Mise en grappe pour les appareils Firepower 4100/9300

La mise en grappe vous permet de regrouper plusieurs nœuds défense contre les menaces 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.

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 57.

À propos de la mise en grappe sur les châssis Firepower 4100/9300

Lorsque vous déployez une grappe sur le Châssis Firepower 4100/9300 , elle effectue les opérations suivantes :

- Pour une mise en grappe d'instances native : crée une *liaison de commande de grappe* (par défaut, le canal de port 48) pour la communication de nœud à nœud.

  Pour la mise en grappe de plusieurs instances: vous devez préconfigurer les sous-interfaces sur un ou plusieurs EtherChannels de type grappe; chaque instance a besoin de sa propre liaison de commande de grappe.

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, ce lien utilise le fond de panier Firepower 9300 pour les communications de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel pour les communications entre les châssis.

- Crée la configuration de démarrage de grappe dans l'application.

  Lorsque vous déployez la grappe, le superviseur de châssis envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe.

- Affecte des interfaces de données à la grappe en tant *qu'interfaces étendue*s.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, les interfaces étendues ne se limitent pas aux EtherChannels, comme c'est le cas pour la mise en grappe avec plusieurs châssis. Le superviseur Firepower 9300 utilise la technologie EtherChannel en interne pour équilibrer la charge du trafic vers plusieurs modules sur une interface partagée, de sorte que tout type d'interface de données fonctionne pour le mode étendu. Pour la mise en grappe avec plusieurs châssis, vous devez utiliser des EtherChannels étendus pour toutes les interfaces de données.

Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

- Attribue une interface de gestion à toutes les unités de la grappe.

Voir l'une des sections suivantes pour plus d'informations sur la mise en grappe.

Configuration du démarrage

Lorsque vous déployez la grappe, le superviseur de châssis Firepower 4100/9300 envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic.

L'unité de **contrôle** est l'un des membres de la grappe. L'unité de contrôle est déterminée automatiquement. Tous les autres membres sont des unités **de données**.

Vous devez effectuer toute la configuration sur l'unité de contrôle uniquement; la configuration est ensuite reproduite dans les unités de données.

Certaines fonctionnalités ne sont pas évolutives dans une grappe, et l'unité de contrôle gère tout le trafic pour ces fonctionnalités. .

Liaison de commande de grappe

Pour la mise en grappe d'instances natives : la liaison de commande de grappe est automatiquement créé à l'aide de l'interface du canal de port 48.

Pour la mise en grappe de plusieurs instances: vous devez préconfigurer les sous-interfaces sur un ou plusieurs EtherChannels de type grappe; chaque instance a besoin de sa propre liaison de commande de grappe.

Pour une grappe isolée de modules de sécurité dans un châssis Firepower 9300, cette interface n'a pas d'interface membre. Cet EtherChannel de type de grappe utilise le fond de panier Firepower 9300 pour les communications de la grappe. Pour la mise en grappe avec plusieurs châssis, vous devez ajouter une ou plusieurs interfaces à l'EtherChannel.

Dans le cas d'une grappe à deux châssis, ne connectez pas directement la liaison de commande de grappe d'un châssis à l'autre. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

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

Dimensionner la liaison de commande de grappe

Si possible, vous devez dimensionner la liaison de commande de grappe en fonction du débit attendu de chaque châssis afin que la liaison de commande de grappe puisse gérer les scénarios les plus défavorables.

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées. Par exemple :

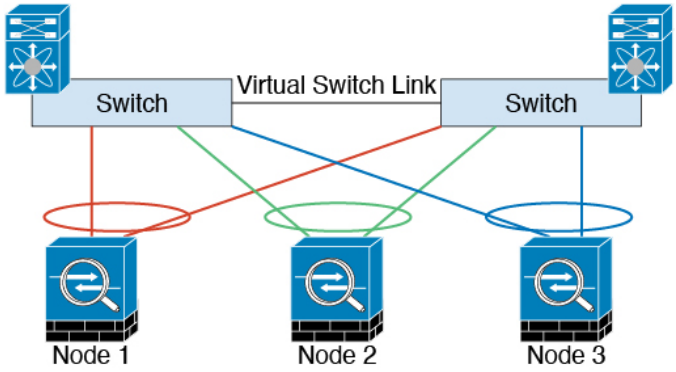
- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe pour la mise en grappe inter-châssis

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Réseau de liaison de commande de grappe

Le Châssis Firepower 4100/9300 génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID de châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot-id*. Pour les grappes à instances multiples, qui utilisent généralement des sous-interfaces VLAN différentes du même EtherChannel, la même adresse IP peut être utilisée pour différentes grappes en raison de la séparation des VLAN. Le réseau de liaison de commande de grappe ne peut pas comprendre de routeurs entre les unités; seule la commutation de couche 2 est autorisée.

le réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Management Interface (interface de gestion)

Vous devez affecter une interface de type gestion à la grappe. Cette interface est une interface individuelle spéciale, par opposition à une interface étendue. L'interface de gestion vous permet de vous connecter directement à chaque unité. L'interface logique de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le Cisco Secure Firewall Management Center. Elle utilise sa propre authentification locale, son adresse IP et son routage statique. Chaque membre de la grappe utilise une adresse IP distincte sur le réseau de gestion que vous avez définie lors de la configuration de démarrage.

L'interface de gestion est partagée entre l'interface logique de gestion et l'interface logique de *dépistage*. L'interface logique de dépistage est facultative et n'est pas configurée dans le cadre de la configuration de démarrage. L'interface de dépistage peut être configurée avec le reste des interfaces de données. Si vous choisissez de configurer l'interface de dépistage, configurez une adresse IP de grappe principale en tant

qu'adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de dépistage cohérent à une adresse; Lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que l'accès à la grappe se poursuit de façon transparente. Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Interfaces de la grappe

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, vous pouvez affecter des interfaces physiques ou des EtherChannels (également appelés canaux de port) à la grappe. Les interfaces affectées à la grappe sont des interfaces étendues qui équilibrent la charge du trafic entre tous les membres de la grappe.

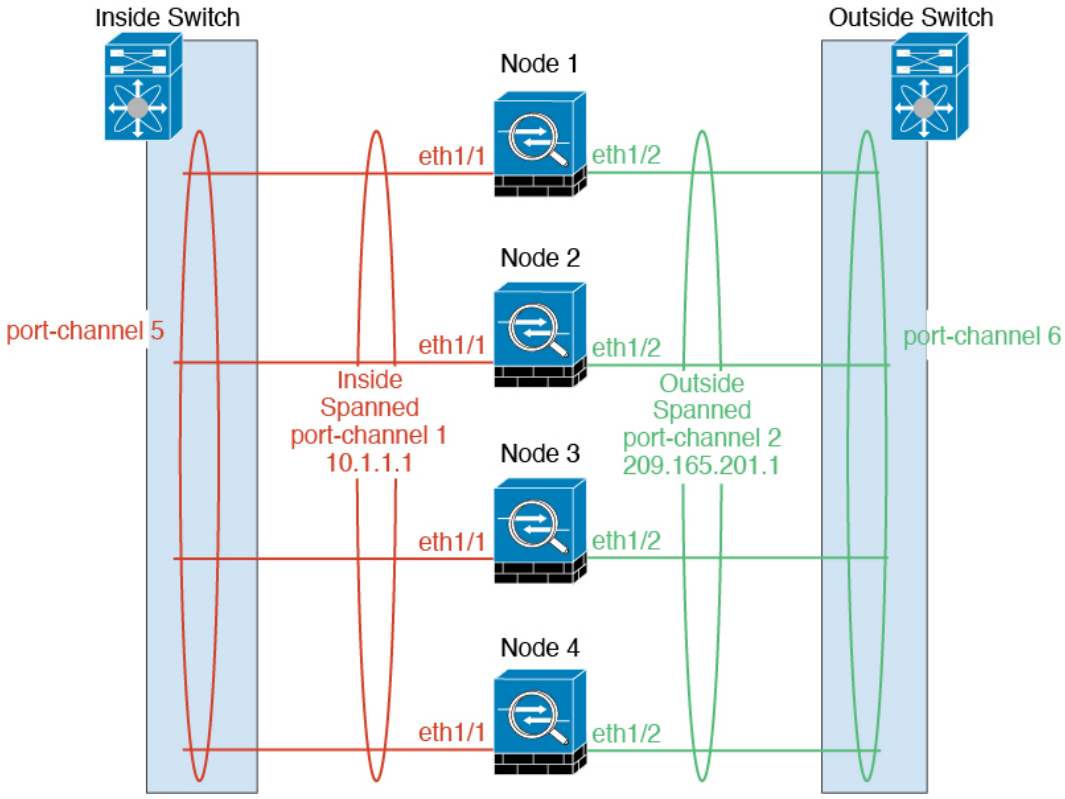
Pour la mise en grappe avec plusieurs châssis, vous pouvez uniquement affecter des EtherChannels de données à la grappe. Ces EtherChannels étendus comprennent les mêmes interfaces membre sur chaque châssis; Sur le commutateur en amont, toutes ces interfaces sont incluses dans un seul EtherChannel, de sorte que le commutateur ne sache pas qu'il est connecté à plusieurs périphériques.

Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

EtherChannels étendus

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. Un EtherChannel étendu peut être configuré dans les modes de pare-feu routé et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts. L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.

Pour les grappes à instances multiples, chaque grappe nécessite des EtherChannels de données dédiés; vous ne pouvez pas utiliser des interfaces partagées ou des sous-interfaces VLAN.



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.

Licences pour la mise en grappe

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez un nœud de grappe à centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Vous pouvez modifier les licences de la grappe dans la zone **Devices** > **Device Management** > **Cluster** > **License** (Périphériques > Gestion des périphériques > Grappe > Licence).

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Exigences et conditions préalables à la mise en grappe

Prise en charge des modèles de grappe

Défense contre les menaces prend en charge la mise en grappe sur les modèles suivants :

- Firepower 9300 – Vous pouvez inclure jusqu'à 16 nœuds dans la grappe. Par exemple, vous pouvez utilisermodule dans 16 châssis, ou modules dans 8 châssis, ou toute combinaison offrant un maximum de 16 modules. Prend en charge la mise en grappe avec plusieurs châssis et la mise en grappe isolée pour les modules de sécurité dans un châssis.
- Firepower 4100 : pris en charge pour un maximum de 16à nœuds grâce à la mise en grappe avec plusieurs châssis.

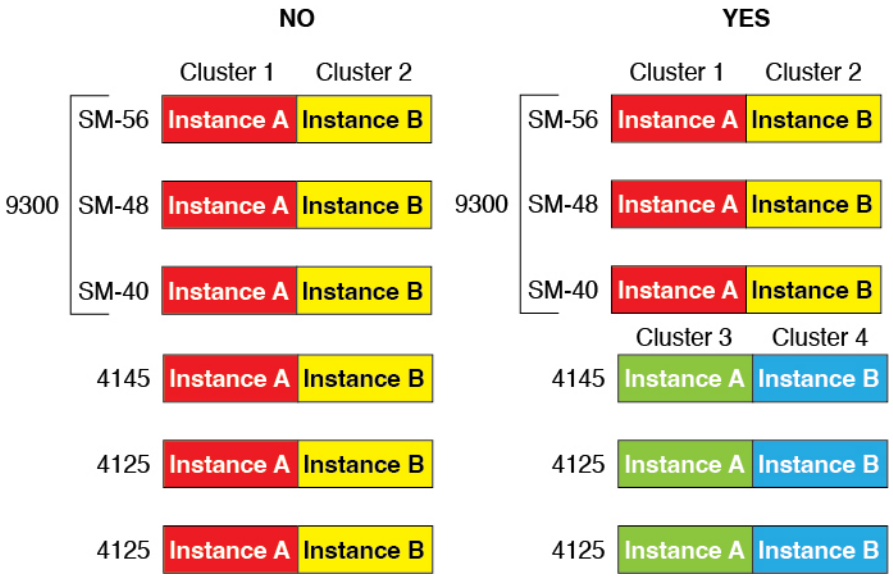
Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Exigences matérielles et logicielles en matière de mise en grappe

Tous les châssis d'une grappe :

- Mise en grappe native des instances : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides.
- Mise en grappe d'instances de conteneur : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.

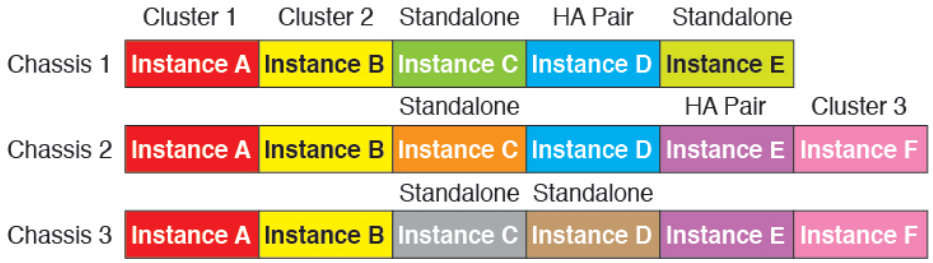


- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.
- Doit utiliser le même serveur NTP. Pour Défense contre les menaces, centre de gestion doit également utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.

Exigences de la mise en grappe en plusieurs instances

- Pas de mise en grappe intra-module/moteur de sécurité : pour une grappe donnée, vous ne pouvez utiliser qu'une seule instance de conteneur par module de sécurité/moteur. Vous ne pouvez pas ajouter deux instances de conteneur à la même grappe si elles fonctionnent sur le même module.

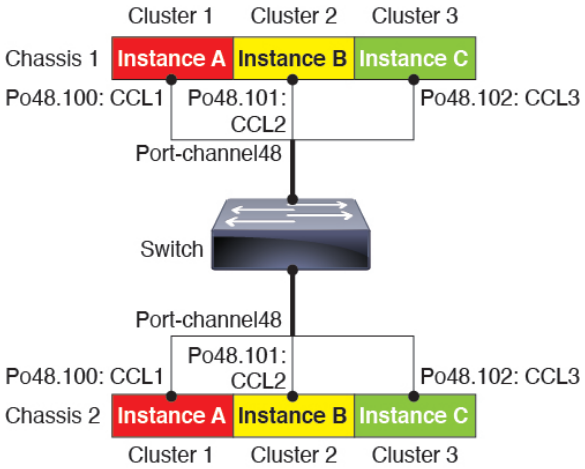
- Combinez les grappes et les instances autonomes : toutes les instances de conteneur sur un module ou un moteur de sécurité n'ont pas besoin d'appartenir à une grappe. Vous pouvez utiliser certaines instances en tant que nœuds autonomes ou à haute disponibilité. Vous pouvez également créer plusieurs grappes en utilisant des instances distinctes sur le même module/moteur de sécurité.



- Les 3 modules d'un appareil Firepower 9300 doivent appartenir à la grappe : Pour le périphérique Firepower 9300, une grappe nécessite une seule instance de conteneur sur les 3 modules. Vous ne pouvez pas créer une grappe à l'aide d'instances du module 1 et 2, puis utiliser une instance native sur le module 3, ou example.

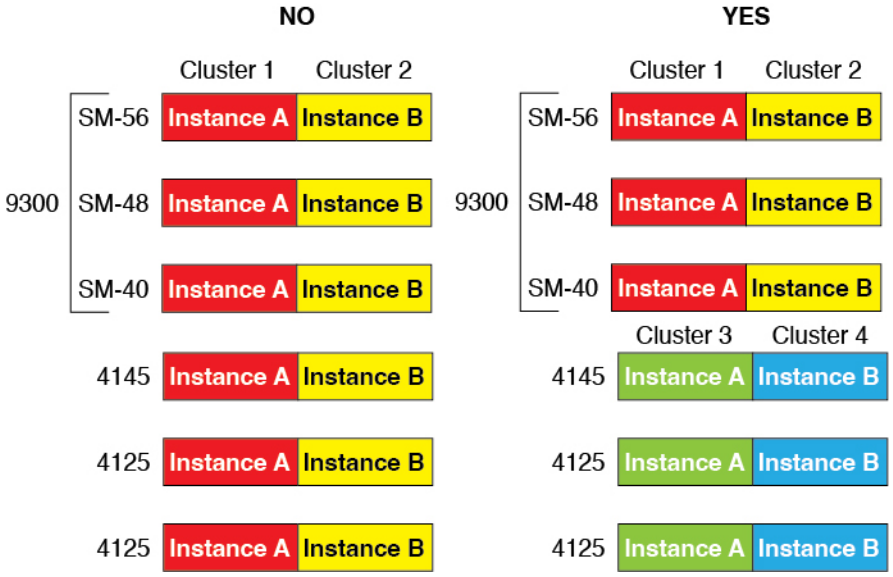
- Faire correspondre les profils de ressources : Nous recommandons que chaque nœud de la grappe utilise les mêmes attributs de profils de ressources; cependant, des ressources non concordantes sont autorisées lors du remplacement des nœuds de la grappe par un profil de ressource différent ou lors de l'utilisation de différents modèles.

