe au moins 2 instructions NAT pour le même hôte.
  - Les flux avant et arrière d'une connexion ont des protocoles différents. Par exemple, le flux avant est UDP ou TCP, le flux arrière est ICMP.
  - L'inspection d'erreurs ICMP est activée.

# Capturer les paquets

Pour capturer des paquets, procédez comme suit.

### Procédure

**Étape 1** Activez les fonctionnalités de capture de paquets pour l'analyse de paquets et l'isolement des défaillances de réseau :

**capture** *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes* ] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**file-size** ] [**headers-only** ] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

**Exemple :**

```
ciscoasa# capture captest interface inside
```

Vous devez configurer une interface pour capturer tous les paquets. Utilisez le même *capture_name* sur plusieurs instructions **capture** pour capturer plusieurs types de trafic.

Le mot clé **type asp-drop** capture les paquets abandonnés par le chemin de sécurité accélérée. Dans une grappe, les paquets de données abandonnés d'une unité à une autre sont également capturés. En mode de contexte multiple, lorsque cette option est activée dans l'espace d'exécution du système, tous les paquets de données abandonnés sont capturés; lorsque cette option est émise dans un contexte, seuls les paquets de données abandonnés qui proviennent d'interfaces appartenant à ce contexte sont capturés.

Les mots clés **type raw-data** capturent les paquets entrants et sortants. Il s'agit du paramètre par défaut.

La paire mot clé-argument **inline-tag** *tag* spécifie une balise pour une valeur SGT particulière ou la laisse non spécifiée pour capturer un paquet étiqueté avec n'importe quelle valeur SGT.

Le mot clé **buffer** définit la taille de la mémoire tampon utilisée pour stocker le paquet. Lorsque la mémoire tampon d'octets est pleine, la capture de paquets s'arrête. Lorsqu'elle est utilisée dans une grappe, il s'agit de la taille par unité, et non de la somme de toutes les unités. Le mot clé **circular-buffer** remplace la mémoire tampon, en commençant par le début, lorsqu'elle est pleine.

Le mot clé **ethernet-type** définit un type Ethernet à capturer. Les types Ethernet pris en charge comprennent 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP et VLAN. Une exception se produit avec le type 802.1Q ou VLAN. La balise 802.1Q est automatiquement ignorée et le type Ethernet interne est utilisé pour la mise en correspondance. L'IP est le type Ethernet par défaut.

Le mot clé **interface** définit le nom de l'interface sur laquelle utiliser la capture de paquets.

Pour capturer des paquets dans le plan de données, utilisez le mot clé **asa_dataplane**.

Pour configurer la taille du fichier de capture, utilisez le mot clé **file-size**. La taille du fichier peut être comprise entre 32 et 10 000 Mo.

Si vous souhaitez capturer uniquement les en-têtes de paquet L2, L3 et L4 sans données, utilisez la commande **headers-only** .

Le mot clé **match** capture la correspondance du protocole, des adresses IP source et de destination et des ports facultatifs. Vous pouvez utiliser ce mot clé jusqu'à trois fois dans une même commande. Le mot clé **any** capture uniquement le trafic IPv4. Vous pouvez utiliser les mots clés **any4** et **any6** pour capturer le trafic réseau IPv4 et IPv6 correspondant, respectivement. L'opérateur peut être l'une des options suivantes :

- lt : inférieur à
- gt : supérieur à
- eq : égal à

Le mot clé **real-time** affiche les paquets capturés en permanence en temps réel.

Le mot clé **reinject-hide** spécifie qu'aucun paquet réinjecté ne sera capturé et s'applique uniquement dans un environnement de mise en grappe.

**Remarque**
Si l'optimisation ACL est configurée, vous ne pouvez pas utiliser la commande **access-list** dans la capture. Vous ne pouvez utiliser que la commande **access-group**. Une erreur s'affiche si vous essayez d'utiliser la commande **access-list** dans ce cas.

**Étape 2** Capturez le trafic de liaison de commande de la grappe :

**capture** *capture_name* {**type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes* ] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

**capture** *capture_name* **interface cluster** [**buffer** *buf_size*] [**cp-cluster**] [**ethernet-type** *type*] [**packet-length** *bytes* ] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

**Exemple :**

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

Vous pouvez capturer le trafic de liaison de commande de grappe de deux manières : pour capturer tout le trafic sur la liaison de commande de grappe, utilisez le mot clé **cluster** pour le nom de l'interface. Pour capturer uniquement les paquets cLACP, spécifiez **type lacp**, puis indiquez l'ID de l'interface physique au lieu du nom de l'interface. Il existe deux types de paquets sur la liaison de commande de grappe : les paquets de plan de commande et les paquets de plan de données, qui comprennent tous deux le trafic de données transféré et les messages LU de la grappe. Le champ TTL de l'en-tête d'adresse IP est codé pour différencier ces deux types de paquets. Lorsque des paquets de données transférés sont capturés, leurs terminaisons de mise en grappe sont incluses dans le fichier de capture à des fins de débogage.

Le mot clé **cp-cluster** ne capture que les paquets du plan de commande sur la liaison de commande de grappe (et aucun paquet de plan de données). Cette option est utile dans le système en mode de contexte multiple où vous ne pouvez pas faire correspondre le trafic à l'aide d'une liste de contrôle d'accès.

**Étape 3** Capturez les paquets à l'échelle de la grappe :

**cluster exec capture** *capture_name arguments*

**Étape 4** Arrêtez la capture de paquets :

**no capture** *capture_name*

Pour terminer une capture de paquets en temps réel, utilisez les touches **Ctrl + c.** Pour supprimer définitivement la capture, utilisez la forme **no** (non) de cette commande. L'option en temps réel s'applique uniquement aux captures **raw-data** et **asp-drop**.

