

Grappe ASA pour l'ASA virtuel pour le cloud privé

La mise en grappe vous permet de regrouper plusieurs ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer les grappes ASA virtuel à l'aide de :

- KVM
- VMware

Remarque Seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 43.

- À propos de la mise en grappe d'ASA virtuel, à la page 2
- Licences pour la mise en grappe d'ASA virtuel, à la page 8
- Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 9
- Lignes directrices de la mise en grappe d'ASA virtuel, à la page 9
- Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0, à la page 11
- Configurer la mise en grappe ASA virtuel après le déploiement, à la page 14
- Personnaliser l'opération de mise en grappe, à la page 24
- Gérer les nœuds de la grappe, à la page 34
- Supervision de la grappe ASA virtuel, à la page 40
- Exemples de mise en grappe d'ASA virtuel, à la page 42
- Référence pour la mise en grappe, à la page 42
- Historique de la mise en grappe d'ASA virtuel, à la page 58

À propos de la mise en grappe d'ASA virtuel

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent à la ASA Virtual d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance. Le déploiement ASA Virtual comprend une interface de gestion Management 0/0 que vous utiliserez pour gérer les nœuds de la grappe.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et provenant de la grappe à l'aide des interfaces individuelles de couche 3 et de l'une des méthodes suivantes :

- Routage basé sur les politiques : les routeurs en amont et en aval équilibrent la charge entre les nœuds à l'aide de cartes de routage et de listes de contrôle d'accès.
- Routage à chemins multiples à coût égal : les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les nœuds à l'aide de routes statiques ou dynamiques à coût égal.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Nœuds de la grappe

Les membres du nœud collaborent pour partager la politique de sécurité et les flux de trafic. Cette section décrit la nature du rôle de chaque nœud.

Configuration du démarrage

Sur chaque appareil, vous configurez une configuration de démarrage minimale qui inclut le nom de la grappe, l'interface de la liaison de commande de grappe et les autres paramètres de la grappe. Le premier nœud sur lequel vous activez la mise en grappe devient généralement le nœud de *contrôle*. Lorsque vous activez la mise en grappe sur les nœuds suivants, ils rejoignent la grappe en tant que nœuds de *données*.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité dans la configuration de démarrage. La priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds

de données. En règle générale, lorsque vous créez une grappe pour la première fois, le premier nœud que vous ajoutez devient le nœud de contrôle simplement parce que c'est le seul nœud de la grappe à ce moment-là.

Vous devez effectuer toute la configuration (à l'exception de la configuration de démarrage) sur le nœud de contrôle uniquement; la configuration est ensuite reproduite sur les nœuds de données. Dans le cas de ressources physiques, telles que les interfaces, la configuration du nœud de contrôle est reflétée sur tous les nœuds de données. Par exemple, si vous configurez Ethernet 1/2 comme interface interne et Ethernet 1/1 comme interface externe, ces interfaces sont également utilisées sur les nœuds de données en tant qu'interfaces interne et externe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

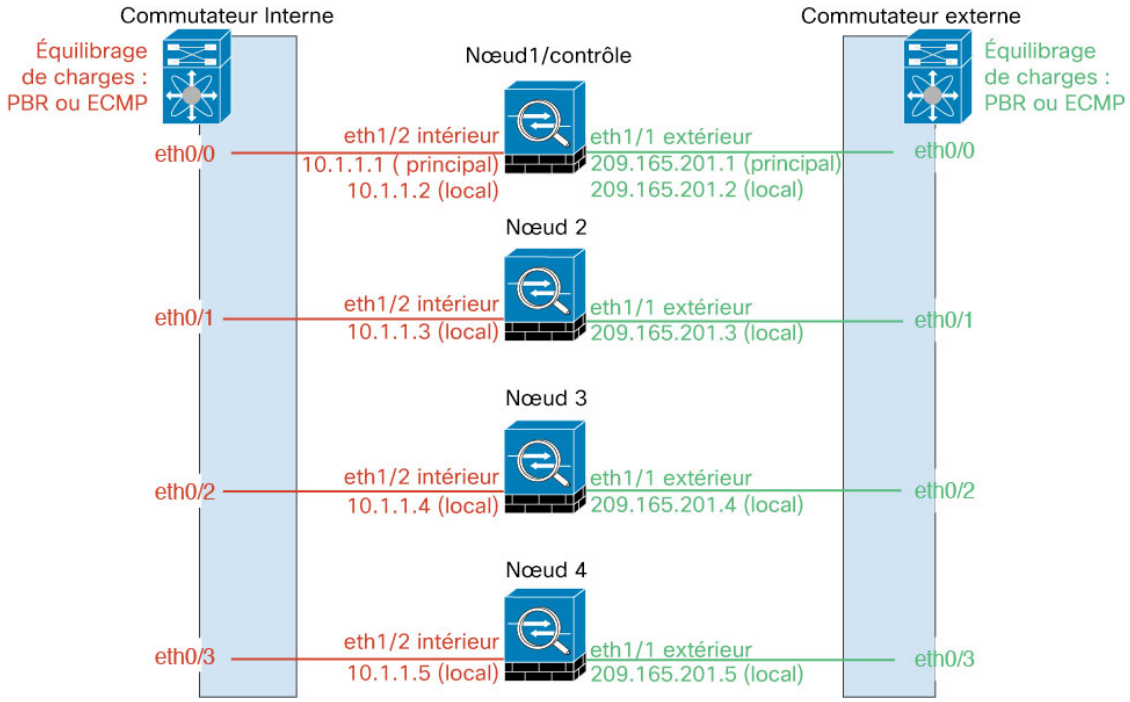
Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre *adresse IP locale* utilisée pour le routage. L'*adresse IP de la grappe principale* pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Comme la configuration de l'interface doit être configurée uniquement sur le nœud de contrôle, vous configurez un ensemble d'adresses IP à utiliser pour une interface donnée sur les nœuds de la grappe, y compris un pour le nœud de contrôle.

L'équilibrage de charge doit être configuré séparément sur le commutateur en amont.



Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Routage à base de règles

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Une méthode d'équilibrage de la charge est le routage basé sur les politiques (PBR).

Nous vous recommandons cette méthode si vous utilisez déjà PBR et que vous souhaitez tirer parti de votre infrastructure existante.

PBR prend des décisions de routage en fonction d'une carte de routage et d'une ACL. Vous devez répartir manuellement le trafic entre toutes les ASA d'une grappe. Comme PBR est statique, il se peut qu'il ne permette pas d'atteindre un résultat d'équilibrage de la charge optimale à tout moment. Pour obtenir les meilleures performances, nous vous recommandons de configurer la politique PBR de sorte que les paquets d'acheminement et de retour d'une connexion soient dirigés vers la même ASA.

Par exemple, si vous avez un routeur Cisco, la redondance peut être obtenue en utilisant Cisco IOS PBR avec Object Tracking. Le suivi d'objets Cisco IOS surveille chaque ASA à l'aide d'un ping ICMP. PBR peut ensuite activer ou désactiver les cartes de routage en fonction de l'accessibilité d'un ASA.

Routage à chemins multiples à coût égal

Lorsque vous utilisez des interfaces individuelles, chaque interface ASA conserve ses propres adresses IP et MAC. Le routage à chemins multiples à coûts égaux (ECMP) est une méthode d'équilibrage de la charge.

Nous vous recommandons cette méthode si vous utilisez déjà ECMP et que vous souhaitez tirer parti de votre infrastructure existante.

Considérations sur le routage ECMP

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants.

Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de l'ASA peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers l'ASA défaillant sera perdu.

Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque ASA pour qu'il participe au routage dynamique.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Interfaces VXLAN.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface ASA Virtual classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe ASA Virtual vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Échec de la liaison de commande de grappe

Si le protocole de liaison de commande de grappe tombe en panne pour une unité, la mise en grappe est désactivée; les interfaces de données sont fermées. Après avoir corrigé la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.

Remarque Lorsque l'ASA virtuel devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue du DHCP ou de l'ensemble d'adresses IP de la grappe. Si vous utilisez un ensemble d'adresses IP de grappe, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion n'est pas accessible (car elle utilise alors l'adresse IP principale, qui est la même que le nœud de contrôle). Vous devez utiliser le port de console (si disponible) pour toute autre configuration.

Test de ping de la MTU de la liaison de commande de grappe

Utilisez les tests ping MTU de liaison de commande de grappe pour

- vérifier la compatibilité de l'unité de transfert vérifier la compatibilité de la MTU entre les nœuds de la grappe au cours du processus de jonction,
- utiliser des tests de fragmentation basés sur le ping pour confirmer que le chemin réseau prend en charge le traitement approprié des paquets, et
- permettre aux nœuds de rejoindre la grappe même si les tests échouent, tout en fournissant des messages de diagnostic pour le dépannage des incompatibilités de MTU.

Lorsqu'un nœud rejoint la grappe, le nœud de contrôle envoie un ping avec une charge utile d'une taille égale à deux fois la MTU. Ce processus teste la capacité du réseau à gérer la fragmentation des paquets, car la couche IP sous-jacente fragmentera les paquets qui dépassent la limite de MTU.

Un ping réussi confirme que le chemin réseau prend en charge une fragmentation appropriée et que la liaison de commande de grappe peut traiter de manière fiable le trafic avec la MTU configurée.

Si le ping échoue, affichez ces messages :

- **show cluster history**—`Événement : échec du test CCL MTU pour l'unité` *name*
- Console AVERTISSEMENT—`AVERTISSEMENT : L'unité` *name* `n'est pas accessible dans le test ICMP de trame étendue CCL, veuillez vérifier l'interface de grappe et la configuration MTU du commutateur.`

Même si le message ping échoue, le nœud est autorisé à rejoindre la grappe. Dans ce cas, vous devez résoudre la non-concordance de MTU dès que possible.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Gestion des grappes ASA virtuel

L'un des avantages de l'utilisation de la mise en grappe ASA virtuel est la facilité de gestion. Cette section décrit comment gérer la grappe.

Réseau de gestion

Nous vous conseillons de connecter tous les nœuds à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Interface de gestion

Utilisez l'interface Management 0/0 pour la gestion.



Remarque Vous ne pouvez pas activer le routage dynamique pour l'interface de gestion. Vous devez utiliser une route statique.

Vous pouvez utiliser l'adressage statique ou DHCP pour l'adresse IP de gestion.

Si vous utilisez l'adressage statique, vous pouvez utiliser l'adresse IP de la grappe principale qui est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Pour chaque interface, vous configurez également une plage d'adresses de sorte que chaque nœud, y compris le nœud de contrôle actuel, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de gestion cohérent à une adresse; lorsqu'un nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'adresse IP locale est utilisée pour le routage et est également utile pour la résolution de problèmes. Par exemple, vous pouvez gérer la grappe en vous connectant à l'adresse IP de la grappe principale, qui est toujours associée au nœud de contrôle actuel. Pour gérer un membre, vous pouvez vous connecter à l'adresse IP locale. Pour le trafic de gestion sortant tel que TFTP ou le journal système, chaque nœud, y compris le nœud de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Si vous utilisez DHCP, vous n'utilisez pas un ensemble d'adresses locales ou n'avez pas d'adresse IP de grappe principale.



Remarque Le trafic vers la boîte doit être acheminé vers l'adresse IP de gestion du nœud; le trafic vers la boîte n'est pas transféré sur la liaison de commande de grappe vers un autre nœud.

Gestion de nœud de contrôle vs Gestion de nœud de données

La gestion et la surveillance peuvent avoir lieu sur le nœud de contrôle. À partir du nœud de contrôle, vous pouvez vérifier les statistiques d'exécution, l'utilisation des ressources ou d'autres informations de surveillance sur tous les nœuds. Vous pouvez également transmettre une commande à tous les nœuds de la grappe et reproduire les messages de console des nœuds de données vers le nœud de contrôle.

Vous pouvez surveiller directement les nœuds de données si vous le souhaitez. Bien que cela soit également disponible à partir du nœud de contrôle, vous pouvez effectuer la gestion de fichiers sur les nœuds de données (y compris la sauvegarde de la configuration et la mise à jour des images). Les fonctions suivantes ne sont pas disponibles à partir du nœud de commande :

- Surveillance des statistiques propres à la grappe par nœud.
- Surveillance des journaux système par nœud (sauf pour les journaux système envoyés à la console lorsque la duplication de la console est activée).
- SNMP

- NetFlow

duplication de clé de chiffrement

Lorsque vous créez une clé de chiffrement sur le nœud de contrôle, la clé est répliquée sur tous les nœuds de données. Si vous avez une session SSH sur l'adresse IP de la grappe principale, vous serez déconnecté en cas de défaillance du nœud de contrôle. Le nouveau nœud de contrôle utilise la même clé pour les connexions SSH, de sorte que vous n'avez pas besoin de mettre à jour la clé d'hôte SSH mise en cache lorsque vous vous reconnectez au nouveau nœud de contrôle.