- Liaison de commande de grappe dédiée : pour les grappes à plusieurs châssis, chaque grappe a besoin d'une liaison de commande de grappe dédiée. Par exemple, chaque grappe peut utiliser une sous-interface distincte sur le même EtherChannel de type de grappe, ou utiliser des EtherChannel distincts.



- No Shared Interface (Aucune interface partagée) : les interfaces de type partagé ne sont pas prises en charge avec la mise en grappe. Cependant, les mêmes interfaces de gestion et d'événements peuvent être utilisées par plusieurs grappes.

- No subinterfaces (Pas de sous-interfaces) : une grappe de plusieurs instances ne peut pas utiliser les sous-interfaces VLAN définies par FXOS. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel.
- Combiner les modèles de châssis : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



- Maximum de 6 nœuds : vous pouvez utiliser jusqu'à six instances de conteneur dans une grappe.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez la Compatibilité Cisco FXOS.

Lignes directrices et limites de la mise en grappe

Commutateurs pour la mise en grappe

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe.

- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes d'équilibrage de charge EtherChannel suivants : **source-dest-ip** ou **source-dest-ip-port** (reportez-vous à la commande Cisco Nexus OS et Cisco IOS-XE **port-channel load-balance**). N'utilisez pas de mot-clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe.
- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

  router(config)# **port-channel** *id* **hash-distribution fixed**

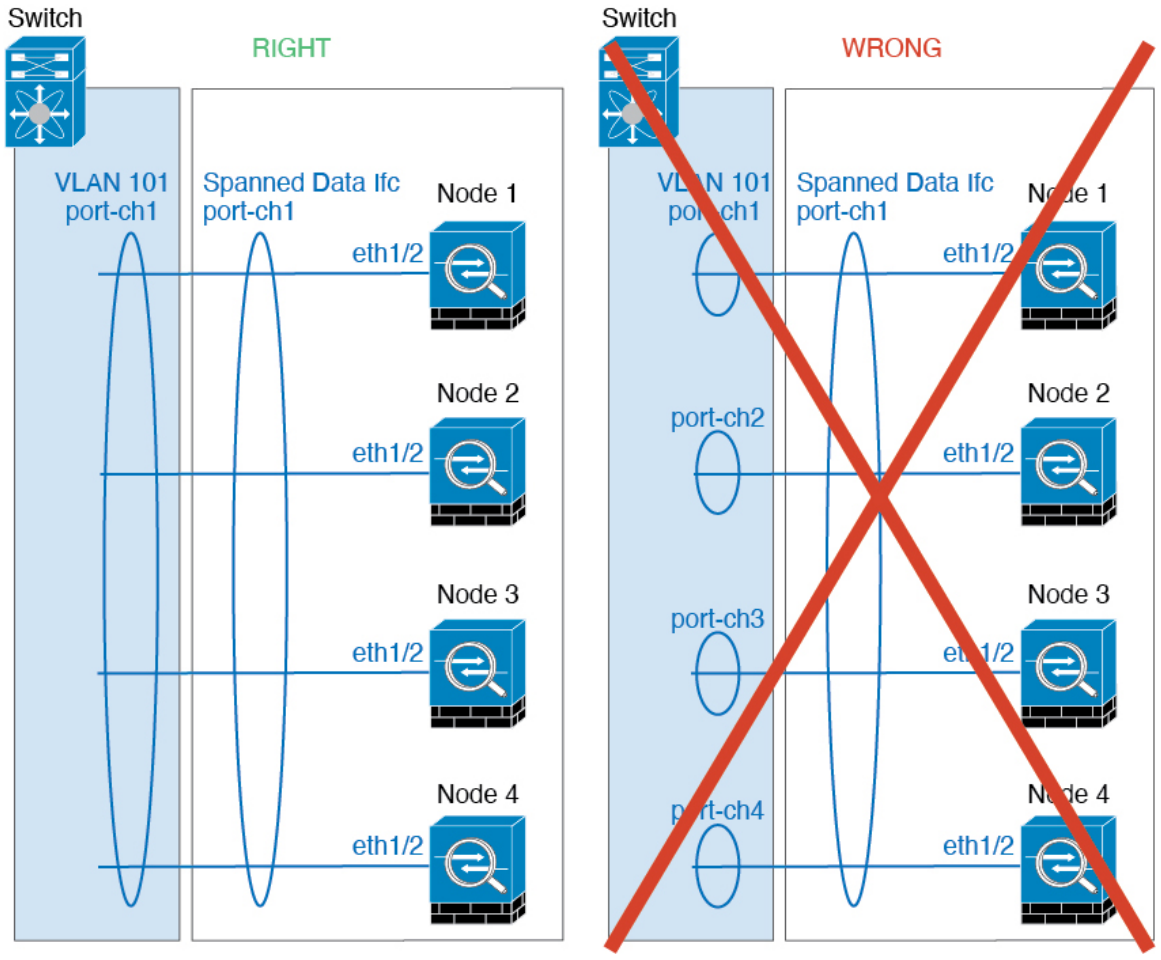
  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

- , les grappes Firepower 4100/9300 prennent en charge la convergence progressive LACP. Ainsi, vous pouvez laisser la convergence progressive LACP activée sur les commutateurs Cisco Nexus connectés.
- Lorsque vous voyez le regroupement lent d'un EtherChannel étendu sur le commutateur, vous pouvez activer un débit LACP rapide pour une interface individuelle sur le commutateur. Le débit du protocole LACP de FXOS EtherChannels est rapide par défaut. Notez que certains commutateurs, comme la série Nexus, ne prennent pas en charge le débit LACP rapide lors des mises à niveau logicielles en service (ISSU). Nous ne recommandons donc pas l'utilisation des ISSU avec la mise en grappe.

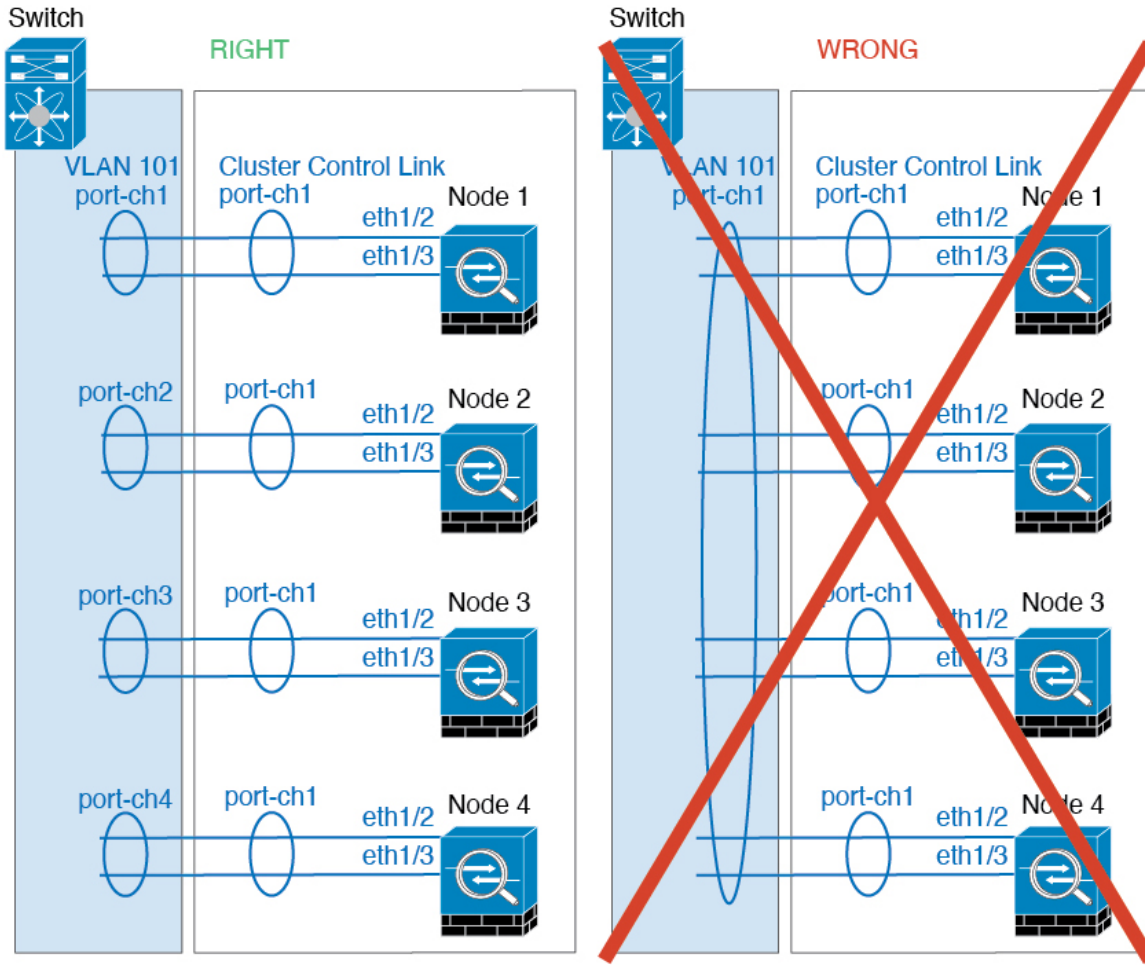
EtherChannels pour la mise en grappe

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.

- Configuration EtherChannel Spanned vs. Device-Local : veillez à configurer le commutateur de manière appropriée pour les Spanned EtherChannels par rapport aux Device-local EtherChannels.
  - Spanned EtherChannels : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



  - Device- local EtherChannels (EtherChannel locaux au périphérique) : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), 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.
- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent suspendre les connexions; 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.
- Si vous utilisez un serveur Windows 2003 connecté à une interface EtherChannel étendue, lorsque le port du serveur syslog est en panne et que le serveur ne limite pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.

- Nous vous recommandons de connecter les EtherChannels à un VSS, à un vPC, à StackWise ou à StackWise Virtual pour la redondance.
- Dans un châssis, vous ne pouvez pas mettre en grappe certains modules de sécurité et exécuter d'autres modules de sécurité en mode autonome; vous devez inclure tous les modules de sécurité dans la grappe.
- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.

Valeurs par défaut

- 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 pour une liaison de commande de grappe défaillante est définie pour permettre un nombre illimité de tentatives toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante est définie à 3 tentatives toutes les 5 minutes, avec un intervalle croissant défini à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe

Vous pouvez facilement déployer la grappe à partir du superviseur Firepower 4100/9300. Toute la configuration initiale est générée automatiquement pour chaque unité. Vous pouvez ensuite ajouter les unités au centre de gestion et les regrouper dans une grappe.

FXOS : Ajouter une grappe Défense contre les menaces

En mode natif : vous pouvez ajouter une grappe à un châssis Firepower 9300 unique qui est isolé des modules de sécurité dans le châssis, ou vous pouvez utiliser plusieurs châssis.

En mode multi-instance : vous pouvez ajouter une ou plusieurs grappes à un seul châssis Firepower 9300 qui sont isolées des modules de sécurité du châssis (vous devez inclure une instance sur chaque module) ou ajouter une ou plusieurs grappes sur plusieurs châssis.

Pour les grappes sur plusieurs châssis, vous devez configurer chaque châssis séparément. Ajoutez la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis sur le châssis suivant pour faciliter le déploiement,

Créer une grappe Défense contre les menaces

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité.

Pour la mise en grappe sur plusieurs châssis, vous devez configurer chaque châssis séparément. Déployer la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis au châssis suivant pour faciliter le déploiement.

Dans un châssis Firepower 9300, vous devez activer la mise en grappe pour les 3 logements de module ou pour les instances de conteneur, une instance de conteneur dans chaque logement, même si aucun module n'est installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.

Avant de commencer

- Téléchargez l'image de l'application que vous voulez utiliser pour l'appareil logique à partir de Cisco.com, puis téléchargez cette image sur le serveur de l'application. Châssis Firepower 4100/9300 .
- Pour les instances de conteneur, si vous ne souhaitez pas utiliser le profil par défaut, ajoutez un profil de ressource en fonction de Permet d'ajouter un profil de ressource pour les instances de conteneur.
- Pour les instances de conteneur, avant de pouvoir installer une instance de conteneur pour la première fois, vous devez réinitialiser le security module/engine pour que le formatage du disque soit correct. Choisissez **Security Modules** (modules de sécurité) ou **Security Engine** (moteur de sécurité), puis cliquez sur Icône réinitialiser (). Un périphérique logique existant sera supprimé, puis réinstallé en tant que nouveau périphérique, perdant toute configuration d'application locale. Si vous remplacez une instance native par des instances de conteneur, vous devrez supprimer l'instance native dans tous les cas. Vous ne pouvez pas migrer automatiquement une instance native vers une instance de conteneur.
- Recueillez les informations suivantes :
  - ID de l'interface de gestion, adresses IP et masque de réseau
  - l'adresse IP de la passerelle
  - centre de gestion l'adresse IP et/ou l'ID NAT de votre choix
  - l'adresses IP du serveur DNS
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Configurer les interfaces.

a) Ajoutez au moins une interface de type de données ou un EtherChannel (également appelé canal de port) avant de déployer la grappe. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port) ou Configurer une interface physique.

Pour la mise en grappe sur plusieurs châssis, toutes les interfaces de données doivent être des EtherChannels étendus avec au moins une interface membre. Ajoutez les mêmes EtherChannels sur chaque châssis. Combinez les interfaces membres de toutes les unités de la grappe en un seul EtherChannel sur le commutateur. Consultez Lignes directrices et limites de la mise en grappe, à la page 10 pour obtenir des renseignements sur les EtherChannels.

Pour la mise en grappe à instances multiples, vous ne pouvez pas utiliser des sous-interfaces VLAN ou des interfaces de partage de données définies par FXOS dans la grappe. Seules les sous-interfaces définies par l'application sont prises en charge. Consultez Interfaces FXOS par rapport aux interfaces d'application pour obtenir de plus amples renseignements.

b) Ajoutez une interface de type de gestion ou un EtherChannel. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port) ou Configurer une interface physique.

L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que l'interface de gestion du châssis qui est utilisée uniquement pour la gestion de ce dernier (dans FXOS, vous pouvez voir l'interface de gestion du châssis affichée comme MGMT, management0, ou d'autres noms similaires).

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface de gestion sur chaque châssis.

Pour la mise en grappe à instances multiples, vous pouvez partager la même interface de gestion sur plusieurs grappes sur le même châssis ou avec des instances autonomes.

c) Pour la mise en grappe sur plusieurs châssis, ajoutez une interface membre à l'EtherChannel de la liaison de commande de grappe (par défaut, le canal de port 48). Consultez Ajouter un canal EtherChannel (canal de port).

N'ajoutez pas d'interface membre pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300. Si vous ajoutez un membre, le châssis suppose que cette grappe utilisera plusieurs châssis et vous permettra uniquement d'utiliser des EtherChannels étendus, par exemple.

Sous l'onglet **Interfaces**, l'interface de type de grappe du canal de port 48 affiche l' **état de l'opération** comme **ayant échoué** si elle n'inclut aucune interface membre. Pour une grappe isolée de modules de sécurité dans un châssis Firepower 9300, cet EtherChannel ne nécessite aucune interface membre et vous pouvez ignorer cet état opérationnel.

Ajoutez les mêmes interfaces membre sur chaque châssis. La liaison de commande de grappe est un EtherChannel local au périphérique sur chaque châssis. Utilisez des EtherChannels distincts sur le commutateur pour chaque périphérique. Consultez Lignes directrices et limites de la mise en grappe, à la page 10 pour obtenir des renseignements sur les EtherChannels.