**Étape 5** Pour arrêter manuellement la capture de paquets sans supprimer les paquets de la mémoire tampon :

**capture** *nom* **stop**

**Étape 6** Pour redémarrer la capture :

**no capture** *nom***stop**

**Étape 7** Capturez les traces de paquet persistantes sur les unités de grappe :

**cluster exec** *capture_test* **persist**

**Étape 8** Effacez les traces de paquet persistantes :

**cluster exec** *clear* **packet-trace**

**Étape 9** Capturez les paquets IPsec déchiffrés :

**cluster exec** *capture_test* **include-decrypted**

**Étape 10** Effacez la capture :

**clear capture** *capture_name*

### Exemples

#### Paquets du plan de commande

Tous les paquets vers et depuis le plan de commande ont une TTL de 255, et le numéro de port 49495 est utilisé pour le port d'écoute du plan de commande de la mise en grappe. L'exemple suivant montre comment créer une capture LACP pour l'environnement de mise en grappe :

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

L'exemple suivant montre comment créer une capture pour les paquets du chemin de commande dans la liaison de mise en grappe :

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

#### Paquets du plan de données

Les paquets de données comprennent ceux transférés d'une unité à l'autre (son propriétaire de connexion) et les messages LU de la grappe. Les messages de mises à jour LU régulières de la grappe ont une TTL de 254, et il existe un paquet LU spécial qui a une TTL de 253. Ce paquet LU spécial est uniquement pour TCP et il ne se produit que lorsque le directeur choisit un nouveau propriétaire de flux; le directeur renvoie le paquet demandé avec le paquet de mise à jour CLU_FULL. Le paquet LU est rempli avec l'en-tête L3/L4 du paquet d'origine pour éviter une situation de concurrence potentielle du côté du récepteur. Les paquets de données transférés ont une TTL inférieure à 4. L'exemple suivant montre comment créer une capture pour les paquets du chemin de données dans la liaison de commande de grappe : Pour capturer tous les messages de « flow logical update » (mise à jour logique du flux) du plan de données inter-grappes, utilisez le port 4193.

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list ccl
```

# Afficher une capture de paquets

Vous pouvez afficher une capture de paquet au niveau de l'interface de ligne de commande, dans un navigateur, ou télécharger une capture sur un serveur de votre choix.

### Procédure

**Étape 1** Affichez la capture sur l'interface de ligne de commande :

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

**Exemple :**

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

Le mot clé **access-list** affiche des renseignements sur les paquets basés sur l'adresse IP ou les champs supérieurs pour l'identification de la liste d'accès spécifique.

Le mot clé **cluster exec** vous permet d'émettre la commande **show capture** sur une unité et d'exécuter la commande sur toutes les autres unités en même temps.

Le mot clé **count** affiche le nombre de paquets de données spécifiés.

Le mot clé **decode** est utile lorsqu'une capture de type **isakmp** est appliquée à une interface. Toutes les données ISAKMP passant par cette interface seront capturées après le déchiffrement et affichées avec plus de renseignements après le décodage des champs. La sortie décodée des paquets dépend du protocole du paquet. Généralement, cette commande prend en charge le décodage IP pour les protocoles ICMP, UDP et TCP. À partir de la version 9.10(1), cette commande prend également en charge le décodage IP pour GRE et IPinIP.

Le mot clé **detail** affiche des renseignements supplémentaires sur le protocole pour chaque paquet.

Le mot clé **dump** affiche un vidage hexadécimal des paquets transportés sur la liaison de données.

Le mot clé **packet-number** commence l'affichage au numéro de paquet spécifié.

**Étape 2** Affichez la capture de paquets dans votre navigateur :

**https://***ip_of_asa***/admin/capture/***capture_name***/pcap**

Si vous omettez le mot clé **pcap**, seul l'équivalent de la sortie de la commande **show capture** *capture_name* est fourni.

En mode de contexte multiple, la commande **copy capture** est disponible seulement dans l'espace d'exécution du système.

**Étape 3** Copiez la capture de paquets sur un serveur. Cet exemple montre le serveur FTP.

[**cluster exec**] **copy /pcap capture:**[*context-name/*]*capture_name* **ftp://***username***:***password***@***server_ip***/***path*

Si vous omettez le mot clé **pcap**, seul l'équivalent de la sortie de la commande **show capture** *capture_name* est fourni.

**Remarque**

Lorsque vous copiez une capture de paquets sur un disque, assurez-vous que le nom de fichier de la capture est inférieur ou égal à 63 caractères. Lorsque le nom de fichier comporte plus de 63 caractères, bien que la capture de paquets soit réussie, la copie de la capture sur un disque échoue.

### Exemples

L'exemple suivant montre une capture de type asp-drop :

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

L'exemple suivant montre une capture de type Ethernet :

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

# Afficher le vidage en cas de panne

Si l'ASA ou l'ASA virtuel tombe en panne, vous pouvez afficher les renseignements de vidage en cas de panne. Nous vous conseillons de communiquer avec le TAC de Cisco si vous souhaitez interpréter le vidage en cas de panne. Consultez la commande **show crashdump** dans la référence de commande.

# Afficher le vidage de la mémoire

Un vidage de la mémoire est un instantané du programme en cours d'exécution lorsque celui-ci s'est terminé de façon anormale ou a planté. Les vidages de la mémoire sont utilisés pour diagnostiquer ou déboguer les erreurs et enregistrer un plantage en vue d'une analyse hors site ultérieure. Le TAC de Cisco peut vous demander d'activer la fonction de vidage de la mémoire pour résoudre les pannes d'application ou de système sur l'ASA ou ASA virtuel. Consultez la commande **coredump** dans la référence de commande.

# Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport d'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne à environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et à environ 60 à 70 % de capacité pendant les heures de pointe.

## Utilisation de vCPU dans l'ASA virtuel

Utilisez la commande **show cpu usage** sur l'ASA virtuel pour afficher les statistiques d'utilisation du processeur. L'utilisation de vCPU dans ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation de vCPU signalée par le fournisseur de services en nuage (comme VMware, Azure, OCI, etc.) comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Temps d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la VM ASA virtuel