Incompatibilité d'adresse IP du certificat de connexion ASDM

Par défaut, un certificat autosigné est utilisé pour la connexion ASDM en fonction de l'adresse IP locale. Si vous vous connectez à l'adresse IP de la grappe principale à l'aide d'ASDM, un message d'avertissement concernant une adresse IP non concordante peut s'afficher, car le certificat utilise l'adresse IP locale, et non l'adresse IP de la grappe principale. Vous pouvez ignorer le message et établir la connexion ASDM. Cependant, pour éviter ce type d'avertissement, vous pouvez inscrire un certificat qui contient l'adresse IP de la grappe principale et toutes les adresses IP locales de l'ensemble d'adresses IP. Vous pouvez ensuite utiliser ce certificat pour chaque membre de la grappe. Consultez https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html pour de plus amples renseignements.

Mise en grappe inter-sites

Pour les installations inter-sites, vous pouvez profiter de la mise en grappe d'ASA virtuel tant que vous suivez les lignes directrices recommandées.

Vous pouvez configurer chaque châssis de grappe pour qu'il appartienne à un ID de site distinct. Les ID de site sont utilisés pour permettre la mobilité de flux à l'aide de l'inspection LISP, la localisation du directeur pour améliorer les performances et réduire la latence aller-retour pour la mise en grappe inter-sites pour les centres de données, et la redondance des sites pour les connexions où un propriétaire de secours d'un flux se trouve toujours sur un autre site que celui du propriétaire.

Consultez les sections suivantes pour en savoir plus sur la mise en grappe inter-sites :

- Dimensionnement de l'interconnexion du centre de données : Exigences et conditions préalables à la mise en grappe d'ASA virtuel, à la page 9
- Lignes directrices inter-sites : Lignes directrices de la mise en grappe d'ASA virtuel, à la page 9
- Configurer la mobilité des flux de grappes : Configurer la mobilité des flux de grappes, à la page 30
- Activer la localisation du directeur : Configurer les paramètres de grappe ASA de base, à la page 25
- Activer la redondance de site : Configurer les paramètres de grappe ASA de base, à la page 25
- Exemples inter-sites : Exemple inter-sites nord-sud de mode routé d'interface individuelle, à la page 42

Licences pour la mise en grappe d'ASA virtuel

Chaque nœud de grappe nécessite la même licence de modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds

pour correspondre au membre le moins performant. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Remarque Si vous annulez l'enregistrement de l'ASA virtuel pour qu'il ne soit pas sous licence, il reviendra à un état de débit fortement limité si vous rechargez l'ASA virtuel. Un nœud de grappe sans licence et à faible performance aura une incidence négative sur les performances de l'ensemble de la grappe. Assurez-vous de conserver tous les nœuds de la grappe sous licence ou de supprimer les nœuds sans licence.

Exigences et conditions préalables à la mise en grappe d'ASA virtuel

Exigences du modèle

- ASAv30, ASAv50, ASAv100
- Les services en cloud privé suivants :
  - KVM
  - VMware
- Un maximum de 16 nœuds dans une grappe sur *deux* hôtes dans une configuration de déploiement 2 x 8. Nous vous conseillons de déployer un maximum de *huit* ASAv sur chacun des *deux* hôtes (2 x 8), ce qui donne une grappe de 16 nœuds.

Plateforme ASA virtuel et configuration logicielle requise

Tous les nœuds d'une grappe :

- Il doit s'agir du même modèle. Nous vous conseillons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Les nouveaux membres de la grappe doivent utiliser le même paramètre de chiffrement SSL (la commande **ssl encryption**) que le nœud de contrôle pour la communication de la liaison de commande de grappe initiale avant la réplication de la configuration.

Lignes directrices de la mise en grappe d'ASA virtuel

Basculement

Le basculement n'est pas pris en charge avec la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, activation ou désactivation d'une interface sur l'ASA ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité de l'interface.
- Lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Nous ne prenons pas en charge les VXLAN pour les interfaces de données; seule la liaison de commande de grappe prend en charge VXLAN.
- Il faut du temps pour répliquer les modifications sur toutes les unités d'une grappe. Si vous apportez une modification importante, par exemple, ajouter une règle de contrôle d'accès qui utilise des groupes d'objets (qui, lorsqu'ils sont déployés, sont divisés en plusieurs règles), le temps nécessaire pour effectuer la modification peut dépasser le délai d'expiration des nœuds de la grappe avec un message de réussite. Si cela se produit, vous pourriez voir le message « Échec de la réplication de la commande ». Vous pouvez ignorer le message.

Valeurs par défaut pour la mise en grappe d'ASA virtuel

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Le rééquilibrage de la connexion est désactivé par défaut. Si vous activez le rééquilibrage de la connexion, l'intervalle par défaut entre les échanges d'informations de chargement est de 5 secondes.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe d'ASA virtuel à l'aide d'une configuration Day0

Configuration Day0 du nœud de contrôle

La configuration Day0 suivante pour le nœud de contrôle comprend la configuration de démarrage suivie de la configuration d'interface qui sera répliquée sur les nœuds de données. Le texte en gras affiche les valeurs que vous devez modifier pour la configuration Day0 du nœud de données.

Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
```

```
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configuration Day0 du nœud de données

La configuration Day0 suivante pour le nœud de données inclut uniquement la configuration de démarrage. Le texte en gras affiche les valeurs que vous devez modifier à partir de la configuration Day0 du nœud de contrôle.

Remarque Cette configuration comprend uniquement la configuration centré sur la grappe. Votre configuration Day0 doit également inclure d'autres paramètres pour les licences, l'accès SSH , l'accès ASDM , etc. Consultez le guide de démarrage pour en savoir plus sur les configurations Day0.

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
```

```
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
```

```
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

Configurer la mise en grappe ASA virtuel après le déploiement

Pour configurer la mise en grappe après avoir déployé vos ASA virtuel, effectuez les tâches suivantes.

Sauvegarder vos configurations (conseillé)

Lorsque vous activez la mise en grappe sur une unité de données, la configuration actuelle est remplacée par une configuration synchronisée à partir de l'unité active. Si vous souhaitez quitter complètement la grappe, il peut être utile d'avoir une configuration de sauvegarde avec une configuration d'interface de gestion utilisable.

Avant de commencer

Effectuez une sauvegarde sur chaque unité.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Backup Configurations (Configurations de sauvegarde)**.

Étape 2 Sauvegardez au moins la configuration en cours d'exécution. Consultez Sauvegarde et restauration de configurations ou d'autres fichiers pour connaître la procédure détaillée.

Configurer les paramètres d'interface

Configurez le mode d'interface de grappe ainsi que les interfaces sur le nœud de contrôle. La configuration d'interface sera répliquée sur les nœuds de données lorsqu'ils rejoignent la grappe. Notez que la configuration de la laison de commande de grappe est traitée dans la procédure de configuration de démarrage.

Configurer le mode d'interface de grappe sur le nœud de contrôle

Avant d'activer la mise en grappe, vous devez convertir le pare-feu pour utiliser des interfaces individuelles. Étant donné que la mise en grappe limite les types d'interfaces que vous pouvez utiliser, ce processus vous permet de vérifier votre configuration existante pour détecter les interfaces incompatibles, puis vous empêche de configurer des interfaces non prises en charge.



Remarque Si vous n'ajoutez pas de nœuds de données à partir du nœud de contrôle, vous devez définir le mode d'interface manuellement sur tous les nœuds en fonction de cette section, pas seulement sur le nœud de contrôle; si vous ajoutez des nœuds de données à partir du nœud de contrôle, ASDM définit automatiquement le mode d'interface sur le nœud de données.

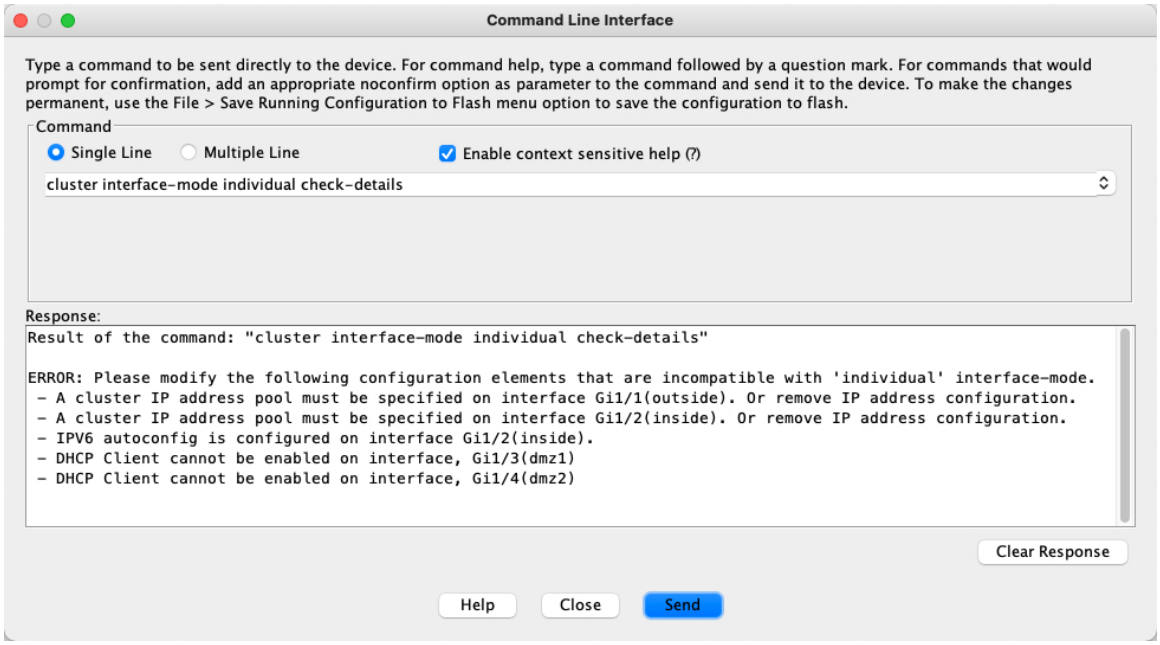
Procédure

Étape 1 Dans ASDM sur le nœud de contrôle, choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.Affichez toute configuration incompatible afin de pouvoir forcer le mode d'interface et corriger votre configuration ultérieurement; le mode n'est pas modifié avec cette commande :

cluster interface-mode individual check-details

Exemple :

Illustration 1 : Sortie de l'interface de commande en ligne



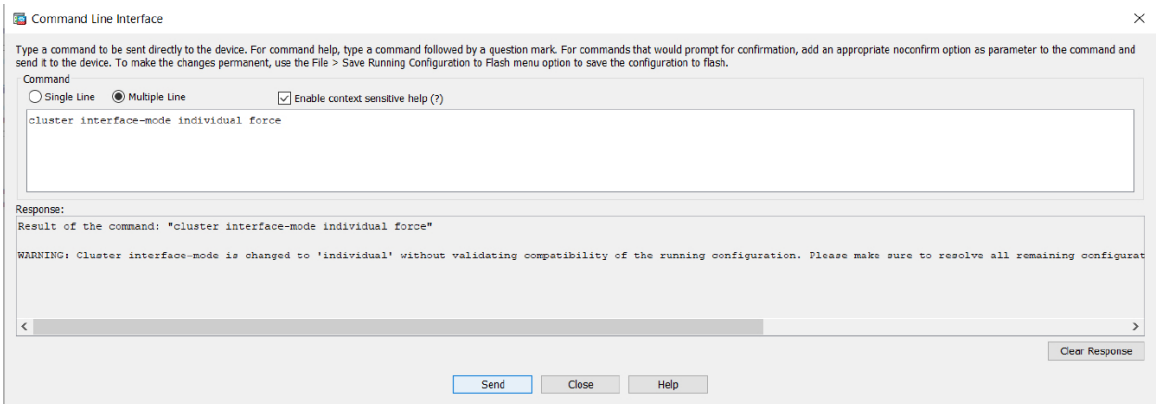
Mise en garde Après avoir défini le mode d'interface, vous pouvez continuer à vous connecter à l'interface; cependant, si vous rechargez l'ASA avant de configurer votre interface de gestion pour respecter les exigences de mise en grappe (par exemple, ajout d'un ensemble d'adresses IP de grappe ou obtention de l'adresse IP de DHCP), vous ne pourrez pas vous reconnecter, car la configuration d'interface incompatible avec la grappe est supprimée. Dans ce cas, vous devrez vous connecter au port de console, si disponible, pour corriger la configuration d'interface.

Étape 2 Définissez le mode d'interface pour la mise en grappe :

cluster interface-mode individual force

Exemple :

Illustration 2 : Définir le mode d'interface



Il n'y a pas de paramètres par défaut; vous devez choisir explicitement le mode. Si vous n'avez pas défini le mode, vous ne pouvez pas activer la mise en grappe.

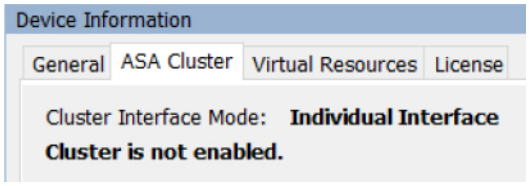
L'option **force** change le mode sans vérifier si votre configuration comporte des paramètres incompatibles. Vous devez résoudre manuellement tous les problèmes de configuration après avoir changé de mode. Étant donné que toute configuration d'interface ne peut être corrigée qu'après avoir défini le mode, nous vous conseillons d'utiliser l'option **force** afin de pouvoir au moins partir de la configuration existante. Vous pouvez réexécuter l'option **check-details** après avoir défini le mode pour obtenir plus de conseils.