Pour la mise en grappe de plusieurs instances, vous pouvez créer des EtherChannels de type grappe supplémentaires. Contrairement à l'interface de gestion, la liaison de commande de grappe ne peut *pas* être partagée entre plusieurs périphériques. Vous aurez donc besoin d'une interface de grappe pour chaque grappe. Cependant, nous vous recommandons d'utiliser des sous-interfaces VLAN au lieu de plusieurs EtherChannels; Consultez l'étape suivante pour ajouter une sous-interface VLAN à l'interface de la grappe.

d) Pour la mise en grappe de plusieurs instances, ajoutez des sous-interfaces VLAN à l'EtherChannel de la grappe afin d'avoir une sous-interface pour chaque grappe. Consultez Ajouter une sous-interface VLAN pour les instances de conteneur.

Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native.

e) (Facultatif) Ajouter une interface d'événement. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port) ou Configurer une interface physique.

Cette interface est une interface de gestion secondaire pour les périphériques défense contre les menaces . Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande défense contre les menaces . Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez les commandes **configure network** dans la référence de commande défense contre les menaces .

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface d'événement sur chaque châssis.

Étape 2 Choisissez **Logical Devices** (périphériques logiques).

Étape 3 Cliquez sur **Add** > **Cluster**, (Ajouter > Grappe > Ajouter un périphérique) et définissez les paramètres suivants :

Illustration 1 : Grappe native

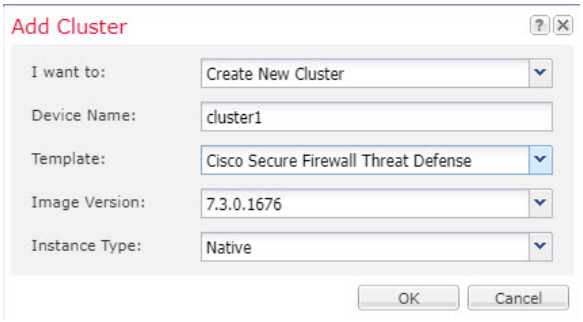
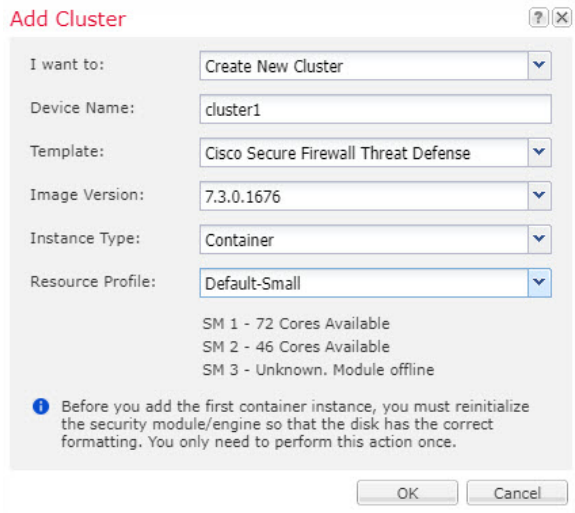


Illustration 2 : Grappe multi-instances



a) Choisir **Je veux :** > **Créer une nouvelle grappe**
b) Indiquez un nom de périphérique (**Device Name**).

   Ce nom est utilisé en interne par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

c) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
d) Choisissez la version de l'image (**Image Version**).
e) Pour le **type d'instance**, , choisissez **Natif** ou **Conteneur**.

   Instance native : une instance native utilise toutes les ressources (CPU, RAM et espace disque) du module/moteur de sécurité, de sorte que vous ne pouvez installer qu'une seule instance native. Instance de conteneur : une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité, de sorte que vous pouvez installer plusieurs instances de conteneur.

f) (Instance de conteneur uniquement) Pour le **type de ressource**, choisissez un des profils de ressource dans la liste déroulante.

   Pour le périphérique Firepower 9300, ce profil sera appliqué à chaque instance de chaque module de sécurité. Vous pouvez définir différents profils par module de sécurité plus loin dans cette procédure; par exemple, si vous utilisez différents types de modules de sécurité et que vous souhaitez utiliser plus de CPU sur un modèle bas de gamme. Nous vous recommandons de choisir le profil approprié avant de créer

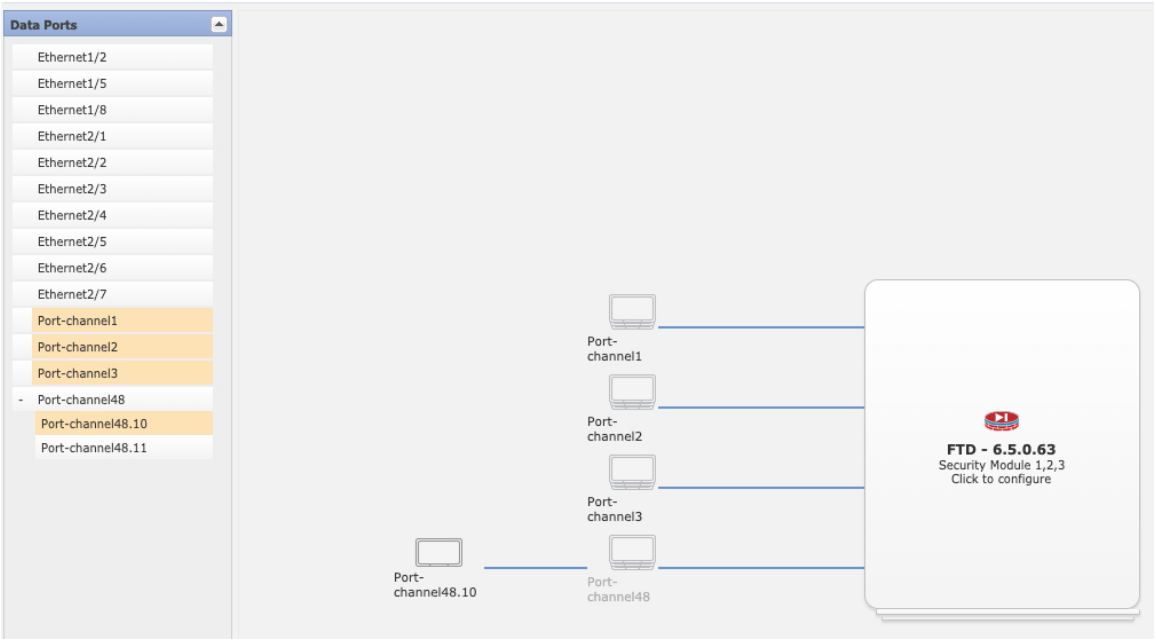
la grappe. Si vous devez créer un nouveau profil, annulez la création de la grappe et ajoutez-en un à l'aide de Permet d'ajouter un profil de ressource pour les instances de conteneur.

Remarque Si vous affectez un profil différent aux instances d'une grappe établie, ce qui permet des profils non concordants, appliquez d'abord le nouveau profil sur les nœuds de données; après leur redémarrage et leur redémarrage, vous pouvez appliquer le nouveau profil au nœud de contrôle.

g) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 4 Choisissez les interfaces que vous souhaitez affecter à cette grappe.



Pour une mise en grappe en mode natif : toutes les interfaces valides sont attribuées par défaut. Si vous avez défini plusieurs interfaces de type grappe, désélectionnez toutes les interfaces sauf une.

Pour une mise en grappe à plusieurs instances : choisissez chaque interface de données que vous souhaitez affecter à la grappe, ainsi que la sous-interface de canal de port ou de sous-interface de canal de port.

Étape 5 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 6 Dans la page des informations de la grappe(**Cluster Information**), procédez comme suit :

Illustration 3 : Grappe native

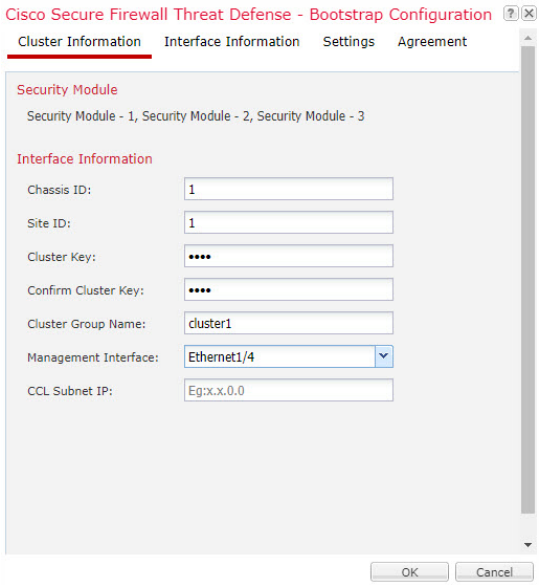
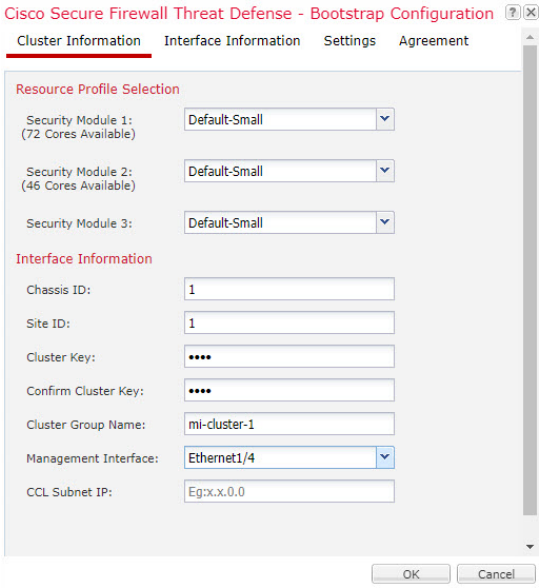


Illustration 4 : Grappe multi-instances



a) (Instance de conteneur pour le Firepower 9300 uniquement) Dans la zone de **sélection du module de sécurité (SM) et du profil de ressources**, vous pouvez définir un profil de ressources différent par module ; par exemple, si vous utilisez différents types de modules de sécurité et que vous souhaitez utiliser plus de CPU sur un modèle d'entrée de gamme.

b) Pour la mise en grappe sur plusieurs châssis, dans le champ **Chassis ID**, saisissez un ID de châssis. Chaque châssis de la grappe doit utiliser un ID unique.

   Ce champ ne s’affiche que si vous avez ajouté une interface membre au canal de port 48 de la liaison de commande de grappe.

c) Pour la mise en grappe inter-sites, dans le champ **Site ID**, saisissez l'ID de site pour ce châssis entre 1 et 8. Fonctionnalité FlexConfig : Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation de directeur, la redondance de site et la mobilité du flux de grappe, peuvent uniquement être configurées à l'aide de la fonctionnalité FlexConfig centre de gestion.

d) Dans le champ **Cluster Key** (clé de la grappe), configurez une clé d'authentification pour le trafic de contrôle sur la liaison de commande de la grappe.

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette option 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.

e) Définissez le **nom du groupe de grappes**, qui est le nom du groupe de grappes dans la configuration de périphérique logique.

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères.

Important À partir de la version 2.4.1, les espaces dans le nom de groupe de la grappe seront considérés comme des caractères spéciaux et peuvent entraîner une erreur lors du déploiement des périphériques logiques. Pour éviter ce problème, vous devez renommer le nom du groupe de grappe sans espace.

f) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

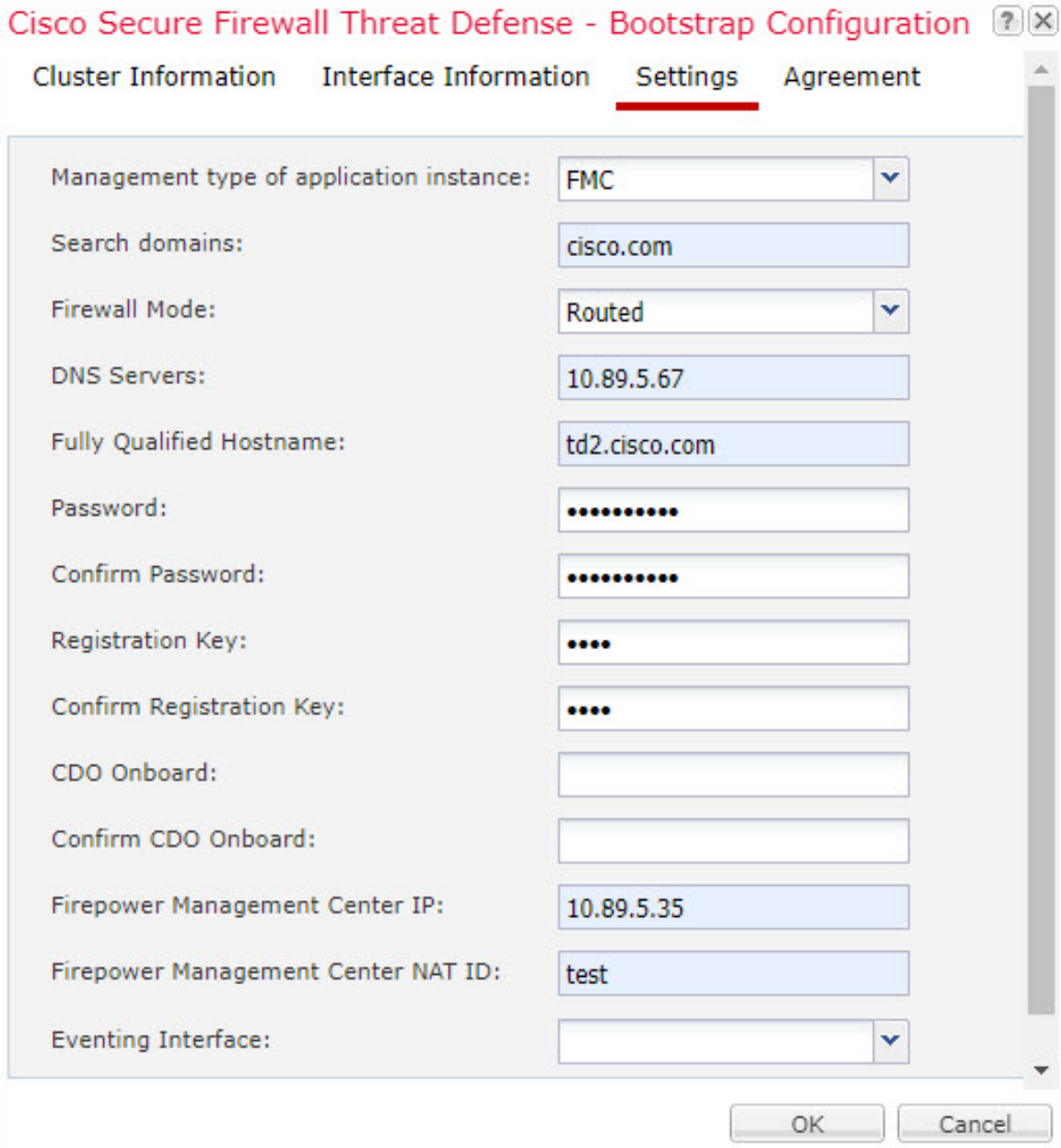
Si vous attribuez une interface pouvant être utilisée par Hardware Bypass comme interface de gestion, un message d'avertissement s'affiche pour vous assurer que cette affectation est intentionnelle.

g) (Facultatif) Définissez l'**adresse IP du sous-réseau CCL** comme *a*.*b*.**0.0**.

Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Dans ce cas, spécifiez n'importe quelle adresse réseau /16 sur un réseau unique pour la grappe, à l'exception des adresses de boucle avec retour (127.0.0.0/8), de multidiffusion (224.0.0.0/4) et internes (169.254.0.0/16). Si vous définissez la valeur sur 0.0.0.0, le réseau par défaut est utilisé.

Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID de logement : *a*.*b*.*id_châssis*.*id_logement*.

Étape 7 Sur la page **Settings** (paramètres), effectuez les opérations suivantes.



a) Dans le champ **Clé d'enregistrement**, entrez la clé à partager entre le centre de gestion et les membres de la grappe lors de l'enregistrement.

   Vous pouvez choisir n'importe quelle chaîne de texte pour cette clé entre 1 et 37 caractères; vous entrez la même clé sur centre de gestion lorsque vous ajoutez Défense contre les menaces.

b) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Défense contre les menaces pour l'accès à l'interface de ligne de commande.

c) Dans le champ **Firepower Management Center IP** field, saisissez l'adresse IP du centre de gestion de gestion.Si vous ne connaissez pas l'adresse IP de centre de gestion, laissez ce champ vide et saisissez une phrase d'accès dans le champ **ID NAT du Firepower Management Center**.

d) (Facultatif) Pour une instance de conteneur, à la question sur l'autorisation du mode expert à partir de sessions SSD FTD (**Permit Expert mode from FTD SSH sessions**): répondez oui (**Yes**) ou non (**No**). Le mode expert fournit à Défense contre les menaces un accès à l'interpréteur de commandes (shell) pour un dépannage avancé.