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

## Exemple d'utilisation du processeur

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- Rapports vSphere : 95 %
- ASA (comme les rapports ASA virtuel) : 40 %

- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

Le surdébit est utilisé pour effectuer des fonctions d'hyperviseur et pour déplacer des paquets entre les NIC et les vNIC à l'aide du vSwitch.

L'utilisation peut dépasser 100 %, car le serveur ESXi peut utiliser des ressources de traitement supplémentaires pour le surdébit au nom de l'ASA virtuel.

# Rapport d'utilisation du CPU VMware

Dans vSphere, cliquez sur l'onglet **VM Performance** (Performances de la VM), puis sur **Advanced** (Avancé) pour afficher la liste déroulante **Chart Options** (Options du graphique), qui indique l'utilisation de vCPU pour chaque état (%Utilisateur, %Inactif, %Sys, etc.) de la VM. Ces renseignements sont utiles pour comprendre le point de vue de VMware sur l'utilisation des ressources de CPU.

Sur l'interface shell du serveur ESXi (vous accédez à l'interface shell en utilisant SSH pour vous connecter à l'hôte), esxtop est disponible. Esxtop a une apparence similaire à la commande **top** de Linux et fournit des renseignements sur l'état de la VM pour les performances de vSphere, notamment les suivantes :

- Détails sur l'utilisation du vCPU, de la mémoire et du réseau
- Utilisation du vCPU pour chaque état de chaque VM.
- Mémoire (type M pendant l'exécution) et réseau (type N pendant l'exécution), ainsi que les statistiques et le nombre d'abandons RX

# ASA virtuel et graphiques vCenter

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et vCenter :

- Les numéros de graphique vCenter sont toujours supérieurs aux numéros d'ASA virtuel.
- vCenter l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

vCenter calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur

Lorsque vous comparez l'utilisation en MHz, les chiffres de vCenter et d'ASA virtuel correspondent. Selon le graphique vCenter, l'utilisation du CPU en % MHz est calculée comme suit : 60/(2499 x 1 vCPU) = 2,4

# Rapports d'utilisation du CPU Amazon CloudWatch

Vous pouvez afficher l'explorateur de mesures pour surveiller les ressources en fonction de leurs balises et de leurs propriétés. Procédez comme suit pour afficher les statistiques d'utilisation du processeur pour une instance en particulier :

**Procédure**

**Étape 1** Ouvrez la console **CloudWatch** et choisissez **Metrics** (Mesures) dans le volet de navigation.

**Étape 2** Sélectionnez l'espace de noms de la mesure **EC2** et sélectionnez la dimension **Per-instance Metrics** (Mesures par instance).

**Étape 3** Saisissez **CPU Utilization** (Utilisation du CPU) dans le champ de recherche et appuyez sur Entrée. Sélectionnez la ligne de l'instance requise pour afficher un graphique de la mesure **CPU Utilization** (Utilisation du CPU) pour cette instance.

Pour en savoir plus, consultez la documentation relative à Amazon CloudWatch.

# ASA virtuel et graphiques Amazon CloudWatch

Les chiffres du graphique Amazon CloudWatch sont supérieurs aux chiffres réels en raison des différentes façons de calculer l'utilisation du CPU sur l'ASA virtuel et le CloudWatch.

Lorsque l'ASA virtuel fonctionne en mode d'interrogation, chaque CPU exécute une boucle de commandes allégées au lieu d'entrer en mode d'économie d'alimentation ou dans tout autre état inactif. Cela améliore les performances en maintenant chaque cœur actif en tout temps au lieu de devoir l'activer/le désactiver ou que leurs horloges soient ajustées en fonction des états d'alimentation Intel.

À l'intérieur de l'ASA virtuel, cette activité est comprise comme un comportement inactif et l'utilisation du CPU est correctement calculée. Cependant, sur Amazon CloudWatch, le comportement inactif ressemble à une activité normale du CPU, car tous les cycles du CPU ont des instructions à exécuter, ce qui conduit le CloudWatch à afficher un pourcentage d'utilisation du CPU élevé (85 à 90 %).

# Rapport d'utilisation du CPU Azure

Effectuez les étapes suivantes pour afficher le % d'utilisation du CPU sur toutes les VM surveillées à l'aide des observations VM du moniteur Azure :

**Procédure**

**Étape 1** Accédez au portail Azure, sélectionnez **Monitor** (Superviser) et choisissez **Virtual Machines** (Machines virtuelles) dans la section **Solutions**.

**Étape 2** Sélectionnez l'onglet **Performance** pour afficher le tableau **CPU Utilization %** (% d'utilisation du CPU). Ce tableau affiche les cinq machines ayant la plus forte utilisation moyenne du processeur.

Effectuez les étapes suivantes pour afficher le tableau du % d'utilisation du CPU directement à partir d'une machine virtuelle Azure spécifique :

**Procédure**

**Étape 1** Accédez au portail Azure et sélectionnez **Virtual Machines** (Machines virtuelles).

**Étape 2** Dans la liste des VM, choisissez une VM.

**Étape 3** Dans la section **Monitoring** (Supervision), sélectionnez **Insights** (Observations).

**Étape 4** Sélectionnez l'onglet **Performance**.

Consultez la section Comment représenter graphiquement les performances avec les observations VM pour en savoir plus.

# Graphiques ASA virtuel et Azure

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Azure. Les numéros du graphique Azure sont toujours supérieurs aux numéros de l'ASA virtuel, car Azure calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Azure limite également la quantité de CPU demandée par le système d'exploitation invité. Imaginez un scénario dans lequel l'ASA virtuel signale une utilisation du CPU à 40 % et l'hyperviseur signale une utilisation du CPU à 90 %. Maintenant, si l'ASA virtuel a besoin de plus de puissance de traitement, l'utilisation du CPU peut dépasser 80 % et l'hyperviseur peut alors signaler l'utilisation du CPU à plus de 95 %. Cela conduit l'hyperviseur à limiter le CPU de l'ASA virtuel même si l'ASA virtuel n'exécute qu'une boucle de commandes légères en mode d'interrogation et présente un comportement inactif.

# Rapport d'utilisation du CPU Hyper-V

En plus d'afficher les renseignements de configuration du CPU, de la RAM et de l'espace disque pour les serveurs en nuage disponibles, vous pouvez également afficher les renseignements sur le disque, les E/S et le réseau. Utilisez ces renseignements pour vous aider à décider quel serveur en nuage correspond à vos besoins. Vous pouvez afficher les serveurs disponibles par le biais du client nova de ligne de commande ou de l'interface du **panneau de commande en nuage**.

Dans la ligne de commande, exécutez la commande suivante :