Sans l'option **force**, en cas de configuration incompatible, vous êtes invité à effacer votre configuration et à la recharger, ce qui vous obligera à vous connecter au port de console (si disponible) pour reconfigurer votre accès de gestion. Si votre configuration est compatible (ce qui est rare), le mode est modifié et la configuration est conservée. Si vous ne souhaitez pas effacer votre configuration, vous pouvez quitter la commande en tapant **n**.

Pour supprimer le mode d'interface, saisissez la commande **no cluster interface-mode**.

Étape 3 Quittez ASDM et rechargez. ASDM doit être redémarré pour prendre correctement en compte le mode d'interface de la grappe. Après le rechargement, vous verrez l'onglet ASA Cluster (Grappe ASA) sur la page d'accueil :

Illustration 3 : ASDM doit être mis à jour



Configurer la liaison de commande de grappe sur le nœud de contrôle

Configurez une interface VXLAN pour l'interface de liaison de commande de grappe avant d'exécuter l'assistant. Pour en savoir plus sur VXLAN et la liaison de commande de grappe, consultez Liaison de commande de grappe, à la page 4.

Avant de commencer

Activez la réservation de bâti grand format pour une utilisation avec la liaison de commande de grappe, afin de pouvoir définir la MTU de la liaison de commande de grappe à la valeur conseillée. L'activation des bâtis grand format entraîne le rechargement de l'ASA. Consultez l'écran **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Remarque Vous devez activer la réservation de bâti grand format sur chaque nœud séparément.

Procédure

Étape 1 Identifiez les adresses IP des homologues du terminal de tunnel VXLAN (VTEP) dans un groupe d'objets réseau.

Consultez la page **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets réseau/Groupes)** et le chapitre « Objets pour le contrôle d'accès » du guide de configuration du pare-feu ASA pour en savoir plus sur les groupes d'objets réseau.

Le réseau IP sous-jacent entre les VTEP est indépendant du réseau de liaison de commande de grappe utilisé par les interfaces VNI (VXLAN Network Identifier). Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Étape 2 Configurez l'interface source VTEP.

L'interface source du VTEP est une interface ASA virtuel classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, et modifiez l'interface que vous souhaitez utiliser pour l'interface source VTEP.
b) Configurez l'**Interface Name** (Nom de l'interface).
c) Cochez la case **VTEP Source Interface (cluster)** (Interface source VTEP (grappe)).
d) Cochez **Enable Interface** (Activer l'interface).
e) Configurez une adresse IPv4 statique.

   L'adresse IP doit être incluse comme l'un des homologues dans le groupe d'objets réseau.

f) Cliquez sur l'onglet **Advanced** (Avancé) et définissez la **MTU** de la liaison de commande de grappe pour être au moins 154 octets supérieure à la MTU la plus élevée des interfaces de données.

   Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous conseillons de définir la MTU de liaison de commande de grappe à 1654 lorsque les interfaces de données sont fixées à 1500; cette valeur nécessite la réservation de bâti grand format, ce qui requiert un rechargement.

Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198.

g) Cliquez sur **OK**.

Étape 3 Associez l'interface source VTEP à l'instance du terminal de virtualisation du réseau (NVE).

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **VXLAN** .
b) (Facultatif) Saisissez une valeur dans **VXLAN Destination Port** (Port de destination VXLAN) si vous souhaitez modifier la valeur par défaut de 4789.
c) Cochez la case **Enable Network Virtualization Endpoint encapsulation using VXLAN** (Activer l'encapsulation du terminal de virtualisation du réseau à l'aide de VXLAN).
d) Choisissez l'option **VTEP Tunnel Interface** (Interface de tunnel VTEP) dans la liste déroulante.
e) Cochez la case **Configure Packet Recipient** (Configurer le destinataire des paquets), cliquez sur le bouton radio **Peer Group** (Groupe d'homologues) et choisissez le groupe d'homologues que vous avez créé.
f) Cliquez sur **Apply** (Appliquer).

Étape 4 Créez l'interface VNI.

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI.

a) Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et cliquez sur **Add (Ajouter)** > **VNI Interface (Interface VNI)**.
b) Saisissez le **VNI ID** (ID VNI) compris entre 1 et 10 000.

Cet ID est simplement un identifiant d'interface interne.

c) Saisissez le **VNI Segment ID** (ID de segment VNI) compris entre 1 et 16777215.

L'ID de segment est utilisé pour le balisage VXLAN.

d) Cochez la case **NVE Mapped to VTEP Interface** (NVE mappé à l'interface VTEP).

Ce paramètre associe l'interface VNI à l'interface source VTEP.

e) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer les interfaces individuelles

Vous devez modifier toute interface actuellement configurée avec une adresse IP pour qu'elle soit prête pour la grappe avant d'activer la mise en grappe. Au minimum, vous devrez peut-être modifier l'interface de gestion à laquelle ASDM est actuellement connecté lorsque vous utilisez une adresse IP statique pour la gestion. Pour les autres interfaces, vous pouvez les configurer avant ou après avoir activé la mise en grappe; nous vous conseillons de préconfigurer toutes vos interfaces afin que la configuration complète soit synchronisée avec les nouveaux nœuds de la grappe.

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe. Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui

appartient toujours au nœud de contrôle actuel. Toutes les interfaces de données doivent être des interfaces individuelles.

Pour l'interface de gestion, vous pouvez configurer un ensemble d'adresses IP ou utiliser le protocole DHCP; seule l'interface de gestion prend en charge l'obtention d'une adresse de DHCP. Pour utiliser DHCP, n'utilisez pas cette procédure; configurez-le plutôt comme d'habitude (voir Configurer les paramètres généraux de l'interface en mode routé).

Avant de commencer

- (Facultatif) Configurez les sous-interfaces.
- Pour l'interface de gestion, vous pouvez utiliser une adresse statique ou le protocole DHCP. Si vous utilisez des adresses IP statiques et que vous vous connectez à distance à l'interface de gestion à l'aide d'ASDM, l'adresse IP actuelle des nœuds de données potentiels est à usage temporaire.
  - Une adresse IP sera attribuée à chaque membre dans l'ensemble d'adresses IP de la grappe défini sur le nœud de contrôle.
  - L'ensemble d'adresses IP de la grappe ne peut pas inclure des adresses déjà utilisées sur le réseau, y compris de potentielles adresses IP secondaires.

    Par exemple :

    1. Vous configurez le nœud de contrôle pour qu'il utilise 10.1.1.1.
    2. Les autres nœuds utilisent 10.1.1.2, 10.1.1.3 et 10.1.1.4.
    3. Lorsque vous configurez l'ensemble d'adresses IP de la grappe sur le nœud de contrôle, vous ne pouvez pas inclure les adresses .2, .3 ou .4 dans l'ensemble, car elles sont déjà utilisées.
    4. Vous devez plutôt utiliser d'autres adresses IP sur le réseau, telles que .5, .6, .7 et .8.

Remarque L'ensemble a besoin d'autant d'adresses qu'il y a de membres dans la grappe, y compris le nœud de contrôle; l'adresse .1 d'origine est l'adresse IP principale de la grappe qui appartient au nœud de contrôle actuel.

    5. Après avoir rejoint la grappe, les anciennes adresses temporaires sont abandonnées et peuvent être utilisées ailleurs.

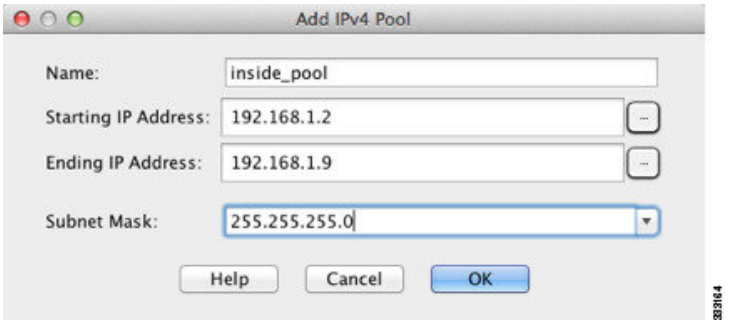
Procédure

Étape 1 Choisissez le volet**Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**). Choisissez **Use Static IP** (Utiliser l'adresse IP statique). Les protocoles DHCP et PPPoE ne sont pas pris en charge.

Étape 3 Pour ajouter l'ensemble d'adresses IP de la grappe IPv4, l'ensemble d'adresses MAC et les adresses MAC spécifiques au site, cliquez sur l'onglet **Advanced** (Avancé) et définissez les paramètres de la zone **ASA Cluster** (Grappe ASA).

a) Créez un ensemble d'adresses IP de grappe en cliquant sur le bouton **…** à côté du champ **IP Address Pool** (Ensemble d'adresses IP). La plage valide affichée est déterminée par l'adresse IP principale que vous avez définie dans l'onglet General (Général).
b) Cliquez sur **Add** (ajouter).
c) Configurez une plage d'adresses qui ne comprend pas l'adresse IP principale de la grappe et qui n'inclut aucune adresse actuellement utilisée sur votre réseau. Vous devez définir une plage suffisamment large pour la taille de la grappe, par exemple, 8 adresses.



d) Cliquez sur **OK** pour créer le nouvel ensemble.
e) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

   Le nom de l'ensemble apparaît dans le champ **IP Address Pool** (Ensemble d'adresses IP).

f) (Facultatif) (Facultatif) Configurez un **MAC Address Pool** (Ensemble d'adresses MAC) si vous souhaitez configurer manuellement des adresses MAC.

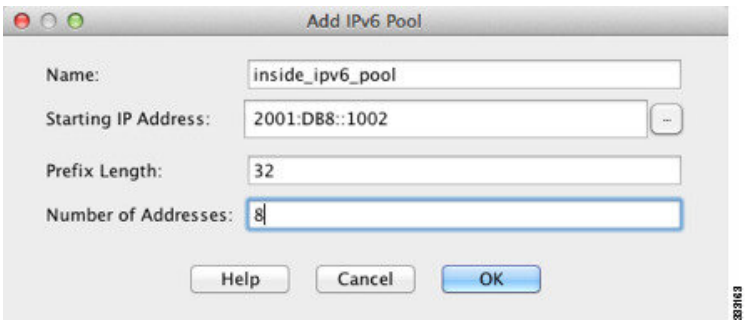
Étape 4 Pour configurer une adresse IPv6, cliquez sur l'onglet **IPv6**.

a) Cochez la case **Enable IPv6** (activer IPv6).
b) Dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

   L'option **Enable address autoconfiguration** (Activer l'autoconfiguration de l'adresse) n'est pas prise en charge. La configuration manuelle de l'adresse Link-Local n'est pas non plus prise en charge.

   La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

c) Dans le champ **Address/Prefix Length** (Longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale et la longueur du préfixe IPv6. Par exemple : 2001:0DB8::BA98:0:3210/48.
d) Cliquez sur le bouton **...** pour configurer l'ensemble d'adresses IP de la grappe.
e) Cliquez sur **Add** (ajouter).



f) Configurez l'adresse IP de départ (préfixe de réseau), la longueur du préfixe et le nombre d'adresses dans le groupe d'adresses.

g) Cliquez sur **OK** pour créer le nouvel ensemble.
h) Sélectionnez le nouvel ensemble que vous avez créé, cliquez sur **Assign** (Affecter), puis cliquez sur **OK**.

Le groupe apparaît dans le champ **ASA Cluster IP Pool** (Ensemble d'adresses IP de grappe ASA).

i) Cliquez sur **OK**.

Étape 5 Cliquez sur **OK** pour revenir au volet Interfaces.

Étape 6 Cliquez sur **Apply** (Appliquer).

Créer ou joindre une grappe à l'aide de l'assistant de haute disponibilité

Chaque nœud de la grappe nécessite une configuration de démarrage pour rejoindre la grappe. Exécutez l'assistant de haute disponibilité et évolutivité sur un nœud (qui deviendra le nœud de contrôle) pour créer la grappe, puis ajoutez-y des nœuds de données.

Avant de commencer

- L'interface source VXLAN VTEP que vous comptez utiliser pour l'interface de liaison de commande de grappe doit être à l'état activée sur le commutateur connecté.
- Lorsque vous ajoutez un nœud à une grappe en cours d'exécution, il se peut que vous constatiez des interruptions temporaires et limitées de paquets/connexions; c'est un comportement prévu.

Procédure

Étape 1 Choisissez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**. Consultez les instructions relatives à l'assistant dans les étapes suivantes.

Étape 2 Dans l'écran ASA Cluster Configuration (Configuration de la grappe ASA), configurez les paramètres de démarrage, notamment :

- **Member Priority (Priorité des membres)**— Définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Site Index** (Index du site) : si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC spécifique au site, entre 1 et 8.
- (Facultatif) **Shared Key (Clé partagée)** : Définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.
- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Si cette option est activée, les ASA d'une grappe échangent périodiquement des informations de chargement et déchargent les nouvelles connexions des appareils plus chargés vers les appareils moins chargés. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées.

Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.

Remarque Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique au sein de la grappe) : active la fonction de vérification de l'intégrité des nœuds de la grappe. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

  - **Time to Wait Before Device Considered Failed** (Temps d'attente avant que l'appareil ne soit reconnu comme défaillant) : cette valeur détermine la durée entre les messages d'état keepalive du nœud, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes.

- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe.
  - **MTU** : spécifiez l'unité de transfert maximale de l'interface source VTEP, qui doit être supérieure d'au moins 154 octets à la MTU la plus élevée des interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous suggérons de définir la MTU de liaison de commande de grappe à 1 654 lorsque les interfaces de données sont définies à 1 500; cette valeur nécessite la réservation de bâti grand format. Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle

aux nœuds de données. **Remarque :** Si vous n'avez pas de réservation de trame étendue pré-activée, vous devez quitter l'assistant, activer les trames étendues, puis relancer cette procédure.

Étape 3 Sur l'écran **Interfaces for Health Monitoring** (Interfaces de contrôle d'intégrité), vous pouvez exempter certaines interfaces de la surveillance en cas d'échec. Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion.



Remarque Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que le changement de configuration est synchronisé avec tous les nœuds, vous pouvez réactiver le contrôle de l'intégrité.

Étape 4 Dans l'écran **Interface Auto Rejoin settings** (Paramètres de la jonction automatique de l'interface), personnalisez les paramètres de la jonction automatique en cas de défaillance de l'interface ou de la liaison de commande de grappe. Pour chaque type, vous pouvez définir les paramètres suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données.

Étape 5 Cliquez sur **Finish** (Terminer).

Étape 6 L'ASA analyse la configuration en cours à la recherche de commandes incompatibles, en vue de cerner des fonctionnalités qui ne sont pas prises en charge avec la grappe, y compris les commandes pouvant être présentes dans la configuration par défaut. Cliquez sur **OK** pour supprimer les commandes incompatibles. Si vous cliquez sur **Cancel** (annuler), la mise en grappe n'est pas activée.

Après un certain temps, pendant qu'ASDM active la mise en grappe et se reconnecte à l'ASA, l'écran d'information apparaît pour confirmer que l'ASA a été ajouté à la grappe.

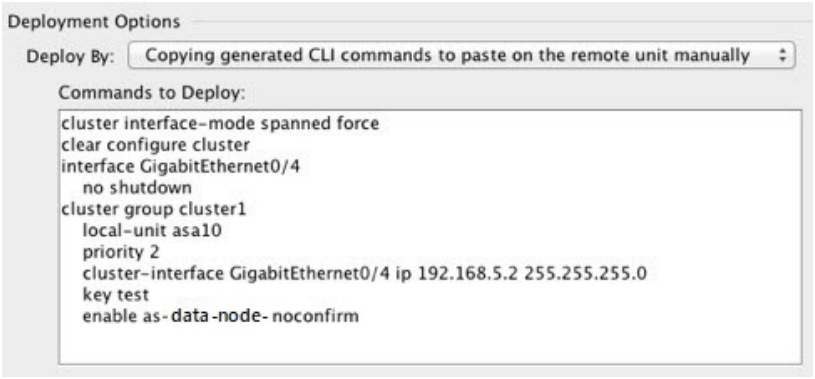
Remarque Dans certains cas, il se peut qu'une erreur se produise lors de la connexion à la grappe, une fois que le processus de l'assistant est terminé. Si ASDM a été déconnecté, ASDM ne recevra aucune erreur subséquente de l'ASA. Si la mise en grappe demeure désactivée après la reconnexion d'ASDM, vous devez vous connecter au port de console d'ASA pour déterminer la condition d'erreur exacte qui a désactivé la mise en grappe; par exemple, la liaison de commande de grappe peut être inactive.

Étape 7 Pour ajouter un nœud de données, cliquez sur **Yes (oui)**.

Si vous réexécutez l'assistant à partir du nœud de contrôle, vous pouvez ajouter des nœuds de données en choisissant l'option **Add another member to the cluster (ajouter un autre membre à la grappe)** lorsque vous lancez l'assistant pour la première fois.

Étape 8 Dans la zone des options de déploiement (**Deployment Options**), choisissez l'une des options suivantes (**Deploy By**) :

- **Envoi de commandes de l'interface de ligne de commande à l'unité distante maintenant—** Envoi de la configuration de démarrage à l'adresse IP de gestion du nœud de données (temporaire). Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.
- **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Personnaliser l'opération de mise en grappe

Vous pouvez personnaliser la surveillance de l'intégrité de la mise en grappe, le délai de réplication de la connexion TCP, la mobilité des flux et d'autres optimisations, dans le cadre de la configuration day0 ou après le déploiement de la grappe.

Exécutez ces procédures sur le nœud de contrôle.

Configurer les paramètres de grappe ASA de base

Vous pouvez personnaliser les paramètres de grappe sur le nœud de contrôle. Si vous n'utilisez pas l'assistant pour ajouter un nœud à la grappe, vous pouvez configurer les paramètres de grappe manuellement. Si vous avez déjà activé la mise en grappe, vous pouvez modifier certains paramètres de grappe; d'autres qui ne peuvent pas être modifiés lorsque la mise en grappe est activée sont grisés. Cette procédure inclut également les paramètres avancés qui ne sont pas inclus dans l'assistant.

Avant de commencer

- Si vous n'avez pas utilisé l'assistant et que vous souhaitez joindre manuellement la grappe, vous devez préconfigurer la liaison de commande de grappe sur chaque nœud avant de joindre la grappe. Consultez Configurer la liaison de commande de grappe sur le nœud de contrôle, à la page 16.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.

Si votre périphérique est déjà dans la grappe et qu'il s'agit du nœud de contrôle, ce volet se trouve dans l'onglet **Cluster Configuration** (Configuration de la grappe).

Étape 2 Cochez la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA).

Si vous décochez la case, les paramètres sont effacés. Ne cochez pas **Participate in ASA cluster** (Participer à la grappe ASA) avant d'avoir défini tous vos paramètres.

Remarque Après avoir activé la mise en grappe, ne décochez pas la case **Configure ASA cluster settings** (Configurer les paramètres de grappe ASA) sans comprendre les conséquences. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Configurez les paramètres de démarrage suivants :

- **Cluster Name** (Nom de la grappe) : nomme la grappe. Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères. Vous ne pouvez configurer qu'une seule grappe par nœud. Tous les membres de la grappe doivent utiliser le même nom.
- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Site Index** (Index du site) : si vous utilisez la mise en grappe inter-sites, définissez l'ID de site pour ce nœud afin qu'il utilise une adresse MAC spécifique au site, entre 1 et 8.
- (Facultatif) **Shared Key** (Clé partagée) : définit une clé de chiffrement pour le trafic de contrôle sur la liaison de commande de grappe. Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères.

Le secret partagé est utilisé pour générer la clé de chiffrement. Ce paramètre n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair. Vous devez configurer ce paramètre si vous activez également le service de chiffrement du mot de passe.

- (Facultatif) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster (Activer le rééquilibrage de connexion pour le trafic TCP sur tous les ASA de la grappe)** : permet de rééquilibrer la connexion. Le paramètre par défaut de ce filtre est désactivé. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données. Si cette option est activée, les ASA échangent périodiquement des renseignements sur les connexions par seconde et déchargent les nouvelles connexions des appareils ayant plus de connexions par seconde vers les appareils moins chargés. Les connexions existantes ne sont jamais déplacées. De plus, comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal. La fréquence, comprise entre 1 et 360 secondes, spécifie la fréquence à laquelle les informations de chargement sont échangées. La valeur par défaut est de 5 secondes.

  Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

  Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

- **Enable cluster load monitor** (Activer le moniteur de charge de la grappe) : vous pouvez superviser la charge de trafic pour les membres de la grappe, y compris le nombre total de connexions, l'utilisation du CPU et de la mémoire, ainsi que les abandons de tampon. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud si les nœuds restants peuvent gérer la charge ou de régler l'équilibrage de charges sur le commutateur externe. Cette fonction est activée par défaut. Vous pouvez superviser périodiquement la charge de trafic. Si la charge est trop élevée, vous pouvez choisir de désactiver manuellement la mise en grappe sur le nœud.

  Définissez les paramètres suivants :

  - **Time Interval** (Intervalle de temps) : définit le temps en secondes entre les messages de supervision, entre 10 et 360 secondes. La valeur par défaut est de 20 secondes.
  - **Number of Intervals** (Nombre d'intervalles) : définit le nombre d'intervalles pour lesquels l'ASA conserve les données, entre 1 et 60. La valeur par défaut est 30.

  Consultez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)** pour afficher la charge de trafic.

- (Facultatif) **Enable health monitoring of this device within the cluster** (Activer la surveillance de l'intégrité de ce périphérique dans la grappe) : active la fonctionnalité de vérification de l'intégrité des nœuds de la grappe et détermine le temps entre les messages d'état de pulsation des nœuds, entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes. **Remarque** : lorsque vous ajoutez de nouveaux nœuds à la grappe et apportez des modifications de topologie à l'ASA ou au commutateur, vous devez désactiver temporairement cette fonctionnalité jusqu'à ce que la grappe soit terminée et désactiver la supervision d'interface pour les interfaces désactivées (**Configuration** > **Device Management [Gestion des périphériques]** > **High Availability and Scalability [Haute disponibilité et évolutivité]** > **ASA Cluster [Grappe ASA]** > **Cluster Interface Health Monitoring [Surveillance de l'intégrité de l'interface de grappe]**). Vous pouvez réactiver cette fonctionnalité une fois les modifications apportées à la grappe et à la topologie terminées. Pour déterminer l'intégrité des nœuds, les nœuds de la grappe ASA envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.

- (Facultatif) **Debounce Time** (Délai antirebond) : configure le délai antirebond avant que l'ASA considère une interface comme défaillante et que le nœud ne soit supprimé de la grappe. Cette fonctionnalité permet une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, l'ASA attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Le délai antirebond par défaut est de 500 ms, avec une plage de 300 ms à 9 secondes.
- (Facultatif) **Replicate console output** (Répliquer l'extrant de la console) : permet la réplication de la console des nœuds de données vers le nœud de contrôle. Par défaut, cette fonction est désactivée. L'ASA peut imprimer certains messages directement sur la console pour certains événements critiques. Si vous activez la réplication de la console, les nœuds de données envoient les messages de la console au nœud de contrôle de sorte que vous ne devez surveiller qu'un seul port de console pour la grappe. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.
- (Facultatif) **Enable Clustering Flow Mobility** (Activer la mobilité des flux de grappes). Consultez Configurer l'inspection LISP, à la page 32.
- (Facultatif) **Enable Director Localization for inter-DC cluster** (Activer la localisation de directeur pour la grappe inter-DC) : pour améliorer les performances et réduire la latence d'aller-retour dans le cas de la mise en grappe inter-sites pour les centres de données, vous pouvez activer la localisation de directeur. Les nouvelles connexions sont généralement équilibrées et appartiennent aux membres de la grappe d'un site donné. Cependant, l'ASA attribue le rôle de directeur à un membre sur *n'importe quel* site. La localisation du directeur permet des rôles de directeur supplémentaires : un directeur local sur le même site que le propriétaire et un directeur global qui peut se trouver sur n'importe quel site. Le fait de garder le propriétaire et le directeur sur le même site améliore les performances. De plus, en cas de défaillance du propriétaire d'origine, le directeur local choisit un nouveau propriétaire de connexion sur le même site. Le directeur global est utilisé si un membre d'une grappe reçoit des paquets pour une connexion appartenant à un autre site.
- (Facultatif) **Site Redundancy** (Redondance de site) : pour protéger les flux contre une défaillance de site, vous pouvez activer la redondance de site. Si le propriétaire de connexion de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La localisation de directeur et la redondance de site sont des fonctionnalités distinctes; vous pouvez configurer l'un ou l'autre, ou configurer les deux.
- (Facultatif) **Enable config sync acceleration** (Activer l'accélération de la synchronisation de la configuration) : lorsqu'un nœud de données a la même configuration que le nœud de contrôle, il ignorera la synchronisation de la configuration et se joindra plus rapidement. Cette fonction est activée par défaut. Cette fonctionnalité est configurée sur chaque nœud et n'est pas répliquée du nœud de contrôle au nœud de données.

Remarque Certaines commandes de configuration ne sont pas compatibles avec la jonction accélérée de grappes; si ces commandes sont présentes sur le nœud, même si la jonction accélérée de grappes est activée, la synchronisation de la configuration se produira toujours. Vous devez supprimer la configuration incompatible pour que la jonction accélérée de grappes fonctionne. Utilisez la commande **show cluster info unit-join-acceleration incompatible-config** pour afficher la configuration incompatible.

- **Enable parallel configuration replicate** (Activer la réplication de configuration parallèle) : permet au nœud de contrôle de synchroniser les modifications de configuration avec les nœuds de données en parallèle. Sinon, la synchronisation a lieu de manière séquentielle et peut prendre plus de temps.
- **Cluster Control Link** (Liaison de commande de grappe) : spécifie l'interface de liaison de commande de grappe.
  - **Interface** : spécifie l'interface VNI.
  - **IP Address** (Adresse IP) : spécifie une adresse IPv4 pour l'adresse IP; IPv6 n'est pas pris en charge pour cette interface.
  - **Subnet Mask** (Filtre d'adresse locale) : spécifie le filtre d'adresse locale.
  - **MTU** : spécifie l'unité de transfert maximale de l'interface source VTEP, qui doit être supérieure d'au moins 154 octets à la MTU la plus élevée des interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets). Définissez la MTU entre 1 554 et 9 198 octets. Par défaut, la MTU est de 1554 octets. Nous vous suggérons de définir la MTU de liaison de commande de grappe à 1 654 lorsque les interfaces de données sont définies à 1 500; cette valeur nécessite la réservation de bâti grand format. Par exemple, lors de l'utilisation d'un bâti grand format, comme la MTU maximale est de 9 198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9 044, tandis que la liaison de commande de grappe peut être définie sur 9 198. Ce paramètre ne fait pas partie de la configuration de démarrage, et est répliqué du nœud de contrôle aux nœuds de données.