Si vous choisissez **Yes** (oui) pour cette option, les utilisateurs qui accèdent à l'instance de conteneur directement à partir d'une session SSH peuvent passer en mode expert. Si vous choisissez **No** (non), seuls les utilisateurs qui accèdent à l'instance de conteneur à partir de l'interface de ligne de commande de FXOS peuvent passer en mode expert. Nous vous recommandons de choisir **No** (non) pour augmenter l'isolement entre les instances.

Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour entrer dans ce mode, utilisez la commande **expert** dans l'interface de ligne de commande de Défense contre les menaces.

e) (Facultatif) Dans le champ **Search Domains** (domaines de recherche), saisissez une liste de domaines de recherche séparés par des virgules pour le réseau de gestion.

f) (Facultatif) Dans la liste déroulante **Mode de pare-feu**, choisissez **Transparent** ou **Routé**.

En mode routage, l'Défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

g) (Facultatif) Dans le champ **Serveurs DNS**, entrez une liste de serveurs DNS séparés par des virgules.

Par exemple, Défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

h) (Facultatif) Dans le champ **ID NAT Firepower Management Center**, saisissez une phrase secrète que vous saisirez également sur centre de gestion lorsque vous ajouterez la grappe en tant que nouveau périphérique.

Normalement, vous avez besoin des deux adresses IP (et d'une clé d'enregistrement) à des fins de routage et d'authentification : le centre de gestion indique l'adresse IP du périphérique et le périphérique indique l'adresse IP centre de gestion. Toutefois, si vous ne connaissez qu'une seule des adresses IP, ce qui est le minimum requis à des fins de routage, vous devez également spécifier un ID NAT unique des deux côtés de la connexion afin d'établir la confiance pour la communication initiale et de rechercher la clé d'enregistrement correcte. Vous pouvez spécifier n'importe quelle chaîne de texte comme ID NAT (de 1 à 37 caractères). Le centre de gestion et le périphérique utilisent la clé d'enregistrement et l'ID NAT (au lieu des adresses IP) pour l'authentification et l'autorisation pour l'enregistrement initial.

i) (Facultatif) Dans le champ **Full Qualified Hostname** (nom d'hôte complet), saisissez un nom qualifié complet pour le périphérique Défense contre les menaces.

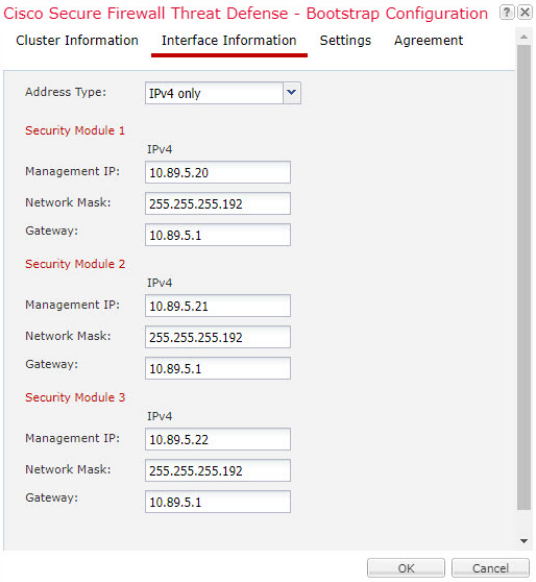
Les caractères valides sont les lettres de a à z, les chiffres de 0 à 9, le point (.) et le tiret (-); Le nombre maximal de caractères est de 253.

j) (Facultatif) Choisissez **l'interface d'événements** dans la liste déroulante, sur laquelle les événements doivent être envoyés. Si aucune interface d'événement n'est pas spécifiée, l'interface de gestion sera utilisée.

Pour spécifier une interface distincte à utiliser pour les événements, vous devez configurer une interface en tant *qu'interface d'événements Firepower*.Si vous affectez une interface pouvant être utilisée par Hardware Bypass comme interface d'événements, un message d'avertissement s'affiche pour vous assurer que cette affectation est intentionnelle.

Étape 8 Dans la page **Interface Information** (information sur l'interface), configurez une adresse IP de gestion pour chaque module de sécurité de la grappe. Sélectionnez le type d'adresse dans la liste déroulante **Address Type**, puis procédez comme suit pour chaque module de sécurité.

Remarque Vous devez définir l'adresse IP pour les 3 logements de module d'un châssis, même si un module n'est pas installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.



a) Dans le champ **Management IP** (Adresse IP de gestion), configurez une adresse IP locale.

Spécifiez une adresse IP unique sur le même réseau pour chaque module.

b) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

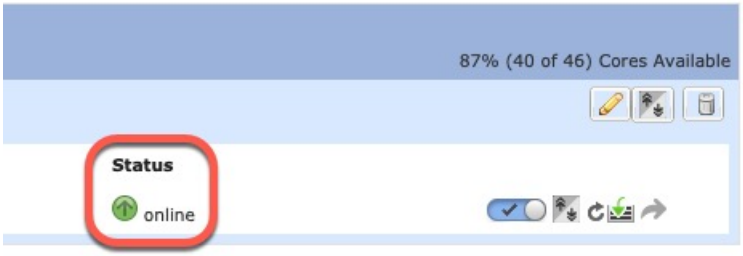
c) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 9 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 10 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 11 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique affiche son **état** comme **en ligne**, vous pouvez ajouter le châssis restant de la grappe ou, pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Étape 12 Pour la mise en grappe sur plusieurs châssis, ajoutez le châssis suivant à la grappe :

a) Sur le premier châssis de gestionnaire de châssis, cliquez sur l'icône **Show Configuration** (afficher la configuration) dans le coin supérieur droit; copiez la configuration de grappe affichée.

b) Connectez-vous à gestionnaire de châssis sur le châssis suivant et ajoutez un périphérique logique en fonction de cette procédure.

c) Choisissez **Je veux : > Rejoindre une grappe existante**.

d) **- OK**.

e) Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.

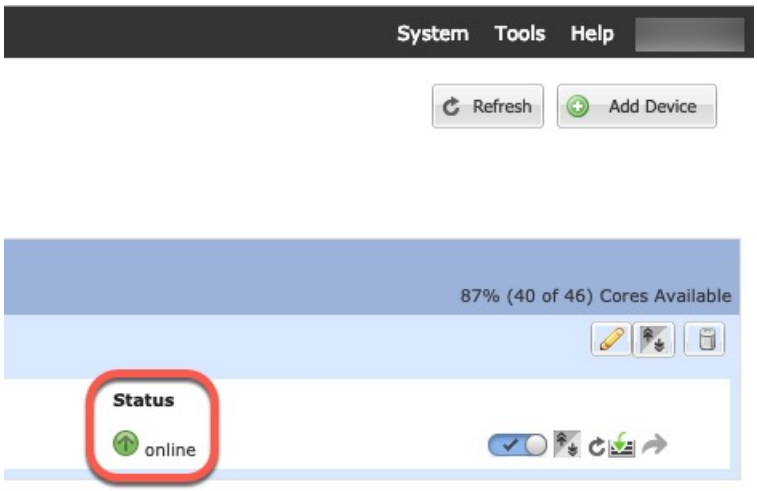
f) Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont pour la plupart préremplies, mais vous devez modifier les paramètres suivants :

- **Chassis ID** : saisissez un ID de châssis unique.
- **Site ID** : pour la mise en grappe inter-sites, saisissez l'ID de site pour ce châssis entre 1 et 8. Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation de directeur, la redondance de site et la mobilité du flux de grappe, peuvent uniquement être configurées à l'aide de la fonctionnalité FlexConfig centre de gestion.
- **Cluster Key**(clé de grappe) : (non préremplie) Saisissez la même clé de grappe.
- **Management IP** : Modifiez l'adresse de gestion pour chaque module afin qu'elle soit une adresse IP unique sur le même réseau que les autres membres de la grappe.

Cliquez sur **OK**.

g) Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Étape 13 Ajoutez l'unité de contrôle à centre de gestion en utilisant l'adresse IP de gestion.

Toutes les unités de grappe doivent faire partie d'une grappe formée avec succès sur FXOS avant d'être ajoutées à centre de gestion.

Le centre de gestion détecte ensuite automatiquement les unités de données.

Ajouter d'autres nœuds de grappe

Ajoutez ou remplacez le nœud de grappe Défense contre les menaces dans une grappe existante. Lorsque vous ajoutez un nouveau nœud de grappe dans FXOS, centre de gestion ajoute automatiquement le nœud.

Remarque Les étapes FXOS de cette procédure s'appliquent uniquement à l'ajout d'un nouveau *châssis*. si vous ajoutez un nouveau module à un Firepower 9300 pour lequel la mise en grappe est déjà activée, le module sera ajouté automatiquement.

Avant de commencer

- Dans le cas d'un remplacement, vous devez supprimer l'ancien nœud de la grappe de centre de gestion. Lorsque vous le remplacez par un nouveau nœud, il est considéré comme un nouveau périphérique sur centre de gestion.
- La configuration de l'interface doit être la même sur le nouveau châssis. Vous pouvez exporter et importer la configuration du châssis FXOS pour faciliter ce processus.

Procédure

Étape 1 Si vous avez déjà mis à niveau l'image Défense contre les menaces à l'aide de centre de gestion, procédez comme suit *sur chaque châssis de la grappe*.

Lorsque vous avez effectué la mise à niveau à partir de centre de gestion, la version au démarrage de la configuration FXOS n'était pas mise à jour et l'ensemble autonome n'était pas installé sur le châssis. Ces deux éléments doivent être définis manuellement pour que le nouveau nœud puisse rejoindre la grappe en utilisant la bonne version d'image.

Remarque Si vous avez uniquement appliqué une version de correctif, vous pouvez ignorer cette étape. Cisco ne fournit pas d'ensembles autonomes pour les correctifs.

a) Installez l'image Défense contre les menaces en cours d'exécution sur le châssis en utilisant la page **System** > **Updates** (mises à jour du système).

b) Cliquez sur **Logical Devices** (Périphériques logiques), puis sur Icône Définir la version (). Pour un périphérique Firepower 9300 avec plusieurs modules, définissez la version pour chaque module.

La **version de démarrage** affiche le paquet d'origine avec lequel vous avez effectué le déploiement. La **version actuelle** affiche la version vers laquelle vous avez effectué la mise à niveau.

c) Dans le menu déroulant **New Version** (nouvelle version), choisissez la version que vous avez téléversée. Cette version doit correspondre à la **version actuelle** affichée et définira la version au démarrage pour qu'elle corresponde à la nouvelle version.

d) Sur le nouveau châssis, assurez-vous que le nouvel ensemble d'images est installé.

Étape 2 Sur un châssis de grappe existant gestionnaire de châssis, cliquez sur **Logical Devices** (Périphériques logiques).

Étape 3 Cliquez sur l'icône **Show Configuration** (Afficher la configuration) en haut à droite; copiez la configuration de la grappe affichée.

Étape 4 Connectez-vous à gestionnaire de châssis sur le nouveau châssis et cliquez sur **Add** > **Cluster** (Ajouter > Grappe > Ajouter un périphérique > Ajouter un périphérique).

Étape 5 Pour **Device Name** : indiquez un nom pour le périphérique.

Étape 6 - **OK**.

Étape 7 Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.

Étape 8 Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont en partie préremplies, mais vous devez définir les paramètres suivants :

Illustration 5 : Informations sur les grappes

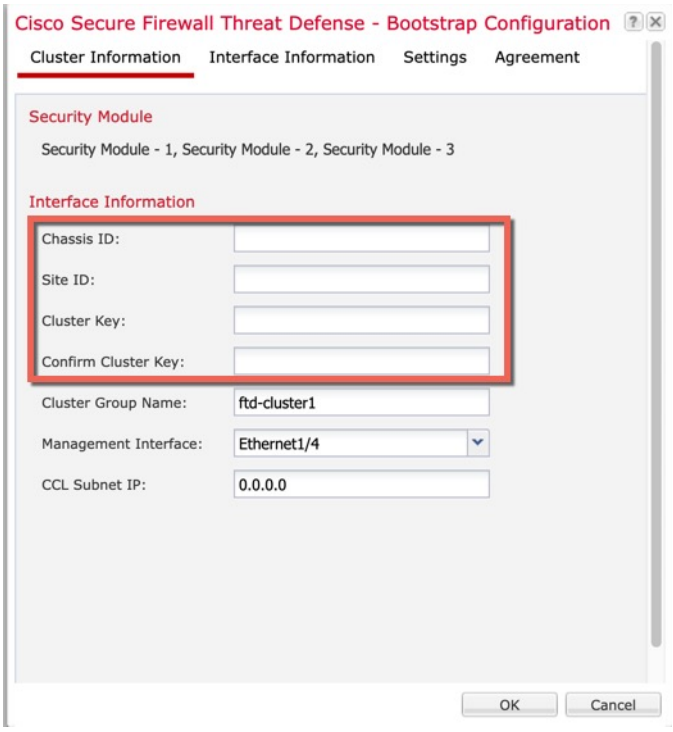


Illustration 6 : Information sur l'interface

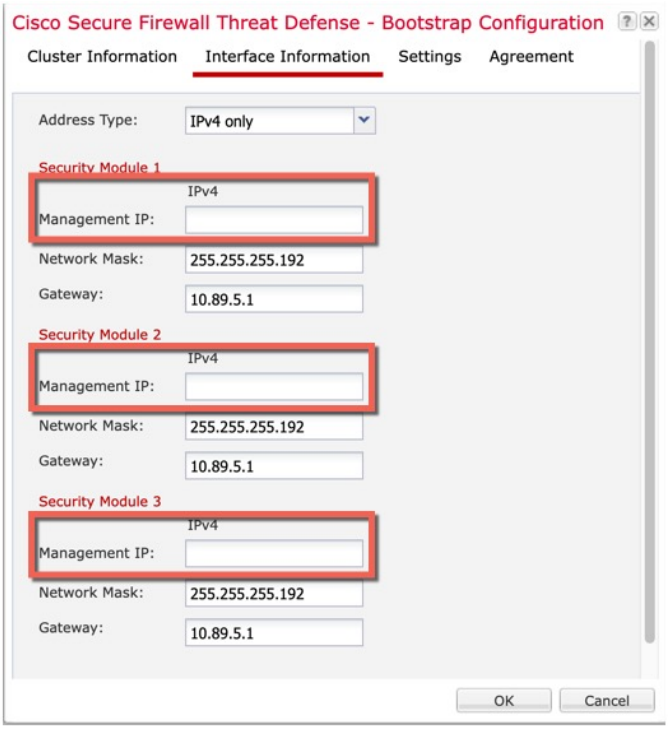
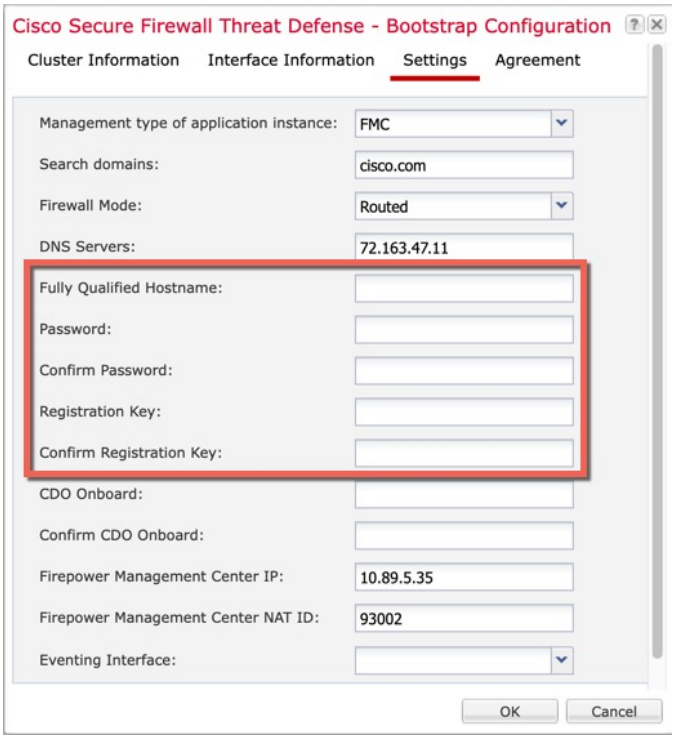


Illustration 7 : Paramètres

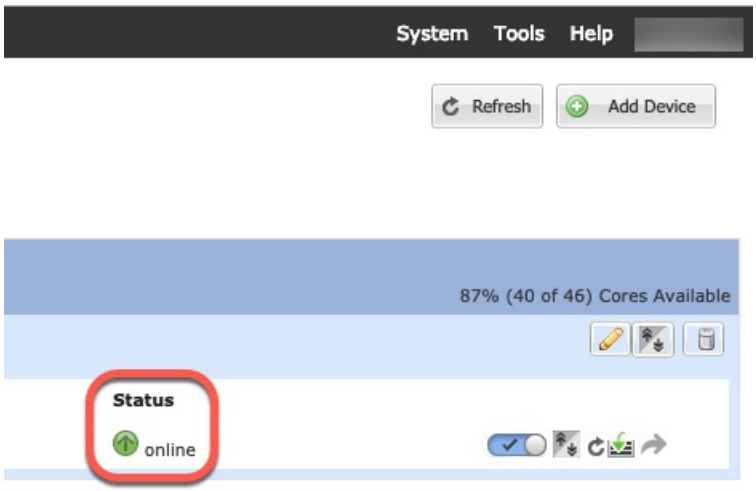


- **Chassis ID** : saisissez un ID de châssis *unique*.
- **Site ID** : pour la mise en grappe inter-sites, saisissez l'ID de site pour ce châssis entre 1 et 8. Cette fonctionnalité peut uniquement être configurée à l'aide de la fonctionnalité FlexConfig centre de gestion.
- **Cluster Key**(clé de grappe) : saisissez la *même* clé de grappe.
- **Management IP** (Adresse IP de gestion) : Modifiez l'adresse de gestion pour chaque module afin qu'elle soit une adresse IP *unique* sur le même réseau que les autres membres de la grappe.
- **Full Qualified Hostname**(nom d'hôte complet) : saisissez le *même* nom d'hôte.
- **Password**(mot de passe) : saisissez le *même* mot de passe.
- **Registration Key**(clé d'enregistrement) : saisissez la *même* clé d'enregistrement.