```
nova flavor-list
```

Toutes les configurations de serveur disponibles sont affichées. La liste contient les renseignements suivants :

- ID – ID de configuration du serveur
- Name – nom de la configuration, étiqueté par taille de RAM et type de performance
- Mémoire_Mo – la quantité de RAM pour la configuration
- Disque – la taille du disque en Go (pour les serveurs en nuage à usage général, la taille du disque système)
- Éphémère – la taille du disque de données
- Permutation – la taille de l'espace de permutation
- VCPU – le nombre de CPU virtuels associés à la configuration
- Facteur_RXTX – la quantité de bande passante, en Mbit/s, allouée aux ports PublicNet, aux ports ServiceNet et aux réseaux isolés (réseaux en nuage) reliés à un serveur.
- Est_Public – non utilisé

# Graphiques ASA virtuel et Hyper-V

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Hyper-V :

- Les numéros de graphique Hyper-V sont toujours supérieurs aux numéros d'ASA virtuel.
- Hyper-V l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

Hyper-V calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur

**Remarque** Il est conseillé de consulter les rapports d'ASA virtuel pour obtenir un pourcentage d'usage précis du processeur.

# Rapport d'utilisation du CPU OCI

Vous pouvez afficher le % d'utilisation du processeur dans le protocole OCI à l'aide de la mesure d'instance de calcul : **oci_computeagent**. La mesure d'utilisation du CPU affiche le niveau d'activité du CPU et est exprimée en pourcentage de temps total. Effectuez les étapes suivantes pour afficher les tableaux de mesures pour une seule instance de calcul :

**Procédure**

**Étape 1** Ouvrez le menu de navigation et cliquez sur **Instances** sous **Compute** (Calcul).

**Étape 2** Cliquez sur une instance, puis sur **Metrics** (Mesures) sous **Resources** (Ressources).

**Étape 3** Sélectionnez **oci_computeagent** dans la liste Metric namespace (Espace de noms de mesures).

Consultez la section Mesures des instances de calcul pour en savoir plus.

# ASA virtuel et graphiques OCI

Les numéros du graphique OCI sont toujours supérieurs aux numéros de l'ASA virtuel, car l'OCI calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

# Tester votre configuration

Cette section décrit comment tester la connectivité pour l'ASA en mode unique ou pour chaque contexte de sécurité, comment envoyer un message Ping aux interfaces ASA et comment autoriser les hôtes d'une interface à envoyer un message Ping aux hôtes sur une autre interface.

# Tester la connectivité de base : envoi d'un ping à des adresses

Ping est une commande simple qui vous permet de déterminer si une adresse particulière est active et réactive. Les rubriques suivantes fournissent des renseignements supplémentaires sur la commande et les types de tests que vous pouvez effectuer avec celle-ci.

## Ce que vous pouvez tester en utilisant le ping

Lorsque vous envoyez un message Ping à un périphérique, un paquet est envoyé à ce dernier, qui renvoie une réponse. Ce processus permet aux périphériques réseau de se détecter, de s'identifier et de se tester mutuellement.

Vous pouvez utiliser les messages Ping pour effectuer les tests suivants :

- Test de boucle avec retour de deux interfaces : vous pouvez initier l'envoi d'un message Ping d'une interface à une autre sur le même ASA, en tant que test de boucle avec retour externe pour vérifier l'état « opérationnel » de base et le fonctionnement de chaque interface.
- Envoyer un message Ping à un ASA : vous pouvez envoyer un message Ping à une interface sur un autre ASA pour vérifier qu'il est opérationnel et qu'il répond.
- Envoyer un message Ping via un ASA : vous pouvez envoyer un message Ping via un ASA intermédiaire en effectuant un Ping vers un périphérique situé de l'autre côté de l'ASA. Les paquets traverseront deux interfaces ASA intermédiaires dans chaque direction. Cette action effectue un test de base des interfaces, du fonctionnement et du temps de réponse de l'unité intermédiaire.
- Envoyer un message Ping pour tester le fonctionnement suspect d'un appareil réseau : vous pouvez envoyer un message Ping d'une interface ASA vers un appareil réseau que vous soupçonnez de fonctionner de manière incorrecte. Si l'interface est configurée correctement et qu'aucun écho n'est reçu, il pourrait y avoir des problèmes avec l'appareil.
- Envoyer un message Ping pour tester les communications intermédiaires : vous pouvez envoyer un message Ping à partir d'une interface ASA vers un appareil réseau connu pour fonctionner correctement. Si l'écho est reçu, le bon fonctionnement de tous les appareils intermédiaires et la connectivité physique sont confirmés.

## Choisir entre le ping ICMP et TCP

L'ASA comprend le Ping traditionnel, qui envoie des paquets de requête d'écho ICMP et reçoit les paquets de réponse d'écho en retour. Il s'agit d'un outil standard qui fonctionne bien si tous les périphériques du réseau autorisent le trafic ICMP. Avec le Ping ICMP, vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6, ou aux noms d'hôte.

Cependant, certains réseaux interdisent le protocole ICMP. Si cela est le cas pour votre réseau, vous pouvez plutôt utiliser le Ping TCP pour tester la connectivité du réseau. Avec le Ping TCP, le Ping envoie des paquets TCP SYN et considère le Ping comme réussi s'il reçoit un SYN-ACK en réponse. Avec le Ping TCP, vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais vous ne pouvez pas envoyer un message Ping à des adresses IPv6.

Gardez à l'esprit qu'un message Ping ICMP ou TCP réussi signifie simplement que l'adresse que vous utilisez est active et répond à ce type de trafic. Cela signifie que la connectivité de base fonctionne. D'autres politiques exécutées sur un périphérique peuvent empêcher des types de trafic de passer avec succès par un périphérique.

## Activer le protocole ICMP

Par défaut, vous pouvez envoyer un message Ping d'une interface à haute sécurité vers une interface à faible sécurité. Il vous suffit d'activer l'inspection ICMP pour permettre le trafic de retour. Si vous souhaitez effectuer un message Ping depuis une interface moins sécurisée vers une interface hautement sécurisée, vous devez appliquer une ACL pour autoriser le trafic.

Lors de l'envoi d'un message Ping à une interface ASA, toutes les règles ICMP appliquées à l'interface doivent autoriser les paquets de requête d'écho et de réponse d'écho. Les règles ICMP sont facultatives : si vous ne les configurez pas, tout le trafic ICMP vers une interface est autorisé.

Cette procédure explique toute la configuration ICMP que vous pourriez devoir effectuer pour activer l'envoi d'un message Ping ICMP des interfaces ASA ou pour l'envoi d'un message Ping par l'intermédiaire d'un ASA.

### Procédure

**Étape 1** Assurez-vous que les règles ICMP autorisent la requête d'écho/la réponse d'écho.

Les règles ICMP sont facultatives et s'appliquent aux paquets ICMP envoyés directement à une interface. Si vous n'appliquez pas de règles ICMP, tous les accès ICMP sont autorisés. Dans ce cas, aucune action n'est requise.

Cependant, si vous mettez en œuvre des règles ICMP, assurez-vous d'inclure au moins les éléments suivants sur chaque interface, en remplaçant « inside » par le nom d'une interface sur votre périphérique.

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

**Étape 2** Assurez-vous que les critères d'accès autorisent le protocole ICMP.

Lors de l'envoi d'un message Ping à un hôte via un ASA, les critères d'accès doivent autoriser le trafic ICMP à sortir et à revenir. Le critère d'accès doit autoriser au moins les paquets ICMP de requête d'écho/réponse d'écho. Vous pouvez ajouter ces règles en tant que règles globales.

En supposant que vous avez déjà des critères d'accès appliqués aux interfaces ou appliqués globalement, ajoutez simplement ces règles à l'ACL appropriée, par exemple :

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any anyecho

ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

Sinon, autorisez tous les ICMP :

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

Si vous n'avez pas de critères d'accès, vous devrez également autoriser l'autre type de trafic souhaité, car l'application de critères d'accès à une interface ajoute un refus implicite, de sorte que tout autre trafic sera abandonné. Utilisez la commande **access-group** pour appliquer l'ACL à une interface ou globalement.

Si vous ajoutez simplement la règle à des fins de test, vous pouvez utiliser la forme **no** (non) de la commande **access-list** pour supprimer la règle de l'ACL. Si l'ACL complète sert simplement à des fins de test, utilisez la commande **no access-group** pour supprimer l'ACL de l'interface.

**Étape 3** Activez l'inspection ICMP.

L'inspection ICMP est nécessaire lors de l'envoi d'un message Ping à l'ASA, par opposition à l'envoi d'un message Ping à une interface. L'inspection permet de renvoyer le trafic (c'est-à-dire le paquet de réponse d'écho) à l'hôte qui a initié le message Ping et garantit également qu'il y a une réponse par paquet, ce qui empêche certains types d'attaques.

Vous pouvez simplement activer l'inspection ICMP dans la politique d'inspection globale par défaut.