    Remarque : si vous n'avez pas activé au préalable la réservation de bâti grand format, activez les bâtis grand format, puis recommencez cette procédure.

Étape 4 Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA) pour rejoindre la grappe.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer les paramètres de surveillance de l'intégrité de l'interface et de jonction automatique

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Interface Health Monitoring (Surveillance de l'intégrité de l'interface de grappe)**.

Étape 2 Dans la zone **Monitored Interfaces** (Interfaces surveillées), sélectionnez une interface et cliquez sur **Add** (Ajouter) pour la déplacer vers la zone **Unmonitored Interfaces** (Interfaces non surveillées).

Les messages d'état de l'interface détectent une défaillance de liaison. Si un nœud ne reçoit pas de messages d'état d'interface dans le délai de rétention, le temps avant que l'ASA ne supprime un membre de la grappe dépend du fait que le nœud soit un membre établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces.

Vous pouvez désactiver la surveillance de l'intégrité des interfaces non essentielles, par exemple, l'interface de gestion. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur l'ASA ou le commutateur), vous devez désactiver le contrôle d'intégrité (**Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**) et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver le contrôle d'intégrité.

Étape 3 Cliquez sur l'onglet **Auto Rejoin** (Jonction automatique) pour personnaliser les paramètres de la jonction automatique en cas de défaillance de l'interface, du système ou de la liaison de commande de grappe. Pour chaque type, cliquez sur **Edit** (Modifier) pour définir les éléments suivants :

- **Maximum Rejoin Attempts** (Nombre maximal de tentatives de jonction) : Permet de définir le nombre de tentatives de jonction à la grappe en sélectionnant **Unlimited** (Illimité) ou une valeur comprise entre 0 et 65 535. **0** désactive la jonction automatique. La valeur par défaut est **Unlimited** (Illimité) pour l'interface de grappe et **3** pour l'interface de données et le système.
- **Rejoin Interval** (Intervalle de jonction) : permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est **5** minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente en définissant la variation d'intervalle entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente) ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l'interface de grappe et **2** pour l'interface de données et le système.

Cliquez sur **Restore Defaults** pour rétablir les paramètres par défaut.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer le délai de réplication TCP de la grappe

Activez le délai de réplication de la grappe pour les connexions TCP pour aider à éliminer le « travail inutile » lié aux flux de courte durée en retardant la création du flux directeur/de sauvegarde. Notez que si une unité tombe en panne avant la création du flux directeur/de sauvegarde, ces flux ne peuvent pas être récupérés. De même, si le trafic est rééquilibré vers une autre unité avant la création du flux, le flux ne peut pas être récupéré. Vous ne devez pas activer la réplication TCP pour le trafic sur lequel vous désactivez la répartition aléatoire TCP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster Replication (Réplication de la grappe ASA)**.

Étape 2 Cliquez sur **Add** (Ajouter) et réglez les valeurs suivantes :

- **Replication delay** (Délai de réplication) : définissez les secondes entre 1 et 15.
- **HTTP** : définissez le délai pour tout le trafic HTTP.
- **Critères de source**
  - **Source** : définissez l'adresse IP source.
  - **Service** : (Facultatif) Définissez le port source. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.
- **Critères de destination**
  - **Source** : définissez l'adresse IP de destination.
  - **Service** : (Facultatif) Définissez le port de destination. En général, vous définissez soit le port source, soit le port de destination, mais pas les deux.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer les fonctionnalités inter-sites

Pour la mise en grappe inter-sites, vous pouvez personnaliser votre configuration pour améliorer la redondance et la stabilité.

Configurer la mobilité des flux de grappes

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

À propos de l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux entre les sites.

À propos de LISP

La mobilité des machines virtuelles de centres de données, comme VMware VMotion, permet aux serveurs de migrer entre les centres de données tout en maintenant les connexions avec les clients. Pour prendre en charge une telle mobilité de serveur de centre de données, les routeurs doivent être en mesure de mettre à jour la route d'entrée vers le serveur lorsqu'il se déplace. L'architecture Cisco Locator/Protocole de séparation d'ID (LISP) sépare l'identité du périphérique, ou l'identifiant de terminal (EID), de son emplacement, ou localisateur de routage, dans deux espaces de numérotation différents, ce qui rend la migration du serveur

transparente pour les clients. Par exemple, lorsqu'un serveur est déplacé vers un nouveau site et qu'un client envoie du trafic vers le serveur, le routeur redirige le trafic vers le nouvel emplacement.

LISP nécessite des routeurs et des serveurs dans certains rôles, tels que le routeur de tunnel de sortie (ETR) LISP, le routeur de tunnel d'entrée (ITR), les routeurs de premier saut, le résolveur de carte (MR) et le serveur de carte (MS). Lorsque le routeur du premier saut du serveur détecte que le serveur est connecté à un autre routeur, il met à jour tous les autres routeurs et les bases de données afin que l'ITR connectée au client puisse intercepter, encapsuler et envoyer le trafic vers le nouvel emplacement du serveur.

Prise en charge du LISP ASA

L'ASA n'exécute pas le LISP lui-même; il peut, cependant, inspecter le trafic LISP pour détecter les changements d'emplacement, puis utiliser ces informations pour un fonctionnement de mise en grappe transparent. Sans l'intégration du LISP, lorsqu'un serveur est déplacé vers un nouveau site, le trafic est acheminé vers un membre de la grappe ASA sur le nouveau site plutôt que vers le propriétaire d'origine du flux. Le nouvel ASA transfère le trafic vers l'ASA au niveau de l'ancien site, puis l'ancien ASA doit renvoyer le trafic vers le nouveau site pour qu'il atteigne le serveur. Ce flux de trafic est sous-optimal et est connu comme « tromboning » ou « épingle à cheveux ».

Grâce à l'intégration du LISP, les membres de la grappe ASA peuvent inspecter le trafic LISP passant entre le routeur du premier saut et l'ETR ou l'ITR, puis peuvent changer le propriétaire du flux pour qu'il se trouve sur le nouveau site.

Lignes directrices LISP

- Les membres de la grappe ASA doivent se trouver entre le routeur du premier saut et l'ITR ou l'ETR du site. La grappe ASA elle-même ne peut pas être le premier routeur de saut pour un segment étendu.
- Seuls les flux entièrement distribués sont pris en charge; les flux centralisés, les flux semi-distribués ou les flux appartenant à des nœuds individuels ne sont pas transférés vers de nouveaux propriétaires. Les flux semi-distribués comprennent des applications, telles que SIP, où tous les flux enfants appartiennent au même ASA qui possède le flux parent.
- La grappe déplace uniquement les états de flux de couche 3 et 4; certaines données d'application pourraient être perdues.
- Pour les flux de courte durée ou non essentiels pour l'entreprise, le déplacement du propriétaire peut ne pas valoir la peine. Vous pouvez contrôler les types de trafic pris en charge avec cette fonctionnalité lorsque vous configurez la politique d'inspection. Vous devez limiter la mobilité de flux au trafic essentiel.

Mise en œuvre du LISP ASA

Cette fonctionnalité comprend plusieurs configurations interdépendantes (qui sont toutes décrites dans ce chapitre) :

1. (Facultatif) Limiter les EID inspectés en fonction de l'adresse IP de l'hôte ou du serveur : le routeur de premier saut pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée, vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.
2. Inspection du trafic LISP : l'ASA inspecte le trafic LISP sur le port UDP 4342 pour détecter le message EID-notify envoyé entre le premier saut du routeur et l'ITR ou l'ETR. L'ASA gère un tableau EID qui met en corrélation l'EID et l'ID de site. Par exemple, vous devez inspecter le trafic LISP avec une adresse IP source du routeur du premier saut et une adresse de destination de l'ITR ou de l'ETR. Remarque : le

trafic LISP n'a pas de directeur affecté et le trafic LISP en lui-même ne participe pas au partage de l'état de la grappe.

3. Politique de service pour activer la mobilité des flux sur le trafic spécifié : vous devez activer la mobilité des flux sur le trafic critique. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques.
4. ID de sites : l'ASA utilise l'ID de site pour chaque nœud de la grappe afin de déterminer le nouveau propriétaire.
5. Configuration au niveau de la grappe pour activer la mobilité de flux : vous devez également activer la mobilité de flux au niveau de la grappe. Ce bouton bascule marche/arrêt vous permet d'activer ou de désactiver facilement la mobilité de flux pour une classe particulière de trafic ou d'applications.

Configurer l'inspection LISP

Vous pouvez inspecter le trafic LISP pour activer la mobilité des flux lorsqu'un serveur se déplace entre les sites.

Avant de commencer

- Affectez chaque unité de grappe à un ID de site en fonction de Configurer les paramètres de grappe ASA de base, à la page 25.
- Le trafic LISP n'est pas inclus dans la classe de trafic d'inspection par défaut. Vous devez donc configurer une classe distincte pour le trafic LISP dans le cadre de cette procédure.

Procédure

Étape 1 (Facultatif) Configurez une carte d'inspection LISP pour limiter les EID inspectés en fonction de l'adresse IP et pour configurer la clé partagée LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **LISP**.
b) Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
c) Saisissez un nom (40 caractères maximum) et une description.
d) Pour la commande **Allowed-EID access-list**, cliquez sur **Manage** (Gérer).

Le **gestionnaire ACL** s'ouvre.

Le routeur de premier saut ou l'ITR/ETR pourrait envoyer des messages de notification d'EID pour les hôtes ou les réseaux dans lesquels la grappe ASA n'est pas impliquée; vous pouvez donc limiter les EID à ces serveurs ou réseaux pertinents pour votre grappe. Par exemple, si la grappe ne concerne que 2 sites, mais que le LISP est exécuté sur 3 sites, vous ne devez inclure les EID que pour les 2 sites de la grappe.

e) Ajoutez une ACL avec au moins un ACE en fonction du guide de configuration du pare-feu.
f) Si nécessaire, saisissez la **Validation Key** (Clé de validation).

Si vous avez copié une clé chiffrée, cliquez sur le bouton radio **Encrypted** (Chiffré).

g) Cliquez sur **OK**.

Étape 2 Ajoutez une règle de politique de service pour configurer l'inspection LISP :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Dans la page **Service Policy** (Politique de service), appliquez la règle à une interface ou globalement.

   Si vous avez une politique de service existante que vous souhaitez utiliser, ajoutez une règle à cette politique. Par défaut, l'ASA comprend une politique globale appelée **global_policy**. Vous pouvez également créer une politique de service par interface si vous ne souhaitez pas appliquer la politique à l'échelle mondiale. L'inspection LISP est appliquée au trafic de manière bidirectionnelle, vous n'avez donc pas besoin d'appliquer la politique de service sur les interfaces source et de destination; tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la règle est affecté si le trafic correspond à la carte dans les deux sens.

d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).
f) Spécifiez le trafic que vous souhaitez inspecter. Vous devez spécifier le trafic entre le routeur de premier saut et l'ITR ou l'ETR sur le port UDP 4342. Les ACL IPv4 et IPv6 sont acceptées.
g) Cliquez sur **Next** (suivant).
h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Protocol Inspection** (Inspection du protocole).
i) Cochez la case **LISP**.
j) (Facultatif) Cliquez sur **Configure** (Configurer) pour choisir la carte d'inspection que vous avez créée.
k) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 3 Ajoutez une règle de politique de service pour activer la mobilité des flux pour le trafic critique :

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
b) Cliquez sur **Add** (ajouter).
c) Sur la page **Service Policy** (Politique de service), choisissez la même politique de service que vous avez utilisée pour l'inspection LISP.
d) Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), cliquez sur **Create a new traffic class** (Créer une nouvelle classe de trafic), et sous **Traffic Match Criteria** (Critères de correspondance du trafic), cochez la case **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL)).
e) Cliquez sur **Next** (suivant).
f) Spécifiez le trafic opérationnel critique que vous souhaitez réaffecter au site le plus optimal lorsque les serveurs changent de site. Par exemple, vous pouvez limiter la mobilité de flux au trafic HTTPS uniquement et/ou au trafic vers des serveurs spécifiques. Les ACL IPv4 et IPv6 sont acceptées.
g) Cliquez sur **Next** (suivant).
h) Sur la page ou l'onglet de l'assistant **Rule Actions** (Actions de règles), sélectionnez l'onglet **Cluster** (Grappe).
i) Cochez la case **Enable Cluster flow-mobility triggered by LISP EID messages** (Activer la mobilité des flux de grappe déclenchée par les messages LISP EID).
j) Cliquez sur **Finish** (Terminer) pour enregistrer la règle de politique de service.

Étape 4 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration**

(Configuration de la grappe) > **et cochez la case Enable Clustering flow mobility** (Activer la mobilité des flux de la grappe).

Étape 5 Cliquez sur **Apply** (Appliquer).