Cliquez sur **OK**.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Centre de gestion : ajouter une grappe

Ajoutez l'une des unités de grappe en tant que nouveau périphérique à Cisco Secure Firewall Management Center; le centre de gestion détecte automatiquement tous les autres membres de la grappe.

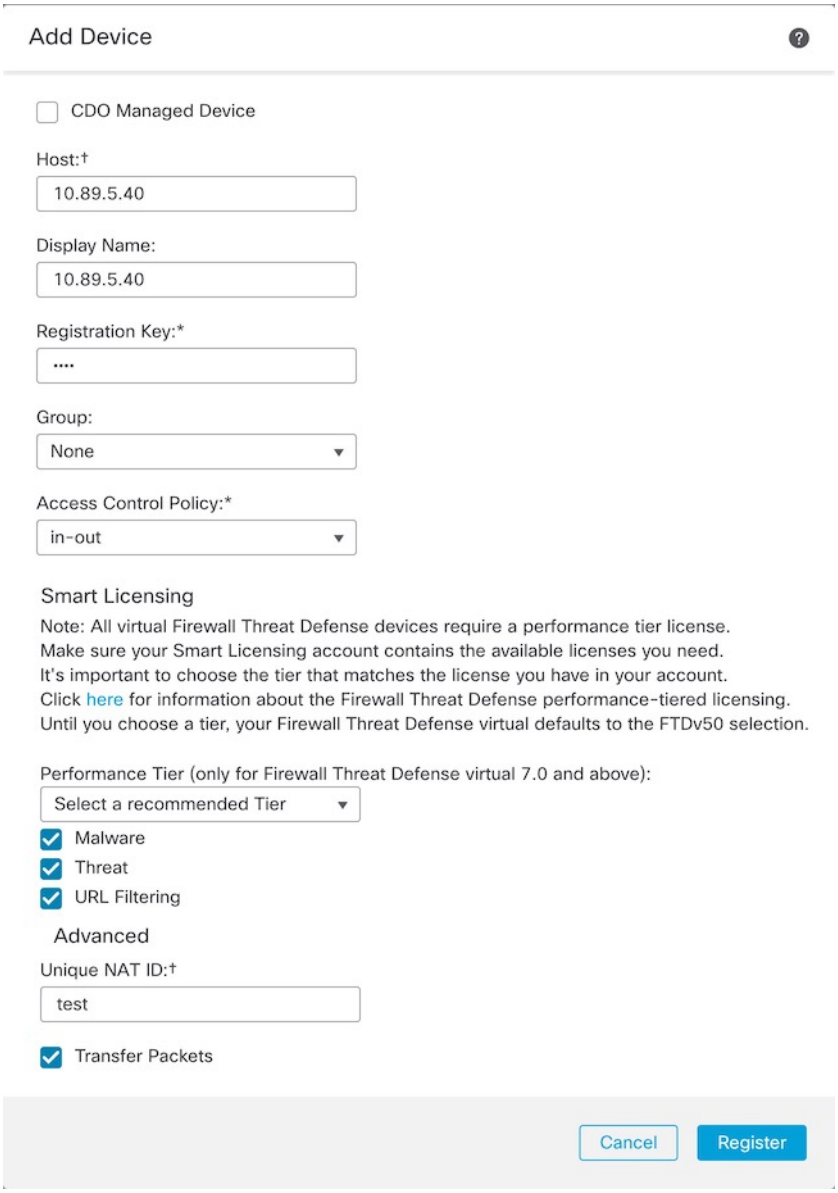
Avant de commencer

- Toutes les unités de grappe doivent faire partie d'une grappe créée avec succès sur FXOS avant d'être ajoutées à la grappe du centre de gestion. Vous devez également vérifier quelle unité est l'unité de contrôle. Reportez-vous à l'écran gestionnaire de châssis **Logical Devices** (Écrans logiques) ou utilisez la commande défense contre les menaces **show cluster info**.

Procédure

Étape 1 Dans le centre de gestion, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, puis choisissez **Add (Ajouter)** > **Add Device (Ajouter un périphérique)** pour ajouter l'unité de contrôle en utilisant l'adresse IP de gestion de l'unité que vous avez attribuée lors du déploiement de la grappe.

Illustration 8 : Ajouter un appareil



a) Dans le champ **Host** (Hôte), saisissez l'adresse IP ou le nom d'hôte de l'unité de contrôle.

   Nous vous recommandons d'ajouter l'unité de contrôle pour obtenir les meilleures performances, mais vous pouvez ajouter n'importe quelle unité de la grappe.

   Si vous avez utilisé un ID NAT lors de la configuration du périphérique , vous n'aurez peut-être pas besoin de remplir ce champ.

b) **Display Name**(Nom d'affichage) : saisissez le nom de l'unité de contrôle comme vous souhaitez qu'il apparaisse dans centre de gestion.

   Ce nom d'affichage n'est pas pour la grappe; elle concerne uniquement l'unité de contrôle que vous ajoutez. Vous pouvez ultérieurement modifier le nom d'autres membres de la grappe et le nom d'affichage de la grappe.

c) Dans le champ **Registration Key** (clé d'enregistrement), saisissez la clé d'enregistrement que vous avez utilisée lors du déploiement de la grappe dans FXOS. La clé d'enregistrement est un code secret partagé à usage unique.

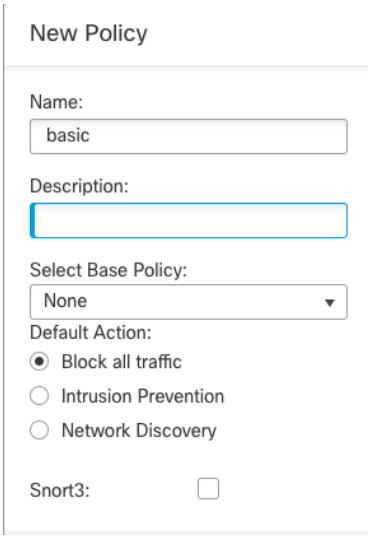
d) Dans un déploiement multidomaine, quel que soit votre domaine actuel, affectez le périphérique à un **domaine descendant**.

Si votre domaine actuel est un domaine descendant, le périphérique est automatiquement ajouté au domaine actuel. Si votre domaine actuel n'est pas un domaine descendant, après l'enregistrement, vous devez passer au domaine descendant pour configurer le périphérique.

e) (Facultatif) Ajouter le périphérique à un **groupe** de périphériques .

f) Choisissez une **politique de contrôle d'accès** initiale à déployer sur le périphérique lors de l'inscription ou créez une nouvelle politique.

Si vous créez une nouvelle politique, vous créez seulement une politique de base. Vous pourrez personnaliser la politique ultérieurement selon vos besoins.



g) Choisissez la licence à appliquer au périphérique.

h) Si vous avez utilisé un ID NAT lors de la configuration du périphérique , développez la section **Advanced** (Avancé) et saisissez le même ID NAT dans le champ **Unique NAT ID** (ID NAT unique).

i) Cochez la case **Transfer Packets** (Transférer les paquets) pour permettre au périphérique de transférer des paquets vers le centre de gestion.

Par défaut, cette option est activée. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous la décochez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

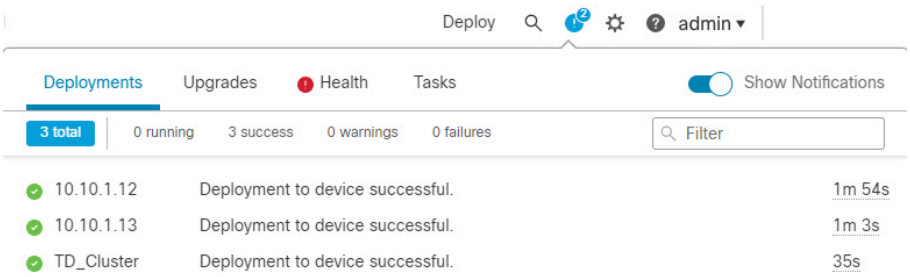
j) Cliquez sur **Register** (Inscrire).

Le centre de gestion identifie et enregistre l'unité de contrôle, puis enregistre toutes les unités de données. Si l'unité de contrôle ne s'enregistre pas avec succès, la grappe n'est pas ajoutée. Un échec de l'enregistrement peut se produire si la grappe n'était pas installée sur le châssis ou en raison d'autres problèmes de connectivité. Dans ce cas, nous vous recommandons d'essayer d'ajouter à nouveau l'unité de grappe.

Le nom de la grappe s'affiche sur la page **Devices (Périphériques)** > **Device Management** (gestion des périphériques); développez la grappe pour voir les unités de la grappe.

Une unité en cours d'enregistrement affiche l'icône de chargement.

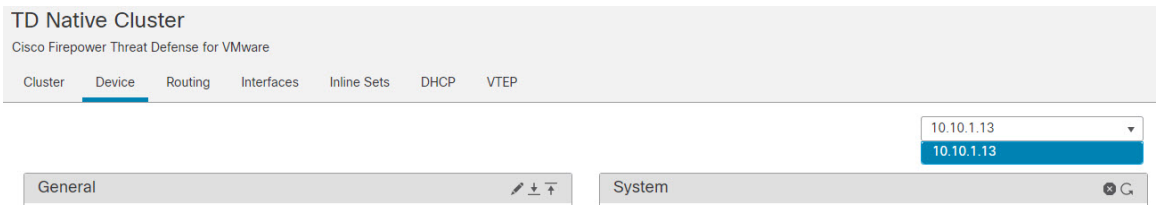
Vous pouvez surveiller l'enregistrement des unités de grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches). centre de gestion met à jour la tâche d'enregistrement de grappe à chaque enregistrement d'unité. Si des unités ne s'enregistrent pas, voir Rapprocher les membres de la grappe, à la page 49.



Étape 2 Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** ( ) de la grappe.

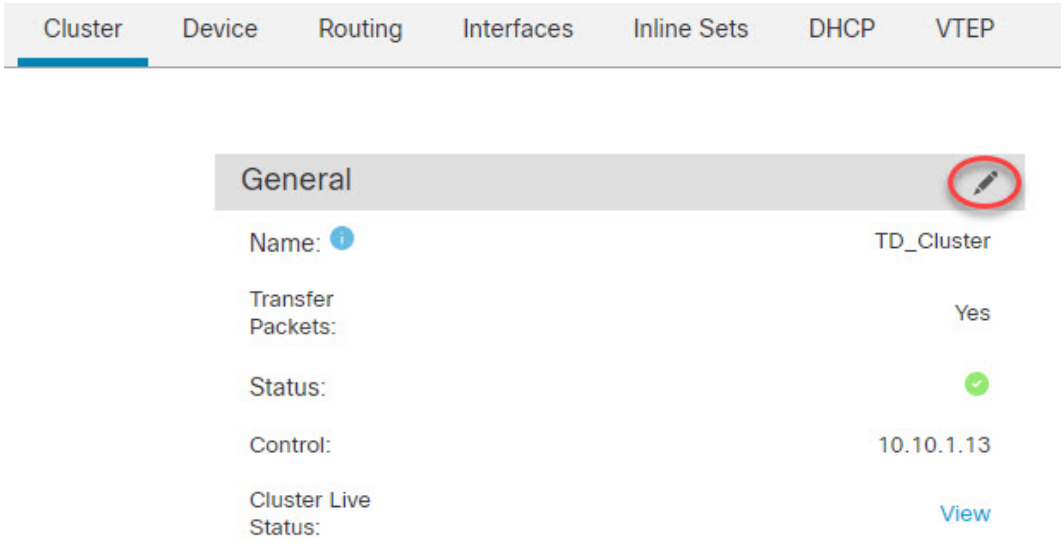
La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux unités membres de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par unité, mais vous ne pouvez configurer que les interfaces pour l'ensemble de la grappe.

Étape 3 Sur l'écran **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** , vous voyez les paramètres **General** (Général) , **License** (Licence), **System** (système), et **Health** (Intégrité).