```
ciscoasa(config)# policy-map  global_policy
```

```
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

## Envoyer un message ping à des hôtes

Pour envoyer un message Ping à n'importe quel appareil, vous devez simplement saisir **ping** avec l'adresse IP ou le nom d'hôte, par exemple **ping 10.1.1.1** ou **ping www.exemple.com**. Pour le ping TCP, vous devez inclure le mot clé **tcp** et le port de destination, par exemple **ping tcp www.exemple.com 80**. C'est généralement tout ce que vous avez à faire pour effectuer un test.

Exemple de sortie pour un envoyer un message Ping réussi :

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Si l'envoi d'un message Ping échoue, la sortie indique ? pour chaque tentative en échec, et le taux de réussite est inférieur à 100 % (un échec complet correspond à 0 %) :

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Cependant, vous pouvez également ajouter des paramètres pour contrôler certains aspects du message Ping. Voici vos options de base :

- Ping ICMP.

  **ping** [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  Lieu :

  - *if_name* spécifie l'adresse IP source pour l'envoi d'un message Ping; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.
  - *host* est le nom IPv4, IPv6 ou le nom d'hôte de l'hôte à qui vous envoyez un message Ping.
  - **repeat** *count* est le nombre de paquets à envoyer. La valeur par défaut est égale à 5.
  - **timeout** *seconds* est le nombre de secondes d'expiration de chaque paquet si aucune réponse n'est reçue. La valeur par défaut est 2.
  - **data** *pattern* est le modèle hexadécimal à utiliser dans les paquets envoyés. La valeur par défaut est 0xabcd.
  - **size** *bytes* est la longueur du paquet envoyé. Par défaut, c'est de 100 octets.
  - **validate** indique que vous souhaitez valider les données de réponse.

- Ping TCP.

  **ping tcp** [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  Lieu :

- *if_name* spécifie l'adresse IP source pour l'envoi d'un message Ping; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.
- *host* est l'adresse IPv4 ou le nom d'hôte de la destination à laquelle vous envoyez un ping. Vous ne pouvez pas utiliser le Ping TCP avec les adresses IPv6.
- *port* est le port TCP de l'hôte auquel vous envoyez un message Ping.
- **repeat** et **timeout** ont la même signification que ci-dessus.
- **source** *host port* indique l'adresse IP source et le port pour envoyer un message Ping. Utilisez le port 0 pour obtenir un port aléatoire.

- Ping interactif.

  **ping**

  En saisissant un message Ping sans paramètres, vous êtes invité à indiquer l'interface, la destination et d'autres paramètres, y compris les paramètres étendus qui ne sont pas disponibles en tant que mots clés. Utilisez cette méthode si vous avez besoin d'un contrôle étendu sur les paquets Ping.

## Tester la connectivité ASA de manière systématique

Si vous souhaitez effectuer un test plus systématique de la connectivité ASA, vous pouvez utiliser la procédure générale suivante.

### Avant de commencer

Si vous souhaitez voir les messages de journal système mentionnés dans la procédure, activez la journalisation (la commande **logging enable**, ou **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation)** dans ASDM).

Bien que cela soit inutile, vous pouvez également activer le débogage ICMP pour afficher des messages sur la console ASA lorsque vous envoyez un message Ping aux interfaces ASA à partir de périphériques externes (vous ne verrez pas les messages de débogage pour les pings qui passent par l'ASA). Nous vous conseillons d'activer uniquement les messages Ping et de débogage pendant le dépannage, car ils peuvent affecter les performances. L'exemple suivant active le débogage ICMP, définit les messages de journal système à envoyer aux sessions Telnet ou SSH, les envoie à ces sessions et active la journalisation. Au lieu d'utiliser la commande **logging monitor debug**, vous pouvez également utiliser la commande **logging buffer debug** pour envoyer les messages du journal à un tampon, puis les afficher ultérieurement à l'aide de la commande **show logging**.

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

Avec cette configuration, vous obtiendrez un résultat similaire à celui-ci pour un ping réussi depuis un hôte externe (209.165.201.2) vers l'interface externe de l'ASA (209.165.201.1) :

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
```

```
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

La sortie affiche la longueur du paquet ICMP (32 octets), l'identifiant de paquet ICMP (1) et le numéro de séquence ICMP (le numéro de séquence ICMP commence à 0 et est incrémenté chaque fois qu'une requête est envoyée).