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

Ajouter un nouveau nœud de données à partir du nœud de contrôle

Vous pouvez ajouter des nœuds de données supplémentaires à la grappe à partir du nœud de contrôle. Vous pouvez également ajouter des nœuds de données à l'aide de l'assistant de haute disponibilité et d'évolutivité. L'ajout d'un nœud de données à partir du nœud de contrôle a l'avantage de configurer la liaison de commande de grappe et de définir le mode d'interface de grappe sur chaque nœud de données que vous ajoutez.

Vous pouvez également vous connecter au nœud de données et configurer la mise en grappe directement sur ce dernier. Cependant, après avoir activé la mise en grappe, votre session ASDM sera déconnectée et vous devrez vous reconnecter.

Avant de commencer

- Si vous souhaitez envoyer la configuration de démarrage sur le réseau de gestion, assurez-vous que le nœud de données a une adresse IP accessible.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

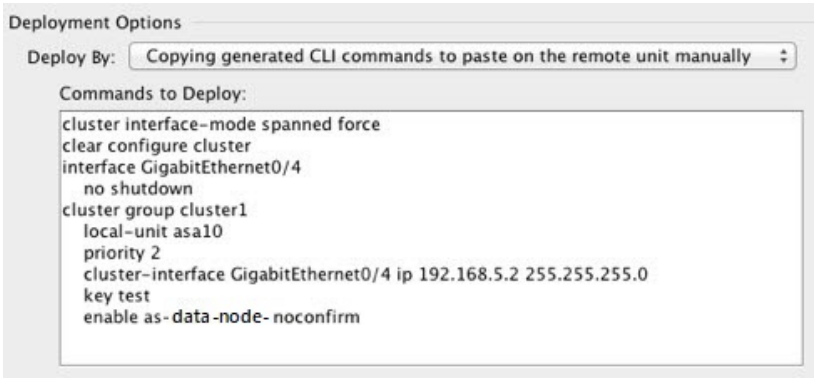
Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Configurez selon les paramètres suivants :

- **Member Name** (Nom de membre) : nomme ce membre de la grappe avec une chaîne ASCII unique de 1 à 38 caractères.
- **Member Priority** (Priorité des membres) : définit la priorité de ce nœud pour les élections du nœud de contrôle, entre 1 et 100, où 1 est la priorité la plus élevée.
- **Cluster Control Link > IP Address** (Liaison de commande de grappe > Adresse IP) : spécifie une adresse IP unique pour ce membre pour la liaison de commande de grappe, sur le même réseau que la liaison de commande de grappe du nœud de contrôle.
- Dans la zone **Deployment Options** (Options de déploiement), choisissez l'une des options **Deploy By** (Déployer par) suivantes :
  - **Sending CLI commands to the remote unit now** (Envoi des commandes de l'interface de ligne de commande vers l'unité distante maintenant) : permet d'envoyer la configuration de démarrage

à l'adresse IP de gestion (temporaire) de l'unité de données. Saisissez l'adresse IP de gestion du nœud de données, le nom d'utilisateur et le mot de passe.

- **Copie des commandes de l'interface de ligne de commande générées pour les coller manuellement sur l'unité distante**— génère les commandes afin que vous puissiez les couper et les coller sur l'interface de commande du nœud de données ou à l'aide de l'outil de l'interface de ligne de commande dans ASDM. Dans la zone des commandes à déployer, sélectionnez et copiez les commandes générées pour une utilisation ultérieure.



Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Devenir un nœud inactif

Pour devenir un membre inactif de la grappe, désactivez la mise en grappe sur le nœud tout en laissant intacte la configuration de mise en grappe.

Remarque Lorsqu'un ASA devient inactif (soit manuellement, soit à la suite d'un échec du contrôle d'intégrité), toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe; ou vous pouvez supprimer complètement le nœud de la grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), alors l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)**.

Étape 2 Décochez la case **Participer à la grappe ASA**.

Remarque Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Étape 3 Cliquez sur **Apply** (Appliquer).

Désactiver un nœud de données à partir du nœud de contrôle

Pour désactiver un nœud de données, procédez comme suit.

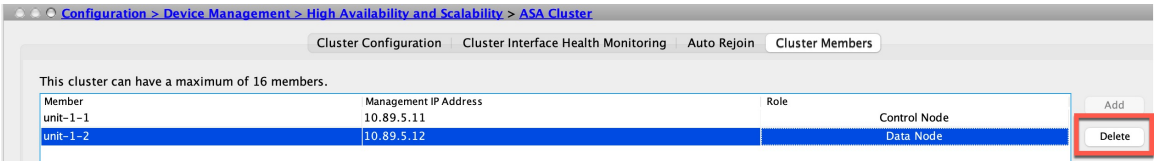
Remarque Lorsqu'un ASA devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe (par exemple, vous avez enregistré la configuration avec la mise en grappe désactivée), l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.

Étape 2 Sélectionnez le nœud de données que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).

Illustration 4 : Supprimer un nœud



La configuration de démarrage du nœud de données reste inchangée afin que vous puissiez rajouter le nœud de données ultérieurement sans perdre votre configuration.

Étape 3 Cliquez sur **Apply** (Appliquer).

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement un membre, vous devez rejoindre manuellement la grappe.

Procédure

Étape 1 Si vous avez toujours l'accès à ASDM, vous pouvez réactiver la mise en grappe dans ASDM en connectant ASDM au nœud que vous souhaitez réactiver.

Vous ne pouvez pas réactiver la mise en grappe pour un nœud de données à partir du nœud de contrôle, sauf si vous l'ajoutez en tant que nouveau membre.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**.
b) Cochez la case **Participate in ASA cluster** (Participer à la grappe ASA).
c) Cliquez sur **Apply** (Appliquer).

Étape 2 Si vous ne pouvez pas utiliser ASDM : Sur la console, passez en mode de configuration de grappe :

cluster group *name*

Exemple :

```
ciscoasa(config)# cluster group pod1
```

Étape 3 Activez la mise en grappe.

enable

Quitter la grappe

Si vous souhaitez quitter complètement la grappe, vous devez supprimer toute la configuration de démarrage de la grappe. Étant donné que la configuration actuelle sur chaque nœud est la même (synchronisée à partir de l'unité active), quitter la grappe implique également de restaurer une configuration antérieure à la grappe à partir d'une sauvegarde ou d'effacer votre configuration et de recommencer pour éviter les conflits d'adresses IP.

Procédure

Étape 1 Pour un nœud de données, désactivez la mise en grappe :

cluster group *cluster_name* **no enable**

Exemple :

```
ciscoasa(config)# cluster group cluster1
```

```
ciscoasa(cfg-cluster)# no enable
```

Vous ne pouvez pas modifier la configuration lorsque la mise en grappe est activée sur un nœud de données.

Étape 2 Effacez la configuration de la grappe :

clear configure cluster

L'ASA désactive toutes les interfaces, y compris l'interface de gestion et la liaison de commande de grappe.

Étape 3 Désactivez le mode d'interface de la grappe :

no cluster interface-mode

Le mode n'est pas stocké dans la configuration et doit être réinitialisé manuellement.

Étape 4 Si vous avez une configuration de sauvegarde, copiez-la dans la configuration en cours d'exécution :

copy *backup_cfg* **running-config**

Exemple :

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

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

Étape 5 Enregistrez la configuration pour le démarrage :

write memory

Étape 6 Si vous n'avez pas de configuration de sauvegarde, reconfigurez l'accès de gestion. Par exemple, assurez-vous de modifier les adresses IP de l'interface et de restaurer le bon nom d'hôte.

Modifier le nœud de contrôle



Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez spécifier le nœud exact que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez toutefois que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle à l'aide de cette procédure, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Summary (Résumé de la grappe)**.

Étape 2 Dans la liste déroulante, choisissez un nœud de données pour devenir le contrôle et cliquez sur le bouton pour en faire le nœud de contrôle.

Étape 3 Vous êtes invité à confirmer le changement de nœud de contrôle. Cliquez sur **Oui**.

Étape 4 Quittez ASDM et reconnectez-vous en utilisant l'adresse IP de la grappe principale.

Exécuter une commande à l'échelle de la grappe

Pour envoyer une commande à tous les nœuds de la grappe ou à un nœud en particulier, procédez comme suit. L'envoi d'une commande **show** à tous les nœuds collecte toutes les sorties et les affiche sur la console du nœud actuel. D'autres commandes, telles que **capture** et **copy**, peuvent également profiter d'une exécution à l'échelle de la grappe.

Avant de commencer

Effectuez cette procédure au niveau de l'outil d'interface de ligne de commande : choisissez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

Procédure

Envoyez une commande à tous les nœuds ou, si vous spécifiez le nom du nœud, à un nœud en particulier :

cluster exec [**unit** *node_name*] *command*

Exemple :

```
ciscoasa# cluster exec show xlate
```

Pour afficher les noms de nœud, saisissez **cluster exec unit ?** (unité d'exécution de grappe?) (pour voir tous les noms à l'exception du nœud actuel), ou saisissez la commande **show cluster info**.

Exemples

Pour copier simultanément le même fichier de capture de tous les nœuds de la grappe vers un serveur TFTP, saisissez la commande suivante sur le nœud de contrôle :

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Plusieurs fichiers PCAP, un pour chaque nœud, sont copiés sur le serveur TFTP. Le nom du fichier de capture de destination est automatiquement associé au nom du nœud, par exemple capture1_asa1.pcap, capture1_asa2.pcap, etc. Dans cet exemple, asa1 et asa2 sont des noms de nœuds de grappe.

Supervision de la grappe ASA virtuel

Vous pouvez superviser et dépanner l'état de la grappe et les connexions.

Supervision de l'état de la grappe

Consultez les écrans suivantes pour superviser l'état de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Cluster Summary (Résumé de la grappe)**

  Ce volet affiche des renseignements sur la grappe concernant le nœud auquel vous êtes connecté, ainsi que les autres nœuds de la grappe. Vous pouvez également modifier le nœud principal à partir de ce volet.

- **Tableau de bord de la grappe**

  Sur la page d'accueil du nœud principal, vous pouvez superviser la grappe à l'aide des tableaux de bord de grappe et de pare-feu de grappe.

Capture des paquets à l'échelle de la grappe

Consultez l'écran suivante pour capturer des paquets dans une grappe :

Wizards (Assistants) > Packet Capture Wizard (Assistant de capture de paquets)

Pour prendre en charge le dépannage à l'échelle de la grappe, vous pouvez activer la capture du trafic spécifique à la grappe sur le nœud de contrôle, qui est ensuite automatiquement activée sur tous les nœuds de données de la grappe.

Supervision des ressources de la grappe

Consultez les écrans suivants pour surveiller les ressources de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > CPU (Processeur)**

  Ce volet vous permet de créer des graphiques ou des tableaux montrant l'utilisation du processeur sur les nœuds de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > System Resources Graphs (Graphiques de ressources système) > Memory (Mémoire)**. Ce volet vous permet de créer des graphiques ou des tableaux montrant la mémoire libre et la mémoire utilisée sur les nœuds de la grappe.

Supervision du trafic de la grappe

Consultez les commandes suivants pour superviser le trafic de la grappe :

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Connections (Connexions)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant les connexions entre les membres de la grappe.

- **Monitoring (Supervision) > ASA Cluster (Grappe ASA) > Trafic Graphs (Graphiques du trafic) > Throughput (Débit)**.

  Ce volet vous permet de créer des graphiques ou des tableaux montrant le débit du trafic entre les membres de la grappe.

- **Monitoring (Supervision)** > **ASA Cluster (Grappe ASA)** > **Cluster Load-Monitoring (Supervision de la charge de la grappe)**

  Cette section comprend les volets **Load Monitor-Information** (Renseignements sur le moniteur de charge) et **Load-Monitor Details** (Détails du moniteur de charge). **Load Monitor-Information** (Renseignements sur le moniteur de charge) affiche la charge de trafic pour les membres de la grappe pour le dernier intervalle ainsi que la moyenne du nombre total d'intervalles configurés (30 par défaut). Utilisez le volet **Load-Monitor Details** (Détails du moniteur de charge) pour afficher la valeur de chaque mesure à chaque intervalle.

Supervision de la liaison de commande de grappe

Consultez l'écran suivant pour superviser l'état de la grappe :

Monitoring (Supervision) > Properties (Propriétés) > System Resources Graphs (Graphiques des ressources du système) > Cluster Control Link (Liaison de commande de grappe).

Ce volet vous permet de créer des graphiques ou des tableaux indiquant l'utilisation de la capacité de réception et de transmission de la liaison de commande de grappe.

Supervision du routage de la grappe

Consultez l'écran suivant pour le routage de la grappe :

- **Monitoring (Supervision)** > **Routing (Routage)** > **LISP-EID Table (Tableau LISP-EID)**

  Affiche le tableau EID de l'ASA qui indique les EID et les ID de site.