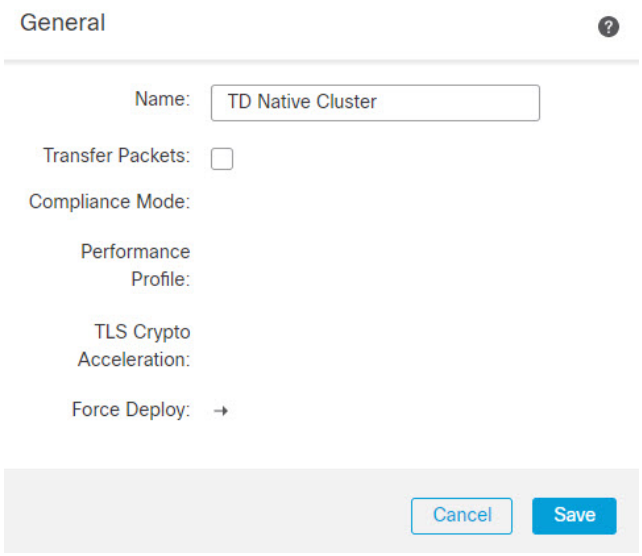


Consultez les éléments suivants, propres à la grappe :

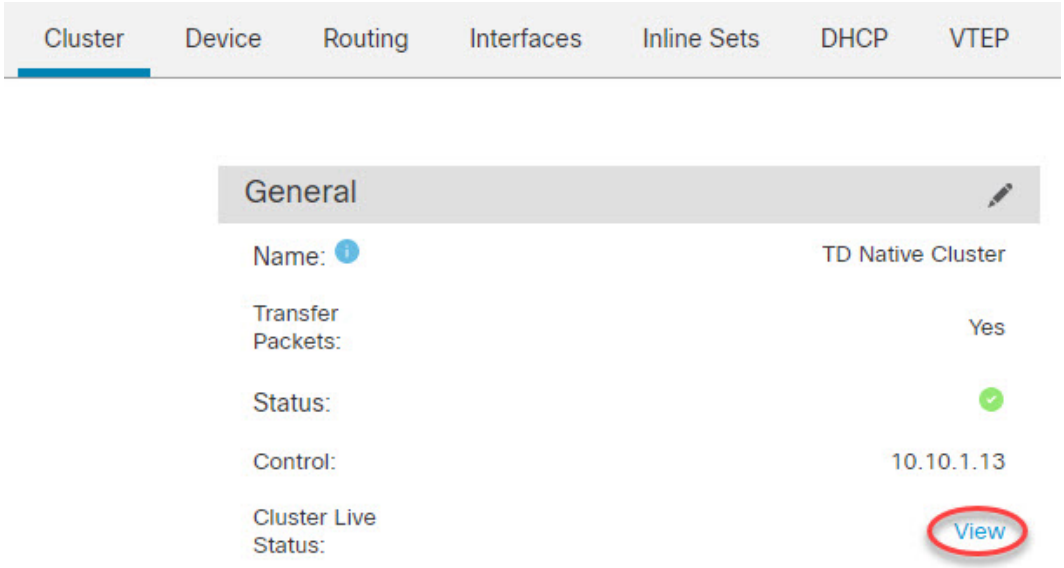
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



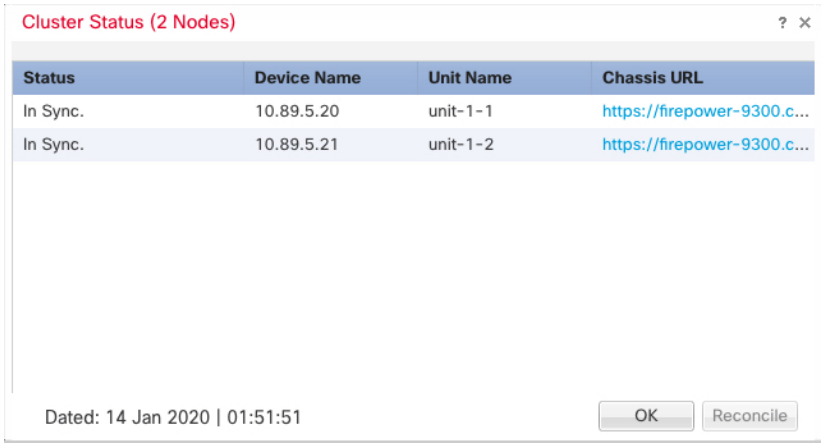
Définissez ensuite le champ **Name** (Nom).



- **General > View cluster status**(afficher l'état de la grappe) : Cliquez sur le lien **View cluster status** (afficher l'état de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).



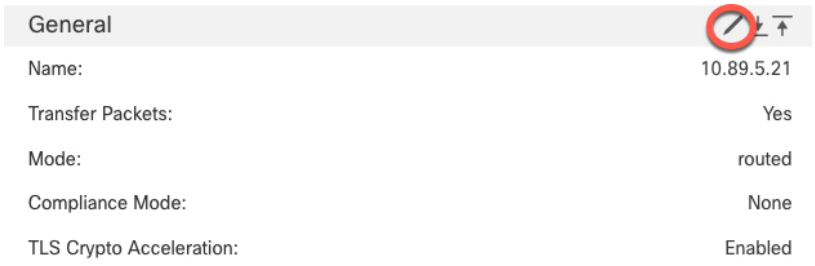
La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de réessayer l'enregistrement de l'unité de données en cliquant sur **Reconcile** (Rapprocher).



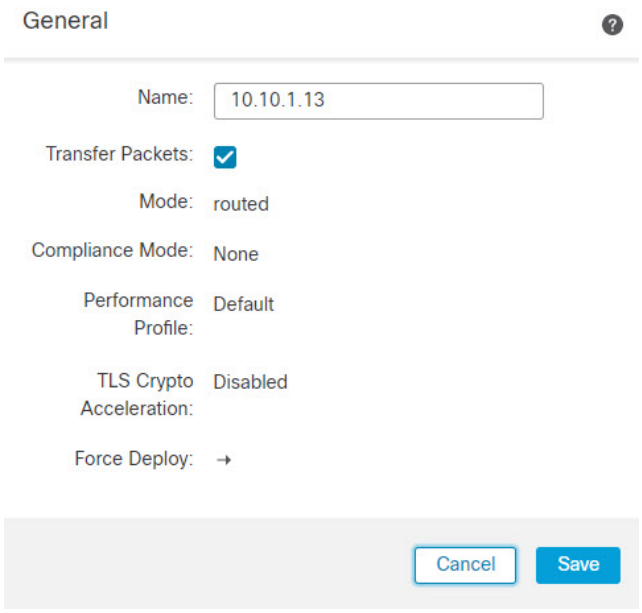
- **License** (Licence) : cliquez sur **Edit** (✎) pour définir les droits de licence.

Étape 4 Sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

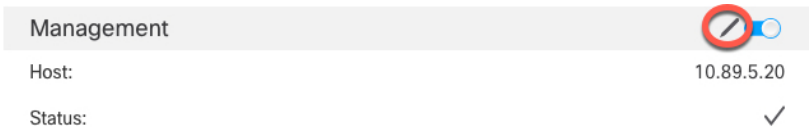
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** (✎).



Définissez ensuite le champ **Name** (Nom).



- **Management > Host** (Gestion > Hôte) : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, votre modification doit correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau; Modifiez l'adresse de l' **hôte** dans la zone **Management** (Gestion).



Centre de gestion : configurer les interfaces de grappe, de données et de dépistage

Cette procédure configure les paramètres de base pour chaque interface de données que vous avez affectée à la grappe lorsque vous l'avez déployée dans FXOS. Pour la mise en grappe sur plusieurs châssis, les interfaces de données sont toujours des interfaces EtherChannel étendus. Pour l'interface de liaison de commande de

grappe pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300, vous devez augmenter la MTU par rapport à la valeur par défaut. Vous pouvez également configurer l'interface de dépistage, qui est la seule interface pouvant être exécutée comme une interface individuelle.

Remarque Lorsque vous utilisez des EtherChannels étendus pour la mise en grappe sur plusieurs châssis, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers une unité qui n'est pas une unité active dans la grappe.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Edit** (✎) à côté de la grappe.

Étape 2 Cliquez sur **Interfaces**.

Étape 3 Configurer la liaison de commande de grappe

Pour la mise en grappe sur plusieurs châssis, définissez la MTU de la liaison de commande de grappe sur au moins 100 octets au-dessus de la MTU la plus élevée des interfaces de données. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. Nous vous suggérons de définir la MTU au maximum de 9184; la valeur minimale est de 1400 octets. Par exemple, comme la MTU maximale est de 9084 octets, la MTU de l'interface de données la plus élevée peut s'établir à 8984, tandis que la liaison de commande de grappe peut être définie sur 9084.

Pour les grappes natives : l'interface de liaison de commande de grappe utilise le canal de port 48 par défaut. Si vous ne savez pas quelle interface constitue la liaison de commande de grappe, vérifiez la configuration FXOS pour châssis pour l'interface de type grappe affectée à la grappe.

a) Cliquez sur **Edit** (✎) pour l'interface de liaison de commande de la grappe.
b) Dans la page **General** (Généralités) , dans le champ **MTU**, saisissez une valeur comprise entre 1400 et 9184. Nous vous suggérons d'utiliser le maximum, 9184.
c) Cliquez sur **OK**.

Étape 4 Configurer les interfaces de données.

a) (Facultatif) Configurer les sous-interfaces VLAN sur l'interface de données. Le reste de cette procédure s'applique aux sous-interfaces. Consultez Ajouter une sous-interface.
b) Cliquez sur **Edit** (✎) pour l'interface de données.
c) Configurez le nom, l'adresse IP et d'autres paramètres en fonction de Configurer les interfaces en mode routé ou Configurer les interfaces de groupe de ponts.

Remarque Si la MTU de l'interface de liaison de commande de grappe ne dépasse pas d'au moins 100 octets la MTU de l'interface de données, vous verrez une erreur indiquant que vous devez réduire la MTU de l'interface de données. Consultez Étape 3, à la page 36 pour augmenter la MTU de liaison de commande de grappe, après quoi vous pouvez continuer à configurer les interfaces de données.

d) Pour la mise en grappe sur plusieurs châssis, définissez une adresse MAC globale manuelle pour l'EtherChannel. Cliquez sur **Avancé**, et dans le champ **Adresse MAC active**, entrez une adresse MAC au format H.H.H, où H est un chiffre hexadécimal de 16 bits.

Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

Ne définissez pas l'**adresse MAC en veille**; elle est ignorée.

Vous devez configurer une adresse MAC pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

e) Cliquez sur **OK**. Répétez les étapes ci-dessus pour les autres interfaces de données.

Étape 5 (Facultatif) Configurez l'interface de dépistage.

L'interface de dépistage est la seule interface qui peut s'exécuter en mode d'interface individuelle. Vous pouvez utiliser cette interface pour les messages syslog ou SNMP, par exemple.

a) Choisissez **Objects** > **Object Management** > **Address Pools** pour ajouter un ensemble d'adresses IPv4 et/ou IPv6. Consultez Réserves d'adresses.

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. L'adresse IP virtuelle ne fait pas partie de ce ensemble, mais doit se trouver sur le même réseau. Vous ne pouvez pas déterminer l'adresse locale exacte attribuée à chaque unité à l'avance.

b) Dans **Devices** > **Device Management** > **Interfaces** (Périphériques > Gestion des périphériques > Interfaces), cliquez sur **Edit** (✎) pour l'interface de dépistage.
c) Dans **IPv4**, entrez **l'adresse IP** et le masque. Cette adresse IP est une adresse fixe pour la grappe et appartient toujours à l'unité de contrôle actuelle.
d) Dans la liste déroulante **IPv4 Address Pool** (ensemble d'adresses IPv4), choisissez l'ensemble d'adresses que vous avez créé.
e) Sur **IPv6 > Basic**, dans la liste déroulante **IPv6 Address Pool** (ensemble d'adresses IPv6), choisissez l'ensemble d'adresses que vous avez créées.
f) Configurez les autres paramètres de l'interface normalement.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Centre de gestion : configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 9 : Paramètres de surveillance de l'intégrité de la grappe

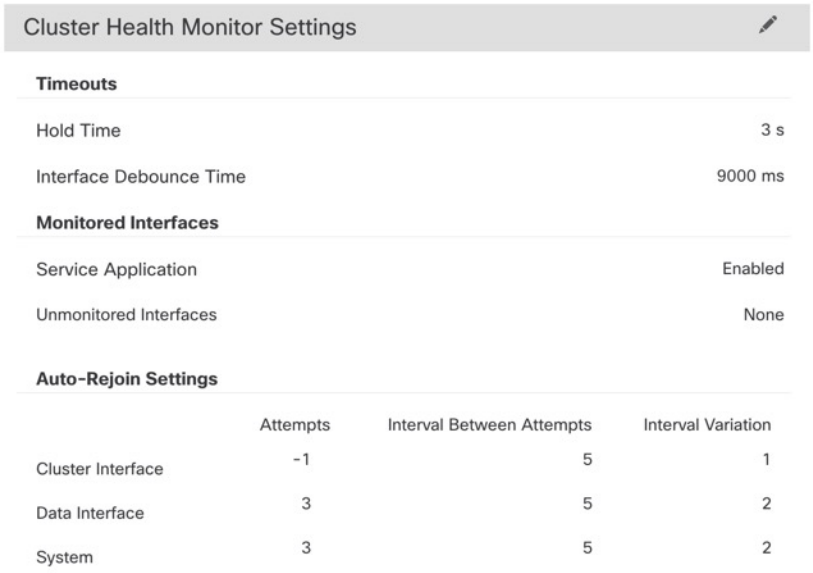


Tableau 1 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe 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.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.

Champ	Description
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

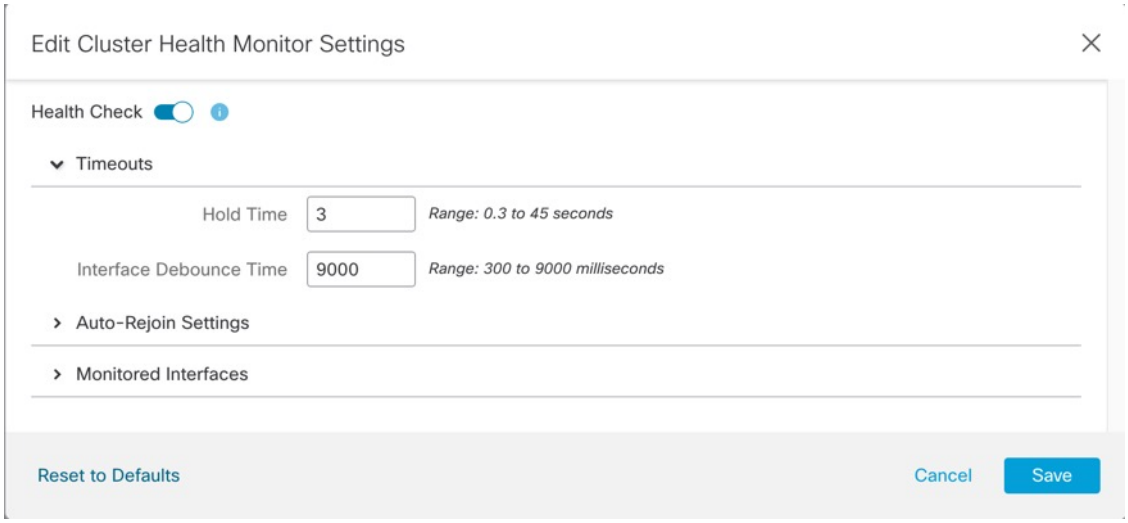
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 10 : Désactiver la vérification de l'intégrité du système



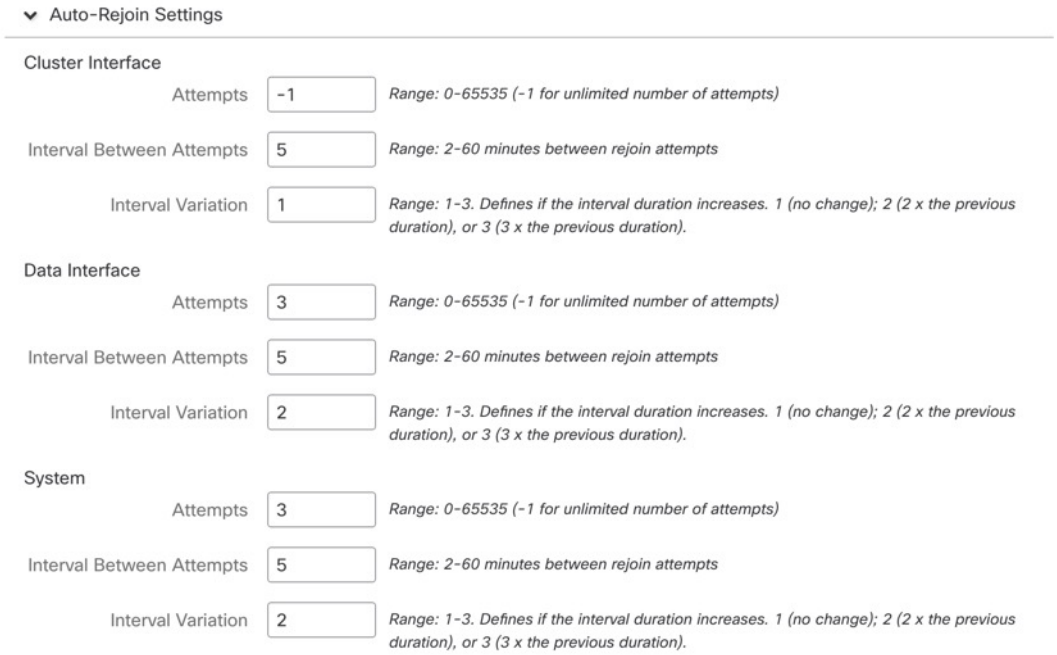
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité 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 tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent 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, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 11 : Configurer les paramètres de jonction automatique