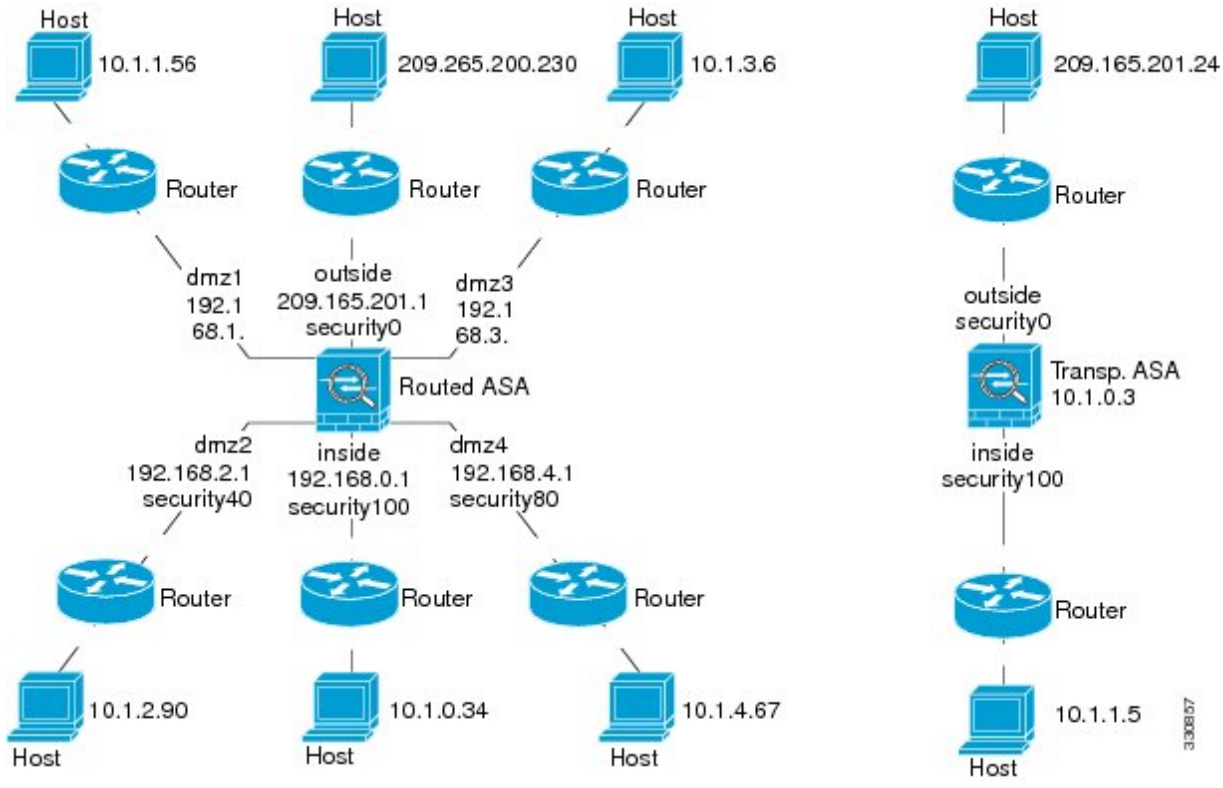
Lorsque vous avez terminé les tests, désactivez le débogage. Laisser la configuration en place peut présenter des risques de performance et de sécurité. Si vous avez activé la journalisation uniquement à des fins de test, vous pouvez également la désactiver.

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

## Procédure

**Étape 1** Tracez un diagramme de votre ASA ou de votre contexte de sécurité en mode unique qui affiche les noms d'interface, les niveaux de sécurité et les adresses IP. Le diagramme doit également inclure tous les routeurs directement connectés et un hôte de l'autre côté du routeur à partir duquel vous allez envoyer un message Ping à l'ASA.

***Illustration 1 : Diagramme de réseau avec interfaces, routeurs et hôtes***



**Étape 2** Envoyez un ping à chaque interface ASA à partir des routeurs directement connectés. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test garantit que les interfaces ASA sont actives et que la configuration d'interface est correcte.

Un message Ping peut échouer si l'interface ASA n'est pas active, si la configuration d'interface est incorrecte ou si un commutateur entre l'ASA et un routeur est en panne (voir la figure suivante). Dans ce cas, aucun message de débogage ni message de journal système ne s'affiche, car le paquet n'atteint jamais l'ASA.

***Illustration 2 : Échec de ping à l'interface ASA***

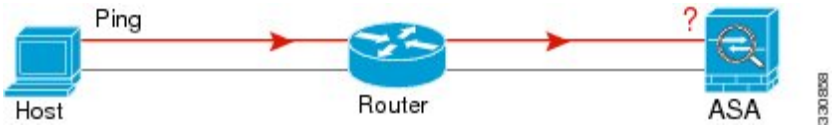
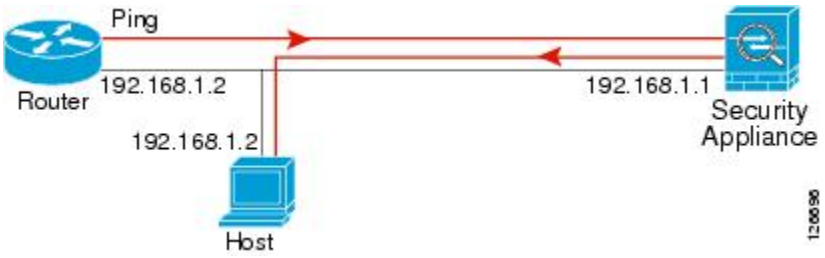



***Illustration 3 : Échec de ping en raison de problèmes d'adressage IP***




Si la réponse Ping ne revient pas au routeur, une boucle de commutation ou des adresses IP redondantes peuvent exister (voir la figure suivante).

**Étape 3** Envoyez un ping à chaque interface ASA à partir d'un hôte distant. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test vérifie si le routeur connecté directement peut acheminer le paquet entre l'hôte et l'ASA et si l'ASA peut correctement acheminer le paquet vers l'hôte.

Un message Ping peut échouer si l'ASA n'a pas de route de retour vers l'hôte par le routeur intermédiaire (voir la figure suivante). Dans ce cas, les messages de débogage indiquent que l'envoi du message Ping a réussi, mais le message de journal système 110001 s'affiche, indiquant qu'une défaillance de routage s'est produite.

***Illustration 4 : Échec de ping, car l'ASA n'a pas de route de retour***


**Étape 4** Envoyez un ping d'une interface ASA vers un périphérique réseau qui fonctionne correctement.

- Si le ping n'est pas reçu, il peut y avoir un problème avec le matériel de transmission ou la configuration de l'interface.
- Si l'interface ASA est configurée correctement et ne reçoit pas de réponse d'écho de l'appareil « connu pour être en bon état de fonctionnement », des problèmes avec la fonction de réception matérielle de l'interface peuvent exister. Si une interface différente ayant une capacité de réception « connue pour être bonne » peut recevoir un écho après avoir envoyé un message ping au même appareil « connu pour être bon », le problème de réception matérielle de la première interface est confirmé.

**Étape 5** Envoyez un ping de l'hôte ou du routeur par l'interface source vers un autre hôte ou routeur sur une autre interface. Répétez cette étape pour autant de paires d'interfaces que vous souhaitez vérifier. Si vous utilisez la NAT, ce test montre que la NAT fonctionne correctement.

Si l'envoi d'un message Ping réussit, un message de journal système s'affiche pour confirmer la traduction d'adresses pour le mode routé (305009 ou 305011) et qu'une connexion ICMP a été établie (302020). Vous pouvez également saisir la commande **show xlate** ou **show conns** pour afficher ces renseignements.

L'envoi d'un message Ping peut échouer parce que la NAT n'est pas configurée correctement. Dans ce cas, un message de journal système s'affiche, indiquant que la NAT a échoué (305005 ou 305006). Si l'envoi d'un message Ping provient d'un hôte externe vers un hôte interne et que vous n'avez pas de traduction statique, vous recevez le message 106010.