Configuration de la journalisation pour la mise en grappe

Consultez l'écran suivante pour configurer la journalisation pour la mise en grappe :

Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Setup (Configuration du journal système)

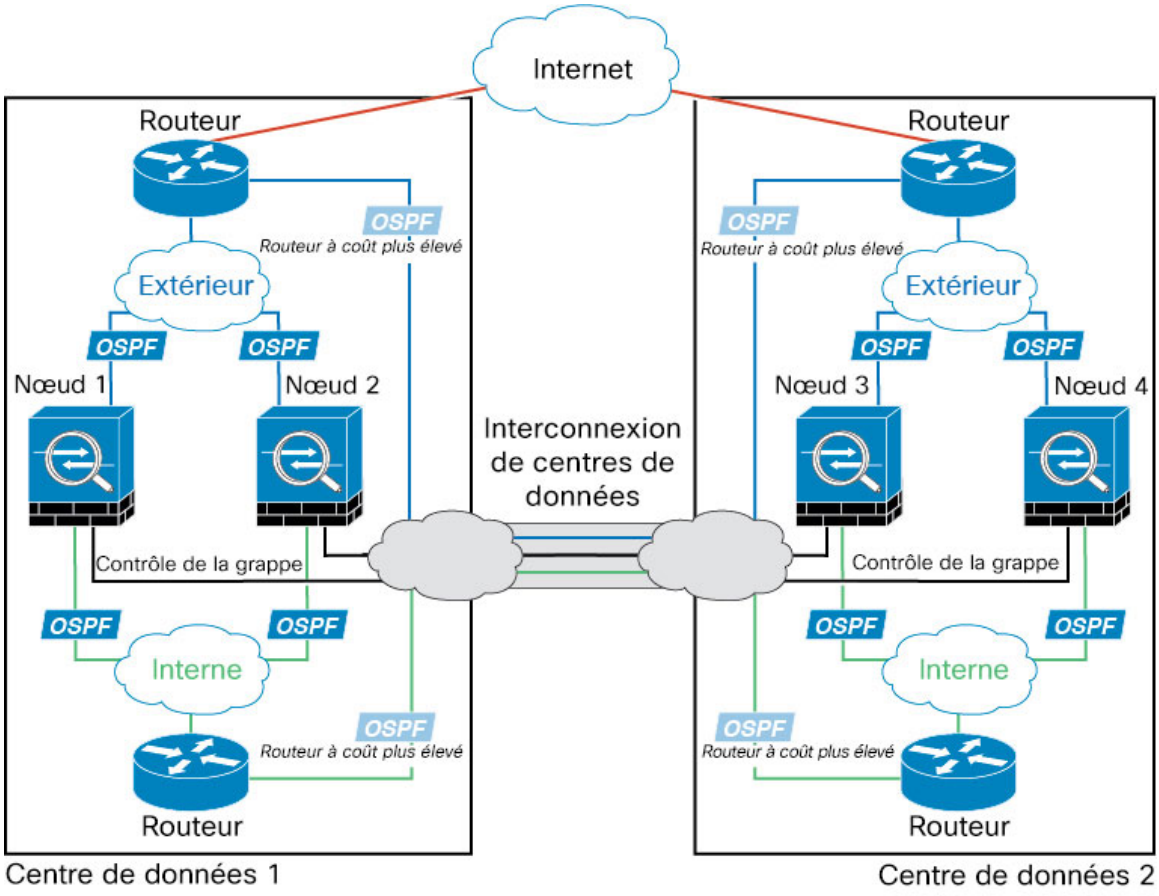
Chaque nœud de la grappe génère des messages de journal système de manière indépendante. Vous pouvez pour générer des messages de journal système avec des ID de périphérique identiques ou différents afin de faire apparaître les messages comme provenant de nœuds identiques ou différents dans la grappe.

Exemples de mise en grappe d'ASA virtuel

Ces exemples incluent toutes les configurations ASA liées aux grappes pour les déploiements typiques.

Exemple inter-sites nord-sud de mode routé d'interface individuelle

L'exemple suivant montre 2 nœuds de grappe ASA dans chacun des 2 centres de données placés entre les routeurs internes et externes (insertion nord-sud). Les nœuds de la grappe sont connectés par la liaison de commande de grappe sur l'interface DCI. Les routeurs internes et externes de chaque centre de données utilisent OSPF et PBR ou ECMP pour équilibrer la charge du trafic entre les membres de la grappe. En attribuant un routage à coût plus élevé sur l'interface DCI, le trafic reste dans chaque centre de données, sauf si tous les nœuds de la grappe ASA d'un site donné tombent en panne. En cas de défaillance de tous les nœuds de la grappe sur un site, le trafic passe de chaque routeur sur l'interface DCI aux nœuds de la grappe ASA sur l'autre site.



Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe de l'ASA

Certaines fonctionnalités d'ASA ne sont pas prises en charge avec la mise en grappe d'ASA, et d'autres le sont uniquement sur le nœud de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

- Fonctionnalités de communication unifiée qui reposent sur le mandataire TLS
- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Interfaces de tunnel virtuel (VTI)
- Les inspections d'application suivantes :
  - CTIQBE
  - H323, H225 et RAS
  - Intercommunication IPsec
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP
- Filtre de trafic de réseau de zombies
- Auto Update Server
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Équilibrage de la charge VPN
- Basculement
- Routage et pont intégrés
- Mode FIPS

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

- Ces inspections d'application sont prises en charge :
  - DCERPC et ESMTP
  - IM
  - NetBIOS et PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET et SUNRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- Autorisation et authentification pour l'accès réseau La comptabilité est décentralisée.
- Services de filtrage
- VPN de site à site
- Routage multidiffusion

Fonctionnalités appliquées aux nœuds individuels

Ces fonctionnalités sont appliquées à chaque nœud ASA, plutôt qu'à la grappe dans son ensemble ou au nœud de contrôle.

- QoS : la politique QoS est synchronisée dans la grappe dans le cadre de la duplication de la configuration. Cependant, la politique est appliquée sur chaque nœud indépendamment. Par exemple, si vous configurez le contrôle en sortie, les valeurs de débit de conformité et de rafale de conformité s'appliquent au trafic sortant d'un ASA particulier. Dans une grappe à 3 nœuds et avec le trafic réparti uniformément, le taux de conformité devient en fait trois fois supérieur au débit de la grappe.
- Détection des menaces : la détection des menaces fonctionne sur chaque nœud indépendamment; par exemple, les statistiques principales sont propres au nœud. La détection de l'analyse de port, par exemple, ne fonctionne pas, car l'analyse du trafic sera équilibrée entre tous les nœuds et un nœud ne verra pas tout le trafic.

- Gestion des ressources : la gestion des ressources en mode contexte multiple est appliquée séparément sur chaque nœud en fonction de l'utilisation locale.
- Trafic LISP : le trafic LISP sur le port UDP 4342 est inspecté par chaque nœud de réception, mais aucun directeur n'est affecté. Chaque nœud ajoute au tableau EID qui est partagé dans la grappe, mais le trafic LISP lui-même ne participe pas au partage de l'état de la grappe.

AAA pour l'accès réseau et la mise en grappe

L'AAA pour l'accès réseau comprend trois composants : l'authentification, l'autorisation et la gestion de comptes. L'authentification et l'autorisation sont mises en œuvre en tant que fonctionnalités centralisées sur le nœud de contrôle de mise en grappe avec la duplication des structures de données sur les nœuds de données de grappe. Si un nœud de contrôle est choisi, le nouveau nœud de contrôle disposera de toute l'information nécessaire pour continuer le fonctionnement ininterrompu des utilisateurs authentifiés établis et de leurs autorisations associées. Les délais d'inactivité et absolus pour l'authentification des utilisateurs sont conservés lorsqu'un changement de nœud de contrôle se produit.

La comptabilité est mise en œuvre en tant que fonctionnalité distribuée dans une grappe. La comptabilité est effectuée flux par flux, de sorte que le nœud de la grappe possédant un flux enverra les messages de démarrage et d'arrêt de comptabilité au serveur AAA lorsque la comptabilité est configurée pour un flux.

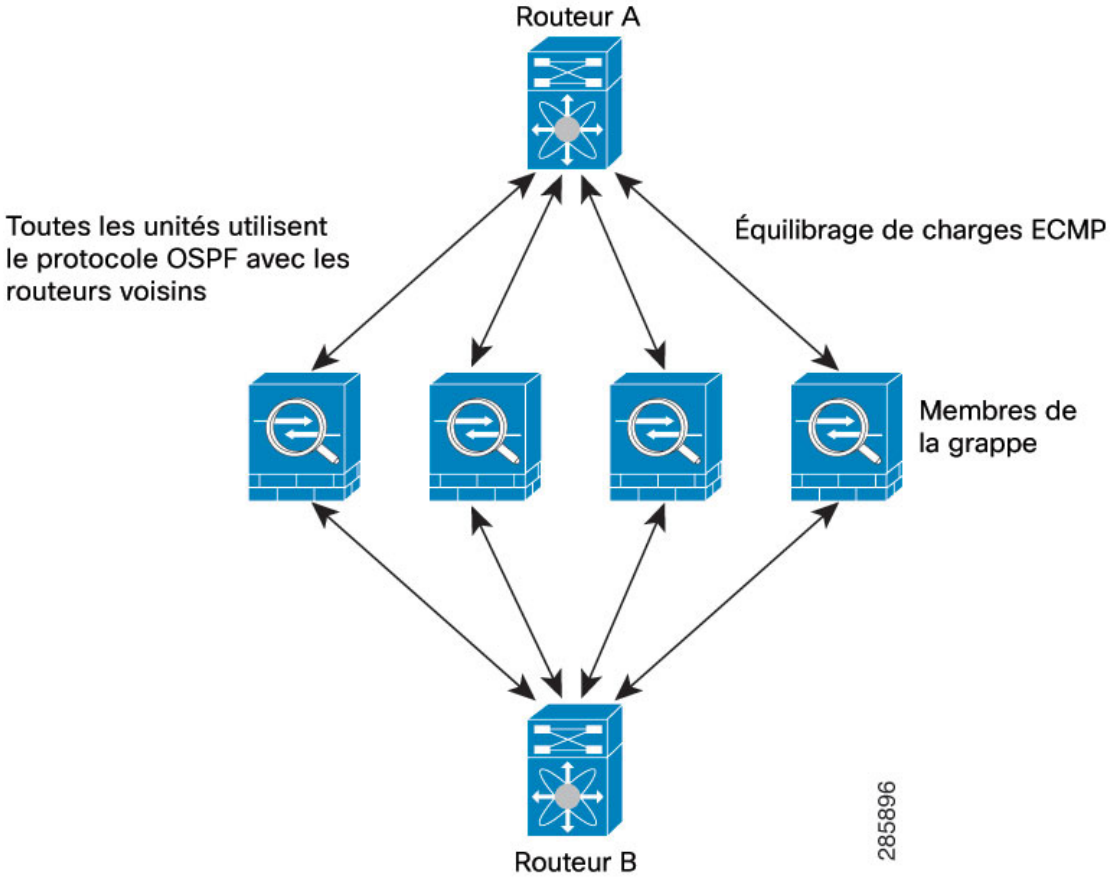
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe (voir **Configuration** > **Firewall** > **Service Policy**, page). Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 5 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Configurer une zone de trafic.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le

propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

- Si vous utilisez l'AAA pour l'accès FTP, le flux du canal de contrôle est centralisé sur le nœud de contrôle.

Inspection ICMP et mise en grappe

Le flux des paquets d'erreurs ICMP et ICMP dans la grappe varie selon que l'inspection d'erreurs ICMP ou ICMP est activée ou non. Sans inspection ICMP, ICMP est un flux unidirectionnel et il n'y a pas de prise en charge de flux directeur. Avec l'inspection ICMP, le flux ICMP devient bidirectionnel et est soutenu par un flux directeur/de sauvegarde. L'une des différences avec un flux ICMP inspecté réside dans le traitement par le directeur du paquet transféré : le directeur transmettra le paquet de réponse d'écho ICMP au propriétaire du flux au lieu de retourner le paquet au transitaire.

Routage multidiffusion et mise en grappe

En mode d'interface individuel, les unités n'agissent pas indépendamment avec la multidiffusion. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle, évitant ainsi la duplication des paquets.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents ASAdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à ASA qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale. Ce n'est pas un problème pour un EtherChannel étendu, car il n'y a qu'une seule adresse IP associée à l'interface de grappe.
- No interface PAT on an Individual interface (Pas de PAT d'interface sur une interface individuelle) Le PAT d'interface n'est pas pris en charge pour les interfaces individuelles.
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.

  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraîneront des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouvel ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, la grappe divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Réutiliser un pool PAT dans plusieurs règles : pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interfaces dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Fonctionnalité PAT par session : bien qu'elle ne soit pas exclusive à la mise en grappe, la fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multisessions doivent être transférées au nœud de contrôle et détenues par celui-ci. Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent un xlate PAT par session, tandis que ICMP et tout le reste du trafic UDP utilise la multisession. Vous pouvez configurer des règles NAT par session pour modifier ces valeurs par défaut pour TCP et UDP, mais vous ne pouvez pas configurer la PAT par session pour ICMP. Par exemple, en raison de l'utilisation croissante du protocole Quic sur le port UDP/443 comme alternative de performance à HTTPS TLS sur TCP/443, vous devriez activer la traduction d'adresses par session (PAT) pour UDP/443. Pour le trafic qui bénéficie de la PAT multisession, comme le H.323, le SIP ou l'interface simplifiée,

vous pouvez désactiver la PAT par session pour les ports TCP associés (les ports UDP de ces ports H.323 et SIP sont déjà multisession en par défaut). Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

SCTP et mise en grappe

Une association SCTP peut être créée sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses connexions multi-hébergement doivent résider sur le même nœud.