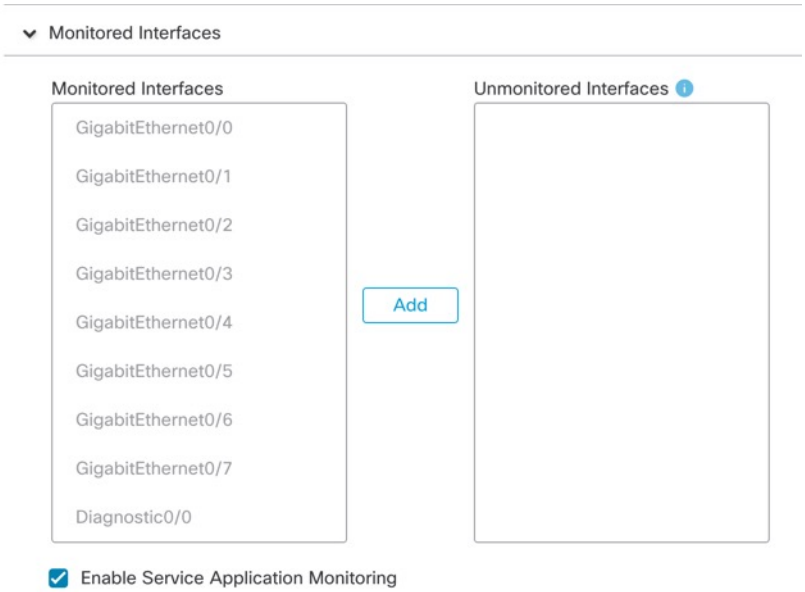


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : 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. définissez la valeur 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**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 12 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud 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 tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

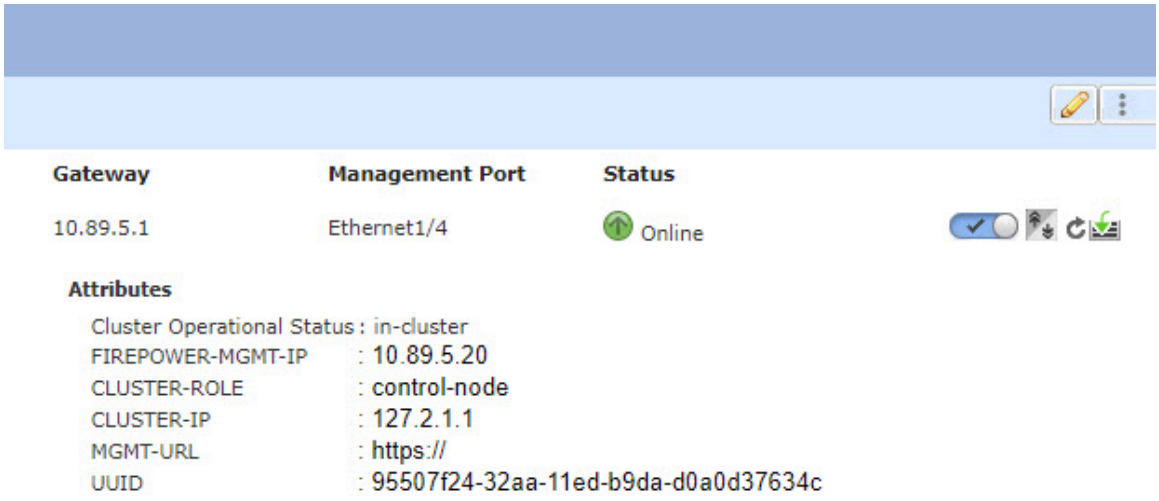
FXOS : Supprimer un nœud de la grappe

Les sections suivantes décrivent comment supprimer des nœuds de façon temporaire ou permanente de la grappe.

Suppression temporaire

Un nœud de grappe sera automatiquement supprimé de la grappe en raison d'une défaillance matérielle ou réseau, par exemple. Cette suppression est temporaire jusqu'à ce que les conditions soient rectifiées, et qu'il puisse rejoindre la grappe. Vous pouvez également désactiver manuellement la mise en grappe.

Pour vérifier si un appareil se trouve actuellement dans la grappe, vérifiez l'état de la grappe dans la page gestionnaire de châssis **Logical Devices**(périphériques logiques) : :



Pour l'utilisation de défense contre les menaces centre de gestion, vous devez laisser le périphérique dans la liste des périphériques centre de gestion afin qu'il puisse reprendre toutes ses fonctionnalités après avoir réactivé la mise en grappe.

- Disable clustering in the application (désactivez la mise en grappe dans l'application) : Vous pouvez désactiver la mise en grappe à l'aide de l'interface de ligne de commande de l'application. Saisissez la commande **cluster remove unit** *name* pour supprimer tout nœud autre que celui auquel vous êtes connecté. La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

  Lorsqu'un périphérique devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion 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 la configuration de démarrage. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe , l'interface de gestion est désactivée.

  Pour réactiver la mise en grappe, dans défense contre les menaces , saisissez **cluster enable**.

- Désactivez l'instance d'application : Dans la page gestionnaire de châssis dans la page **Logical Devices** (Périphériques logiques), cliquez sur **Curseur activé** ( ). Vous pourrez la réactiver ultérieurement à l'aide de **Curseur désactivé** ( ).

- Arrêtez le security module/engine : Dans gestionnaire de châssis sur la page **Security Module/Engine** (module/moteur de sécurité), cliquez sur l'icône **Mettre hors tension**.

- Arrêtez le châssis : dans le gestionnaire de châssis sur la page d'**aperçu**, cliquez sur l'icône**Arrêt**.

Suppression permanente

Vous pouvez supprimer définitivement un nœud de grappe en utilisant les méthodes suivantes.

Pour défense contre les menaces , à l'aide de centre de gestion, veillez à supprimer le nœud de la liste de périphériques centre de gestion après avoir désactivé la mise en grappe sur le châssis.

- Supprimez le périphérique logique :Dans la zone gestionnaire de châssis de la page **Logical Devices** (Périphériques logiques), cliquez sur **Supprimer** ( ). Vous pouvez ensuite déployer un périphérique logique autonome, une nouvelle grappe ou même ajouter un nouveau périphérique logique à la même grappe.
- Supprimez le châssis ou le module de sécurité du service : si vous mettez un périphérique hors du service, vous pouvez ajouter du matériel de remplacement en tant que nouveau nœud de la grappe.

FMC : gérer les membres de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les membres de celle-ci.

Ajouter un nouveau membre à la grappe

Lorsque vous ajoutez un nouveau membre de grappe dans FXOS, Cisco Secure Firewall Management Center ajoute automatiquement le membre.

Avant de commencer

- Vérifiez que la configuration de l'interface est la même sur l'unité de remplacement et sur l'autre châssis.

Procédure

Étape 1 Ajouter la nouvelle unité à la grappe dans FXOS. Consultez le guide de configuration de FXOS.

Attendez que la nouvelle unité soit ajoutée à la grappe. Reportez-vous à l'écran **Logical Devices** (périphériques logiques) du Firepower Chassis Manager ou utilisez la commande Firepower Threat Defense **show cluster info** pour afficher l'état de la grappe.

Étape 2 Le nouveau membre de la grappe est ajouté automatiquement. Pour surveiller l'enregistrement de l'unité de remplacement, consultez les éléments suivants :

- Boîte de dialogue **Cluster Status** (état de la grappe) (qui est accessible à partir de l'icône **Devices (Périphériques)** > **Device Management (Gestion des périphériques) Plus** ( ) ou de l'onglet **Devices** > **Device Management** > **Cluster (Grappe) > zone General** (Afficher l'état de la grappe) **> lien Cluster Live Status** (État de la grappe en direct)—Une unité qui rejoint la grappe sur le châssis affiche " En train de rejoindre la grappe..." Après avoir rejoint le groupe, centre de gestion tente de l'enregistrer et l'état passe à « disponible pour enregistrement ». Une fois l'enregistrement terminé, l'état passe à « In Sync » (en synchronisation). Si l'enregistrement échoue, le périphérique restera « disponible pour enregistrement ». Dans ce cas, forcez le réenregistrement en cliquant sur **Reconcile** (Rapprocher).
- État du système > **Tâches** : centre de gestion affiche tous les événements et les échecs d'enregistrement.

- **Appareils** > **Gestion des périphériques** : Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir qu'une unité est en train de s'enregistrer lorsque l'icône de chargement se trouve à gauche.

Remplacer un membre de la grappe

Vous pouvez remplacer un membre de grappe dans une grappe existante. Le centre de gestion détecte automatiquement l'unité de remplacement. Cependant, vous devez supprimer manuellement l'ancien membre de la grappe dans centre de gestion. Cette procédure s'applique également à une unité qui a été réinitialisée; dans ce cas, bien que le matériel reste le même, il semble s'agir d'un nouveau membre.

Avant de commencer

- Vérifiez que la configuration de l'interface est la même sur l'unité de remplacement et sur les autres châssis.

Procédure

Étape 1 Pour un nouveau châssis, si possible, sauvegardez et restaurez la configuration de l'ancien châssis dans FXOS.

Si vous remplacez un module dans un Firepower 9300, vous n'avez pas besoin d'effectuer ces étapes.

Si vous n'avez pas de configuration FXOS de secours pour l'ancien châssis, effectuez d'abord les étapes décrites dans Ajouter un nouveau membre à la grappe, à la page 44.

Pour en savoir plus sur les étapes ci-dessous, consultez le guide de configuration de FXOS.

a) Utilisez la fonction d'exportation de configuration pour exporter un fichier XML contenant les paramètres de configuration des périphériques logiques et de la plateforme pour votre châssis Firepower 4100/9300.
b) Importez le fichier de configuration dans le châssis de remplacement.
c) Acceptez le contrat de licence.
d) Si nécessaire, mettez à niveau la version de l'instance d'application de périphérique logique pour qu'elle corresponde au reste de la grappe.

Étape 2 Dans centre de gestion de l'ancienne unité, sélectionnez **Devices** > **Device Management** (Périphériques > Gestion des périphériques) > **Plus** (⋮) > **Delete** (Supprimer).

Étape 3 Confirmez que vous souhaitez supprimer l'unité.

L'unité est supprimée de la grappe et de la liste des périphériques centre de gestion.

Étape 4 Le nouveau membre ou le membre réinitialisé est ajouté automatiquement. Pour surveiller l'enregistrement de l'unité de remplacement, consultez les éléments suivants :

- Boîte de dialogue **Cluster Status** (Statut de la grappe) (**Devices** > **Device Management** > icône **Plus** (⋮) ou page **Devices** > **Device Management** > **Cluster** > **zone Générale** **(Voir l'état du cluster)** > **Cluster Live Status** (lien Statut de la grappe en direct)—Une unité qui rejoint la grappe sur le châssis affiche "En train de rejoindre la grappe..." Après avoir rejoint le groupe, centre de gestion tente de l'enregistrer et l'état passe à « disponible pour enregistrement ». Une fois l'enregistrement terminé, l'état passe à « In Sync » (en synchronisation). Si l'enregistrement échoue, le périphérique restera « disponible pour enregistrement ». Dans ce cas, forcez le réenregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- **System** (⚙) > **Tâches** : centre de gestion affiche tous les événements et les échecs d'enregistrement.
- **Appareils** > **Gestion des périphériques** : Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir qu'une unité est en train de s'enregistrer lorsque l'icône de chargement se trouve à gauche.

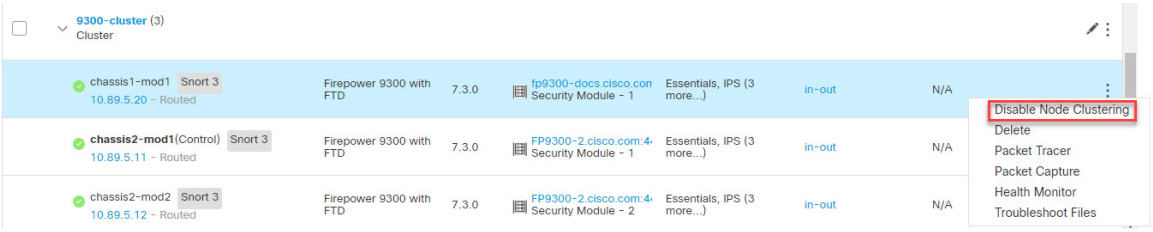
Désactiver un membre

Vous pouvez désactiver un membre en vue de la suppression de l'unité ou temporairement à des fins de maintenance. Cette procédure sert à désactiver temporairement un membre; l'unité apparaîtra toujours dans la liste de périphériques centre de gestion.

Remarque Lorsqu'une unité devient inactive, toutes les interfaces de données sont fermées; seule l'interface de gestion 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 l'unité a reçue lors de la configuration de démarrage. Cependant, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser la console pour toute autre configuration.

Procédure

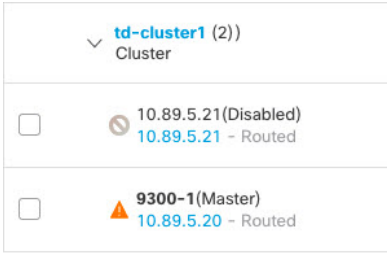
Étape 1 Pour l'unité que vous souhaitez désactiver, choisissez **Devices** > **Device Management** > **Plus** (⋮) > **Disable Clustering**(Périphériques > Gestion des périphériques > Désactiver la mise en grappe).



Vous pouvez également désactiver une unité à partir de la boîte de dialogue **d'état de la grappe** (**Périphériques** > **Gestion des périphériques** > **Plus** (⋮) > **État de la grappe en direct**).

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur l'unité.

L'unité affichera **(Désactivé)** à côté de son nom dans la liste **Devices** > **Device Management** (Périphériques > Gestion des périphériques).



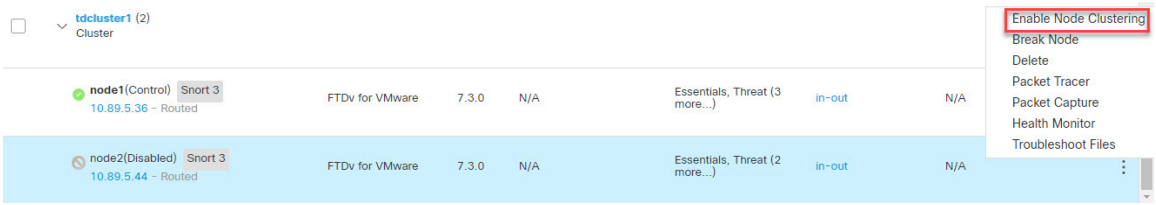
Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 47.

Rejoindre la grappe

Si une unité a été retirée de la grappe, par exemple en raison d'une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe . .

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, choisissez **Périphériques** > **Gestion des périphériques** > **Plus** (⋮) >**Activer la mise en grappe**.



Vous pouvez également réactiver une unité à partir de la boîte de dialogue **d'état de la grappe** (**Périphériques** > **Gestion des périphériques** > **Plus** (⋮) > **État de la grappe en direct**).

Étape 2 Confirmez que vous souhaitez activer la mise en grappe sur l'unité.

Supprimer (annuler l'enregistrement) un nœud de données.

Si vous devez supprimer définitivement un nœud de grappe (par exemple, si vous retirez un module sur le périphérique Firepower 9300 ou un châssis), vous devez le désinscrire de centre de gestion.

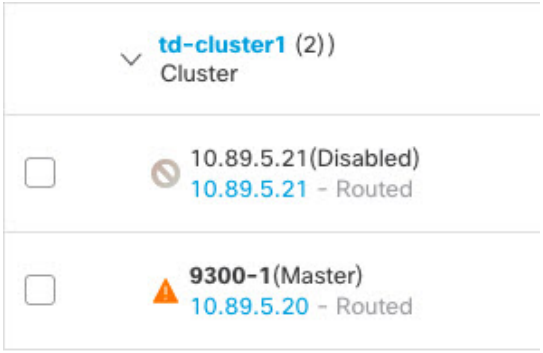
Ne désenregistrez pas le nœud s'il fait toujours partie intégrante de la grappe ou si vous souhaitez uniquement désactiver le nœud temporairement. Pour le supprimer définitivement de la grappe dans FXOS, consultez FXOS : Supprimer un nœud de la grappe, à la page 42. Si vous le désenregistrez du centre de gestion et qu'il fait toujours partie de la grappe, il continuera à laisser passer le trafic et pourrait même devenir le nœud de contrôle, un nœud de contrôle que le centre de gestion ne peut plus gérer.

Avant de commencer

Pour désactiver manuellement le nœud, voir Désactiver un membre, à la page 46. Avant d'annuler l'enregistrement d'un nœud, le nœud doit être inactif, manuellement ou en raison d'un problème d'intégrité.