***Illustration 5 : Échec de ping parce que l'ASA ne traduit pas les adresses***


# Tracer les routes vers les hôtes

Si vous rencontrez des difficultés pour envoyer du trafic vers une adresse IP, vous pouvez tracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin réseau.

**Procédure**

**Étape 1** Rendre l'ASA visible sur les routes de trace, à la page 24.

**Étape 2** Déterminer les routes de paquets, à la page 26.

## Rendre l'ASA visible sur les routes de trace

Par défaut, l'ASA n'apparaît pas sur les routes de trace en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par l'ASA et augmenter la limite de débit pour les messages ICMP inaccessibles.

**Procédure**

**Étape 1** Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez personnaliser les paramètres de connexion.

**class-map** *name*

**match** *parameter*

**Exemple :**

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

Pour en savoir plus sur les instructions correspondantes, consultez le chapitre Politique de service dans le guide de configuration du pare-feu.

**Étape 2** Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

**policy-map** *name* **class** *name*

**Exemple :**

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

**Étape 3** Décrémentez la durée de vie (TTL) sur les paquets correspondant à la classe.

```
set connection decrement-ttl
```

**Étape 4** Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *policymap_name* {**global** | **interface** *interface_name* }

**Exemple :**

```
ciscoasa(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

**Étape 5** Augmentez la limite de débit des messages ICMP inaccessibles afin que l'ASA s'affiche sur la sortie de la route de trace.

**icmp unreachable rate-limit** *rate* **burst-size** *size*

**Exemple :**

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

La limite de débit peut aller de 1 à 100, 1 étant la valeur par défaut. La taille de rafale n'a pas d'importance, mais doit être comprise entre 1 et 10.

### Exemple

L'exemple suivant décrémente la TTL pour tout le trafic globalement et augmente la limite de messages ICMP inaccessibles à 50.

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

## Déterminer les routes de paquets

Utilisez la route de trace pour vous aider à déterminer la route que les paquets emprunteront pour atteindre leur destination. Une route de trace fonctionne en envoyant des paquets UDP ou des échos ICMPv6 à une destination sur un port non valide. Comme le port n'est pas valide, les routeurs situés sur le chemin vers la destination répondent par un message de dépassement de temps ICMP ou ICMPv6 et signalent cette erreur à l'ASA.

La route de trace affiche le résultat de chaque sonde envoyée. Chaque ligne de sortie correspond à une valeur TTL par ordre croissant. Le tableau suivant explique les symboles de sortie.

| Symbole de sortie | Description |
|---|---|
| * | Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration. |
| U | Aucune route vers la destination. |
| *nn* msec | Pour chaque nœud, le temps d'aller-retour (en millisecondes) pour le nombre spécifié de sondes. |
| !N. | Réseau ICMP inaccessible. Pour ICMPv6, l'adresse est hors du champ d'application. |
| !H | Hôte ICMP inaccessible. |
| !P | ICMP inaccessible. Pour ICMPv6, port inaccessible. |
| !A | ICMP administrativement interdit. |
| ? | Erreur ICMP inconnue. |

### Procédure

Tracez la route vers une destination :

**traceroute** [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

**Exemple :**

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa# traceroute 2002::130

Type escape sequence to abort.
Tracing the route to 2002::130

 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

En règle générale, il suffit d'inclure l'adresse IP ou le nom d'hôte de destination, par exemple **traceroute www.example.com**. Cependant, vous pouvez ajuster les caractéristiques de la trace si vous le souhaitez :

- **source** {*source_ip* | *source-interface*} : spécifie l'interface à utiliser comme source de la trace. Vous pouvez définir l'interface par son nom ou par son adresse IP. Pour IPv6, vous ne pouvez pas spécifier l'interface source; vous pouvez uniquement spécifier l'adresse IP source. Une adresse IPv6 n'est valide que si vous avez activé IPv6 sur une interface ASA. En mode transparent, vous devez utiliser l'adresse de gestion.
- **numeric** : indique que seules les adresses IP doivent être affichées dans la route de trace. Sans ce mot clé, la route de trace effectue des recherches DNS pour les adresses et inclut les noms DNS, en supposant que vous configuriez le DNS.
- **timeout** *timeout_value* : durée d'attente d'une réponse avant l'expiration. La valeur par défaut est de 3 secondes.
- **probe** *probe_num* : nombre de sondes à envoyer à chaque niveau TTL. La valeur par défaut est de 3.
- **ttl** *min_ttl max_ttl* : valeurs de durée de vie minimum et maximum pour les sondes. La valeur minimum par défaut est de 1, mais vous pouvez la définir à une valeur plus élevée pour supprimer l'affichage des sauts connus. La valeur par défaut est 30. La route de trace se termine lorsque le paquet atteint sa destination ou lorsque la valeur maximum est atteinte.
- **port** *port_value* : le port UDP à utiliser. La valeur par défaut est 33434.
- **use-icmp** : envoie des paquets ICMP au lieu de paquets UDP pour les sondes.

# Utiliser l'outil Packet Tracer pour tester la configuration de la politique

Vous pouvez tester la configuration de votre politique en modélisant un paquet basé sur des adresses source et de destination, et des caractéristiques de protocole. La trace effectue des recherches de politiques pour tester les critères d'accès, la NAT, le routage, etc., pour voir si le paquet est autorisé ou refusé.

En testant les paquets de cette manière, vous pouvez voir les résultats de vos politiques et vérifier si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés.

### Procédure

**Étape 1** La commande est compliquée, nous l'avons donc divisée en parties. Commencez par choisir l'interface et le protocole de trace :

**packet-tracer input** *ifc_name* [**vlan-id***vlan_id* ] {**icmp** | **tcp** | **udp** | **rawip** | **sctp**} [**inline-tag** *tag*] ...

Lieu :

- **input** *ifc_name* : nom de l'interface à partir de laquelle commencer la trace. Pour un groupe de ponts, spécifiez le nom de l'interface membre du groupe de ponts.
- **vlan-id** *vlan_id* : (Facultatif) Le LAN virtuel, où le traceur de paquets entre dans une interface parent, qui est ensuite redirigée vers une sous-interface. L'identité VLAN est disponible uniquement lorsque l'interface d'entrée n'est pas une sous-interface. Les valeurs valides sont comprises entre 1 et 4 096.