Inspection SIP et mise en grappe

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

La configuration du mandataire TLS n'est pas prise en charge.

SNMP et mise en grappe

Un agent SNMP interroge chaque ASA en fonction de l'adresse IP locale de son . Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud.Vous devez les rajouter sur le nœud de contrôle pour forcer les utilisateurs à se reproduire vers le nouveau nœud, ou directement sur le nœud de données.

STUN et mise en grappe

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en

panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Syslog, NetFlow et la mise en grappe

- Syslog : chaque nœud de la grappe génère ses propres messages de journal système. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.
- NetFlow : chaque nœud de la grappe génère son propre flux NetFlow. Le collecteur NetFlow peut traiter chaque appareil ASA uniquement comme un exportateur NetFlow distinct.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Calcul du débit

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les composants clés concernés dans le processus d'élection du nœud de contrôle sont les suivants :

- Nœuds de grappe : communiquent par la liaison de commande de grappe et participent au processus d'élection
- Demandes d'élection : diffusées toutes les 3 secondes par les nœuds lorsque la mise en grappe est activée
- Valeurs de priorité : définies entre 1 et 100, où 1 correspond à la priorité la plus élevée
- Nœud de contrôle : le nœud choisi qui coordonne les opérations de la grappe

Ces étapes décrivent comment les nœuds de la grappe élisent un nœud de contrôle :

1. Lorsque la mise en grappe est activée pour un nœud (ou lorsque celui-ci démarre pour la première fois alors que la mise en grappe est déjà activée), le nœud diffuse une demande d'élection toutes les 3 secondes.
2. Tout autre nœud ayant une priorité plus élevée répond à la demande d'élection. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud rejoint ultérieurement la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle. Le nœud de contrôle existant conserve toujours son rôle, sauf s'il cesse de répondre, auquel cas un nouveau nœud de contrôle est élu.
5. Dans un scénario de « split brain », où plusieurs nœuds de contrôle sont temporairement présents, le nœud ayant la priorité la plus élevée conserve son rôle tandis que les autres nœuds reprennent leur rôle de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe ASA virtuel

La mise en grappe ASA virtuel assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Supervision de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds

de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Scénario de déconnexion cérébrale

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, toutes les interfaces physiques sont supervisées par défaut; vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant la suppression par l'ASA d'un membre de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'ASA ne supervise pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de l'ASA de la grappe. Le nœud est supprimé après 500 ms, quel que soit son état.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

ASA tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque ASA devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion uniquement peut envoyer et recevoir du trafic. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de l'ensemble d'adresses IP de la grappe. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser le port de console pour toute autre configuration.

Rejoindre la grappe

Après le retrait d'un nœud de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : l'ASA essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment. Ce comportement est configurable.
- Échec de l'interface de données : l'ASA tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'ASA désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe. Ce comportement est configurable.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que la liaison de commande de grappe soit active et que la mise en grappe soit toujours activée. L'ASA tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc. Un nœud tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Ce comportement est configurable.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 1 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
Tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	Comprend les règles AAA (uauth).
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—
VPN distribué (site à site) pour Firepower 4100/9300	Oui	La session de sauvegarde devient la session active, puis une nouvelle session de sauvegarde est créée.

Gestion des connexions par la grappe ASA virtuel

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire de la sauvegarde : nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis.

  Si vous activez la localisation du directeur pour la mise en grappe inter-sites, il existe deux rôles de propriétaire de la sauvegarde : le rôle de sauvegarde locale et de sauvegarde globale. Le propriétaire choisit toujours une sauvegarde locale sur le même site que lui (en fonction de l'ID du site). La sauvegarde globale peut se trouver sur n'importe quel site et peut même se trouver sur le même nœud que la sauvegarde locale. Le propriétaire envoie des informations sur l'état de la connexion aux deux sauvegardes.

  Si vous activez la redondance de sites et que le propriétaire de secours se trouve sur le même site que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre site pour protéger les flux d'une défaillance du site. La sauvegarde de châssis et la sauvegarde de site sont indépendantes. Par conséquent, dans certains cas, un flux comportera à la fois une sauvegarde de châssis et une sauvegarde de site.
- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Si vous activez la localisation de directeur pour la mise en grappe inter-sites, il y a deux rôles de directeur : le directeur local et le directeur global. Pour un paquet de nouveau flux, le membre de réception sélectionne le directeur local parmi les membres du site du membre de réception. Le directeur global peut se trouver sur n'importe quel site et peut même être le même membre que le directeur local. En cas de défaillance du propriétaire d'origine et lorsque la localisation s'applique, le directeur local choisit un nouveau propriétaire de connexion sur le site du directeur local.

Détails du hachage ICMP/ICMPv6 :

- Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
- Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
- Pour les autres paquets, les ports source et de destination sont à 0.

- Transitaire : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Si vous activez la localisation de directeur, le redirecteur interroge le directeur local lorsque la localisation s'applique. Le transitaire interroge le directeur global si le directeur local ne connaît pas le propriétaire, si la connexion appartient à un autre site ou si la localisation est contournée. Une requête de directeur intersite est le comportement attendu dans ces cas. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.



Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Connexions par traduction d'adresse de port

Lorsqu'une connexion utilise la traduction d'adresses de port (PAT), le type de PAT (par session ou multisession) influence quel membre de la grappe devient propriétaire de la nouvelle connexion :

- PAT par session : le propriétaire est le nœud qui reçoit le paquet initial dans la connexion.

  Par défaut, le trafic TCP et DNS UDP utilise une PAT par session.

- PAT multisession : le propriétaire est toujours le nœud de contrôle. Si une connexion PAT multisession est initialement reçue par un nœud de données, le nœud de données transfère la connexion au nœud de contrôle.

  Par défaut, le trafic UDP (à l'exception du trafic UDP DNS) et ICMP utilise la PAT multisession. Ces connexions appartiennent donc toujours au nœud de contrôle.

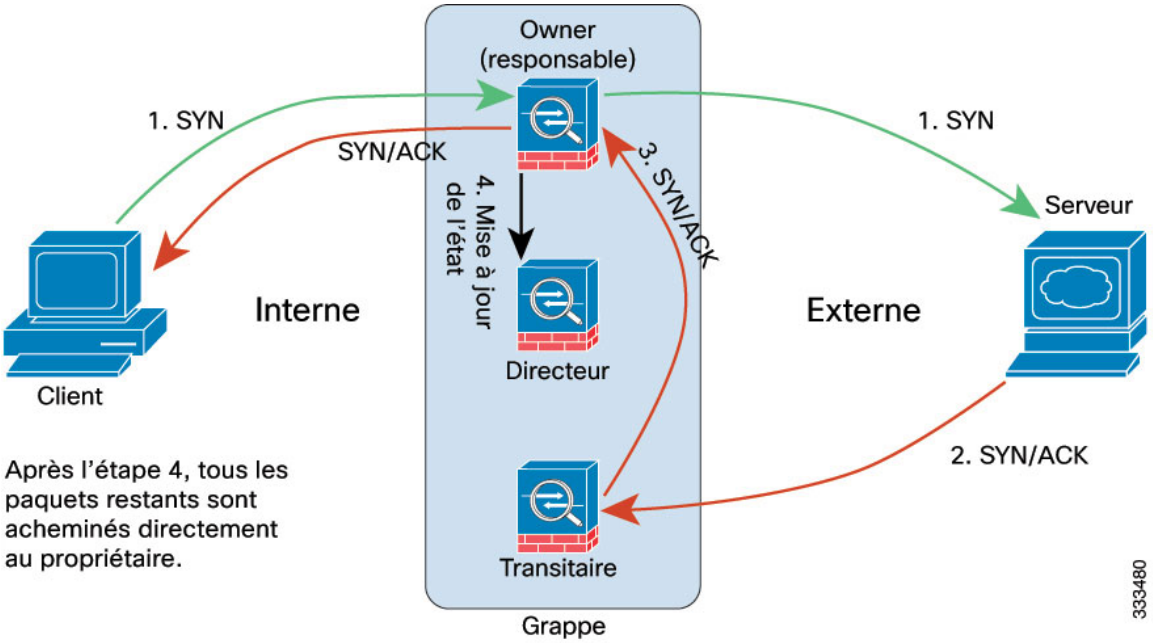
Vous pouvez modifier les valeurs par défaut de PAT par session pour les protocoles TCP et UDP afin que les connexions à ces protocoles soient gérées par session ou multisession selon la configuration. Pour ICMP, vous ne pouvez pas modifier la PAT multisession par défaut. Référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements sur les serveurs mandataires TLS.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Pour de meilleures performances, un bon équilibrage de la charge externe est nécessaire pour que les deux directions d'un flux arrivent au même nœud et pour que les flux soient répartis uniformément entre les nœuds. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

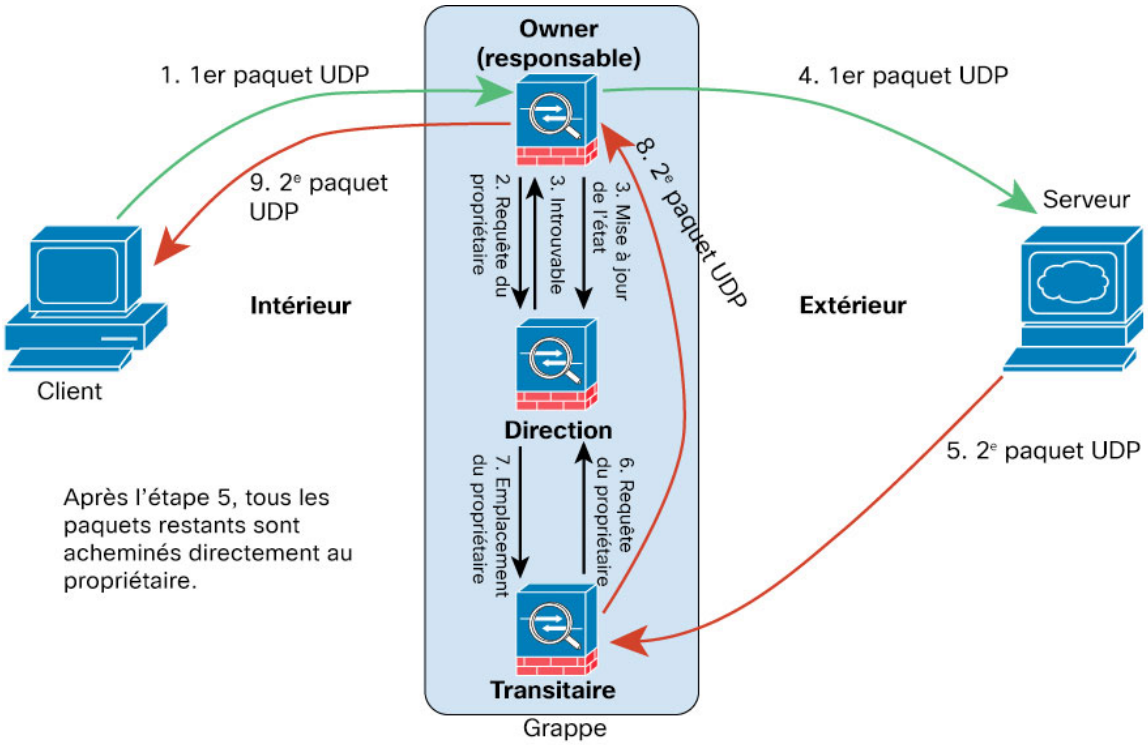


1. Le paquet SYN provient du client et est livré à un ASA (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un ASA différent (selon la méthode d'équilibrage de la charge). Cet ASA est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 6 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un ASA (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Rééquilibrage des nouvelles connexions TCP dans la grappe

Si les capacités d'équilibrage de charges des routeurs en amont ou en aval entraînent une répartition non équilibrée des flux, vous pouvez configurer un rééquilibrage des nouvelles connexions afin que les nœuds ayant le plus de nouvelles connexions par seconde redirigent les nouveaux flux TCP vers d'autres nœuds. Aucun flux existant ne sera déplacé vers d'autres nœuds.

Comme cette commande rééquilibre uniquement en fonction des connexions par seconde, le nombre total de connexions établies sur chaque nœud n'est pas pris en compte, et le nombre total de connexions peut ne pas être égal.

Une fois qu'une connexion est déchargée sur un autre nœud, elle devient une connexion asymétrique.

Ne configurez pas le rééquilibrage de connexion pour les topologies inter-sites; il ne faut pas que les nouvelles connexions soient rééquilibrées entre les membres de la grappe sur un site différent.

Historique de la mise en grappe d'ASA virtuel

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Suppression des propos tendancieux	9.19(1)	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Mise en grappe d'ASAv30, ASAv50 et ASAv100 pour VMware et KVM	9.17(1)	La mise en grappe d'ASA virtuel vous permet de regrouper jusqu'à 16 ASA virtuel en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. La mise en grappe d'ASA virtuel prend en charge le mode d'interface individuelle en mode de pare-feu routé; les EtherChannels étendus ne sont pas pris en charge. L'ASA virtuel utilise une interface virtuelle VNI (VXLAN) pour la liaison de commande de grappe. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** • **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)**

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.