- **icmp**, **tcp**, **udp**, **rawip**, **sctp** : le protocole à utiliser. « rawip » désigne une adresse IP brute, c'est-à-dire des paquets IP qui ne sont pas TCP/ UDP.
- **inline-tag** *tag* : (Facultatif) La valeur de la balise du groupe de sécurité intégrée dans l'en-tête CMD de couche 2. Cette valeur peut être comprise entre 0 et 65 533.

**Étape 2** Ensuite, saisissez l'adresse source et les critères de protocole.

...{*src_ip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}...

Lieu :

- *src_ip* : l'adresse IPv4 ou IPv6 source pour la trace de paquet.
- **user** *username* : l'identité de l'utilisateur au format domaine\utilisateur. L'adresse la plus récemment mappée pour l'utilisateur (le cas échéant) est utilisée dans la trace.
- **security-group** {**name** *name* | **tag** *tag*} : le groupe de sécurité source en fonction de la recherche IP-SGT de Trustsec. Vous pouvez spécifier un nom de groupe de sécurité ou un numéro de balise.
- **fqdn** *fqdn-string* : le nom de domaine complet de l'hôte source, IPv4 uniquement.

**Étape 3** Ensuite, saisissez les caractéristiques du protocole.

- ICMP : saisissez le type ICMP (1 à 255), le code ICMP (0 à 255) et éventuellement l'identifiant ICMP. Vous devez utiliser des chiffres pour chaque variable, par exemple, 8 pour l'écho.

  *type code*... [*ident*]...

- TCP/UDP/SCTP : saisissez le numéro de port source.

  ...*src_port* ...

- Adresse IP brute : saisissez le numéro de protocole, de 0 à 255.

  … *protocol* ...

**Étape 4** Enfin, saisissez les critères d'adresse de destination, le port de destination pour les traces TCP/UDP et les mots clés facultatifs, puis appuyez sur **Enter** (Entrée).

*...dmac* {*dst_ip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

Lieu :

- *dst_ip* : l'adresse IPv4 ou IPv6 de destination pour la trace de paquet.
- **security-group** {**name** *name* | **tag** *tag*} : le groupe de sécurité de destination en fonction de la recherche IP-SGT de Trustsec. Vous pouvez spécifier un nom de groupe de sécurité ou un numéro de balise.
- **fqdn** *fqdn-string* : le nom de domaine complet de l'hôte de destination, IPv4 uniquement.
- *dst_port* : le port de destination pour les traces TCP/UDP/SCTP. N'incluez pas cette valeur pour les traces ICMP ou IP brute.
- *dmac* : (Mode transparent) L'adresse MAC de destination.
- **detailed** : fournit des renseignements détaillés sur les résultats de la trace en plus de la sortie normale.
- **xml** : affiche les résultats de la trace au format XML.

**Étape 5** Saisissez l'option **persist** pour que le traceur de paquets débogue les paquets sur les unités de grappe.

- Vous pouvez autoriser les paquets simulés à quitter l'ASA en utilisant l'option **transmit**.
- Pour ignorer les vérifications de sécurité comme les ACL, les filtres VPN, l'usurpation d'adresse IPsec et uRPF, utilisez l'option **bypass-checks**.
- En utilisant l'option **decrypted**, vous pouvez injecter un paquet déchiffré dans un tunnel VPN et simuler également un paquet qui traverse un tunnel VPN.

**Étape 6** Saisissez l'**id** et l'**origin** pour suivre un paquet spécifique dans les unités de grappe.

- **id** : le numéro d'identité attribué par l'unité qui démarre la trace.
- **origin** : indique l'unité de grappe qui commence la trace.

### Exemple

L'exemple suivant trace un paquet TCP pour le port HTTP de 10.100.10.10 à 10.100.11.11. Le résultat indique que le paquet sera abandonné par la règle implicite de refus d'accès.

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11
 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
```

```
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

# Supervision des connexions

Pour afficher les connexions actuelles avec des renseignements sur la source, la destination, le protocole, etc., utilisez la commande **show conn all detail**.

# Historique des tests et du dépannage

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Prise en charge IPv6 pour les routes de trace | 9.7(1) | La commande **traceroute** a été modifiée pour accep adresse IPv6.<br>Nous avons modifié la commande suivante : **tracero** |
| Prise en charge de l'outil de trace de paquets pour les interfaces membres du groupe de ponts | 9.7(1) | Vous pouvez désormais utiliser l'outil de trace de pa les interfaces membres d'un groupe de ponts.<br>Nous avons ajouté deux nouvelles options à la comm **packet-tracer**; **vlan-id** et **dmac** |
| Démarrer et arrêter manuellement les captures de paquets | 9.7(1) | Vous pouvez maintenant arrêter et démarrer manuell capture.<br>Commandes ajoutées ou modifiées : **capture stop** |

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Capacités améliorées de l'outil de trace de paquets et de la capture de paquets | 9.9(1) | L'outil de trace de paquets a été amélioré avec les f suivantes :<br>• Tracer un paquet lorsqu'il passe entre les uni<br>• Autoriser des paquets simulés à quitter l'AS<br>• Contourner les contrôles de sécurité pour un p<br>• Considérer un paquet simulé comme un paq déchiffré.<br>La capture de paquets a été améliorée avec les fo suivantes :<br>• Capturer les paquets après leur déchiffreme<br>• Capturer les traces et les conserver dans la lis<br>Commandes nouvelles ou modifiées : **cluster exe trace include-decrypted, cluster exec capture persist, cluster exec clear packet-tracer, cluste packet-tracer id, cluster exec show packet-tra packet-tracer persist, packet-tracer transmit, p decrypted, packet-tracer bypass-checks** |
| Prise en charge de la capture de paquets pour le trafic IPv6 correspondant sans l'utilisation d'une ACL | 9.10(1) | Si vous utilisez le mot clé **match** pour la comma le mot clé **any** ne correspond qu'au trafic IPv4. V désormais spécifier les mots clés **any4** et **any6** po trafic IPv4 ou IPv6. Le mot clé **any** continue de uniquement au trafic IPv4.<br>Commandes nouvelles ou modifiées : **capture m** |
| Nouvelle commande **debug telemetry** pour Forepower 9300/4100. | 9.14(1) | Si vous utilisez la commande **debug telemetry**, de débogage liés à la télémétrie s'affichent. Les aident à identifier la cause des erreurs lors de la rapport de télémétrie.<br>Commandes nouvelles ou modifiées : **[ no ] debu telemetry**,**show debug telemetry** |
| Modifications de la commande **ping** | 9.18(2) | Pour prendre en charge l'envoi d'un message pin interface de boucle avec retour, la commande **ping** changé de comportement. Si vous spécifiez l'inte commande, l'adresse IP source correspond à l'ad l'interface spécifiée, mais l'interface de sortie ré déterminée par une recherche de route à l'aide de routage des données.<br>Commandes nouvelles ou modifiées : **ping** |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.