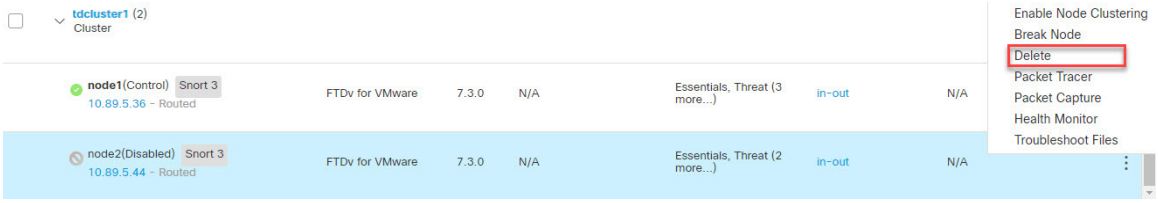
Procédure

Étape 1 Assurez-vous que le nœud est prêt à être désenregistré à partir de centre de gestion. Sur **Devices (périphériques)** > **Device Management**(gestion des périphériques) , assurez-vous que le nœud affiche **(Disabled)**.(désactivé).



Vous pouvez également afficher l'état de chaque nœud dans la boîte de dialogue **Cluster Status** (état de la grappe) accessible à partir de **Plus** (⋮). Si l'état est périmé, cliquez sur **Reconcile All** (Rappeocher tout) dans la boîte de dialogue **Cluster Status** (état de la grappe) pour forcer une mise à jour.

Étape 2 Dans le centre de gestion du nœud de données que vous souhaitez supprimer, choisissez **Périphériques** > **Gestion des périphériques Annuler l'enregistrement Plus** (⋮) **Supprimer.**



Étape 3 Confirmez que vous souhaitez l'enregistrement,supprimer le nœud.

Le nœud est supprimé de la grappe et de la liste des périphériques centre de gestion.

Changer l'unité de contrôle

Mise en garde La meilleure méthode pour changer d'unité de contrôle est de désactiver la mise en grappe sur l'unité de contrôle, d'attendre un nouveau choix de l'unité de contrôle, puis de réactiver la mise en grappe. Si vous devez préciser l'unité *exacte* qui deviendra l'unité de contrôle, utilisez la procédure décrite dans cette section. Notez que pour les fonctionnalités centralisées, si vous forcez un changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Pour changer d'unité de contrôle, procédez comme suit.

Procédure

Étape 1 Ouvrez la boîte de dialogue **ClusterStatus** (état de la grappe) en sélectionnant **Devices** > **Device Management** (Périphériques > Gestion des périphériques) **Plus** (⋮)

Vous pouvez également accéder à la boîte de dialogue **Cluster Status** (état de la grappe) à partir de la page **Périphériques** > **Gestion des périphériques** > **Grappe**, zone **> Général**) » lien **Cluster Live Status** (état actuel de la grappe).

Étape 2 Pour l'unité que vous souhaitez voir devenir l'unité de contrôle, sélectionnez (**Plus** (⋮) **> modifier le rôle en unité de contrôle)**.

Étape 3 Vous êtes invité à confirmer le changement de rôle. Cochez la case , puis cliquez sur **OK**.

Rapprocher les membres de la grappe

Si un membre de la grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du châssis de Cisco Secure Firewall Management Center. Par exemple, une unité de données peut ne pas s'enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management > (Gestion des périphériques) Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en direct de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Vous pouvez également ouvrir la boîte de dialogue **Cluster Status** (état de la grappe) à partir de la page **Devices (Périphériques)** > **Devices Management (Gestion des périphérique)** > **Cluster** (grappe) > zone (**> General** (Générale) **> lien Cluster Live Status** (Lien état actuel de la grappe).

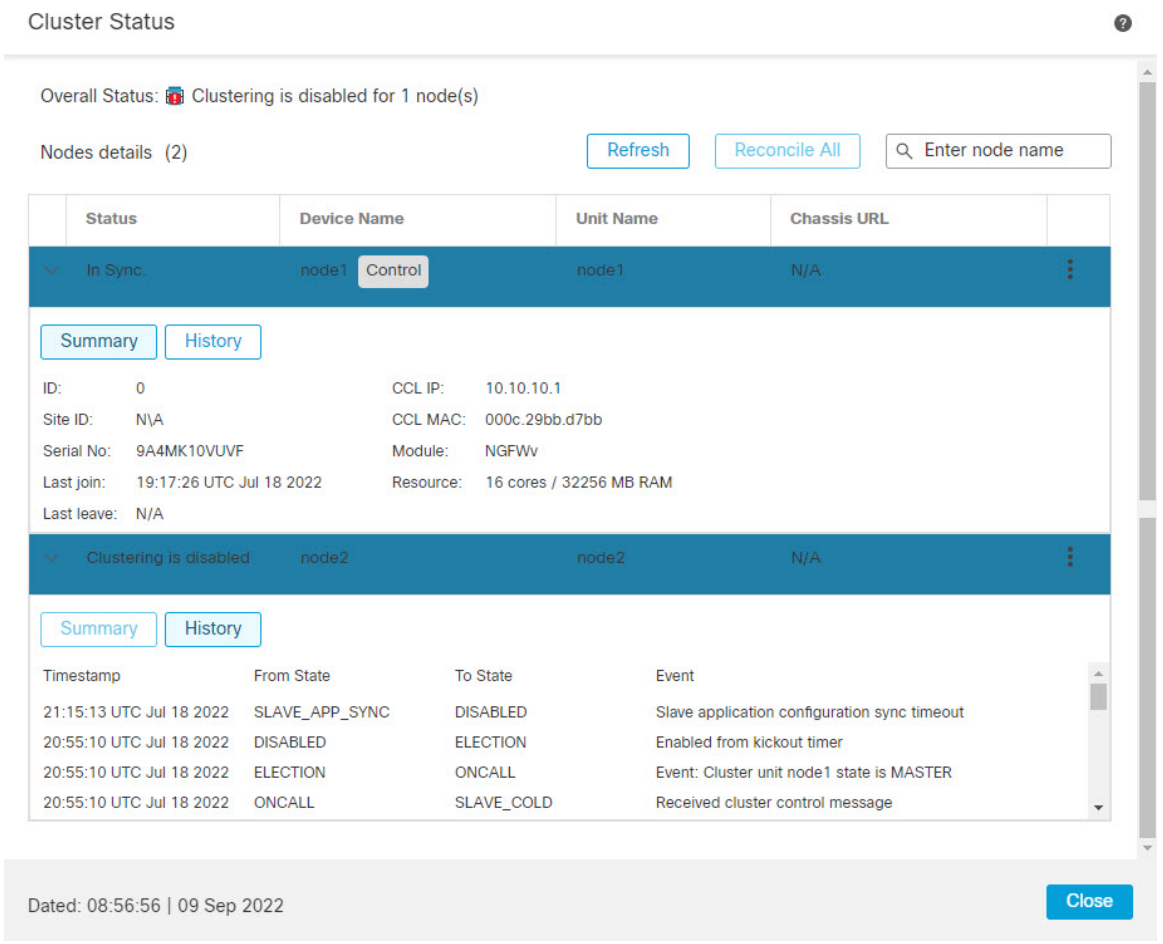
Étape 2 Cliquez sur **Reconcile All** (Tout faire concorder).

Pour plus d'informations sur l'état de la grappe, consultez Centre de gestion : surveillance de la grappe, à la page 50.

Centre de gestion : surveillance de la grappe

Vous pouvez surveiller la grappe dans Cisco Secure Firewall Management Center et sur la CLI défense contre les menaces .

- **Boîte de dialogue Cluster Status**& (état de la grappe), accessible à partir de l' icône **Devices** > **Device Management (gestion des périphériques) Plus** (⋮)ou à partir de la page **Devices** > **Device Management** > **Cluster**(page Périphériques de la gestion des périphériques en grappe) > zone **> General** (généralités) (Afficher l'état de la grappe) > lien **> Cluster Live Status**(état de la grappe en direct).



L'unité de contrôle est dotée d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En Synchro. : l'unité est enregistrée auprès de centre de gestion.
- En attente d'enregistrement : l'unité fait partie de la grappe, mais ne s'est pas encore enregistrée auprès de centre de gestion. Si une unité ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Rapprocher tout**.

- La mise en grappe est désactivée, : l'unité est enregistrée auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer l'unité de la grappe.
- Adhésion à une grappe... : l'unité rejoint la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque unité, vous pouvez afficher le **Résumé** ou l'**historique**.

Pour chaque unité dans le menu **Plus** (⋮), vous pouvez effectuer les modifications d'état suivantes :

- **Désactiver la mise en grappe**
- **Activer la mise en grappe**
- **Changer le rôle à Contrôle**

- **System** (⚙) > page **Tâches** (Tâches).

  La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à mesure que chaque unité s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster_name* (Nom de la grappe).

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir toutes les unités membres, y compris l'unité de contrôle affichée avec son rôle à côté de l'adresse IP. L'icône de téléversement représente les unités en cours d'enregistrement.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

Tableau de bord de surveillance de l'intégrité de la grappe

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte

la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .

- La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

- Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.
- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

Tableau 2 : Mesures de la grappe

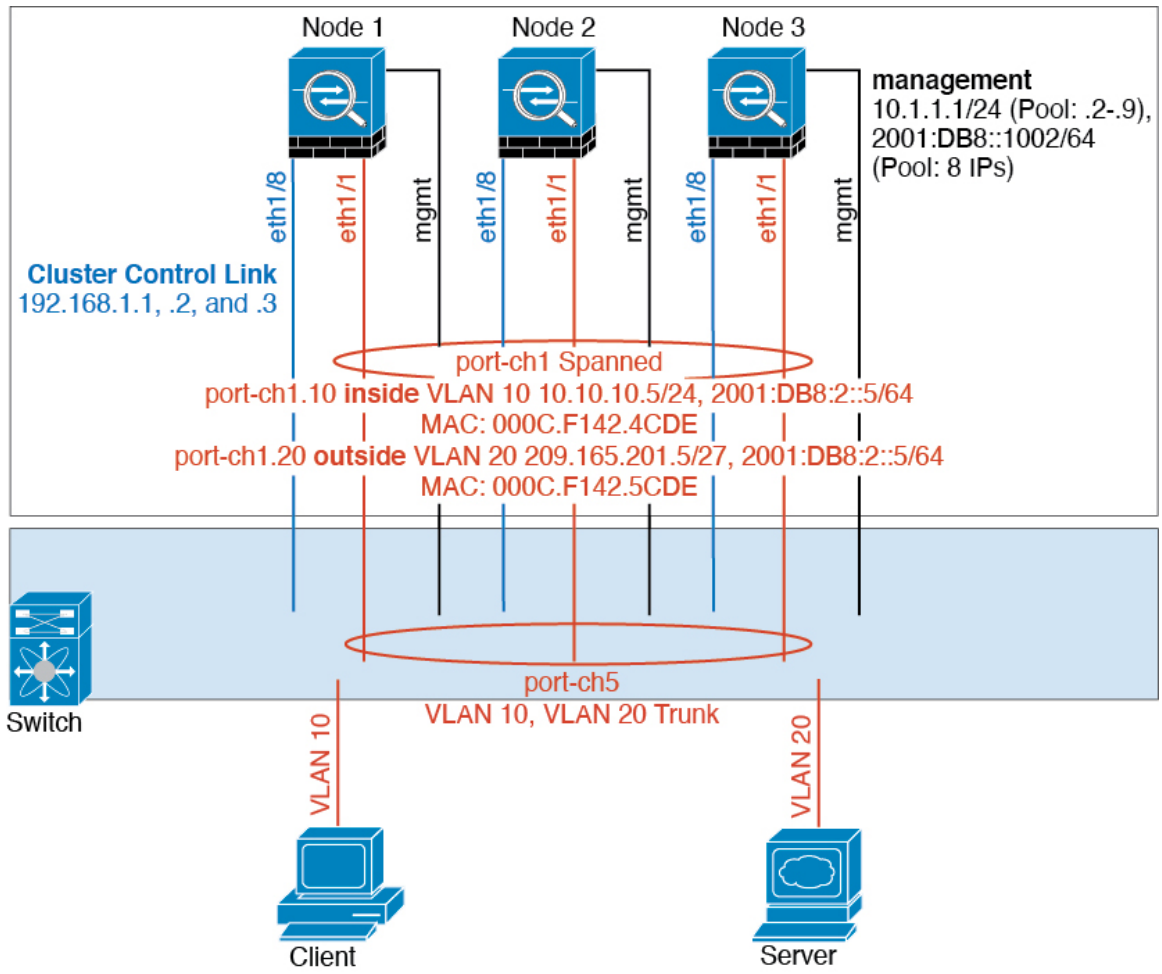
Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage

Unité	Description	Format
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

Exemples de mise en grappe d'

Ces exemples comprennent des déploiements typiques.

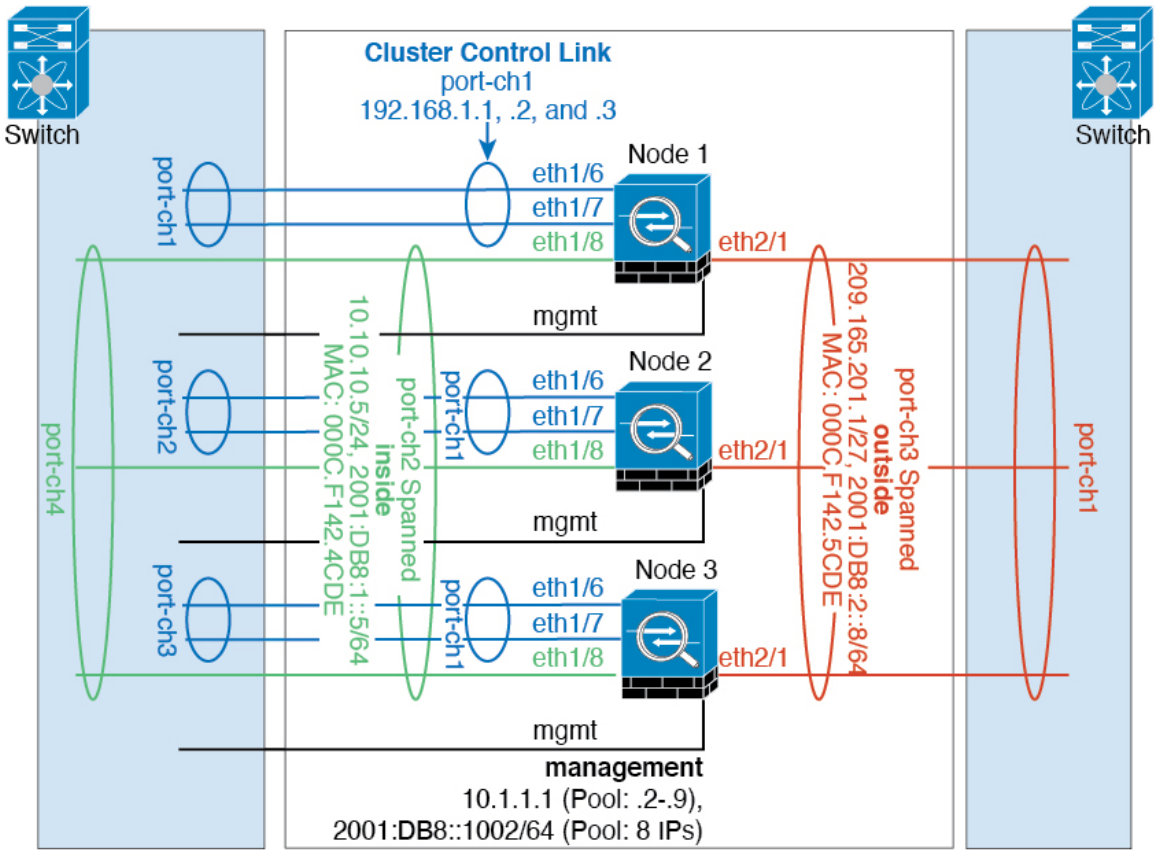
Pare-feu sur clé



Le trafic de données provenant de différents domaines de sécurité est associé à différents VLAN, par exemple, le VLAN 10 pour le réseau interne et le VLAN 20 pour le réseau externe. Chaque dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L' sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l' n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.

Ségrégation du trafic



Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.

Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

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 Défense contre les menaces

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité 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.

Remarque Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig.

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité
- Routage et pont intégrés
- Mode FMC UCAPL/CC

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.

Remarque Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET

- SunRPC
- TFTP
- XDMCP

- Surveillance du routage statique
- VPN de site à site
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

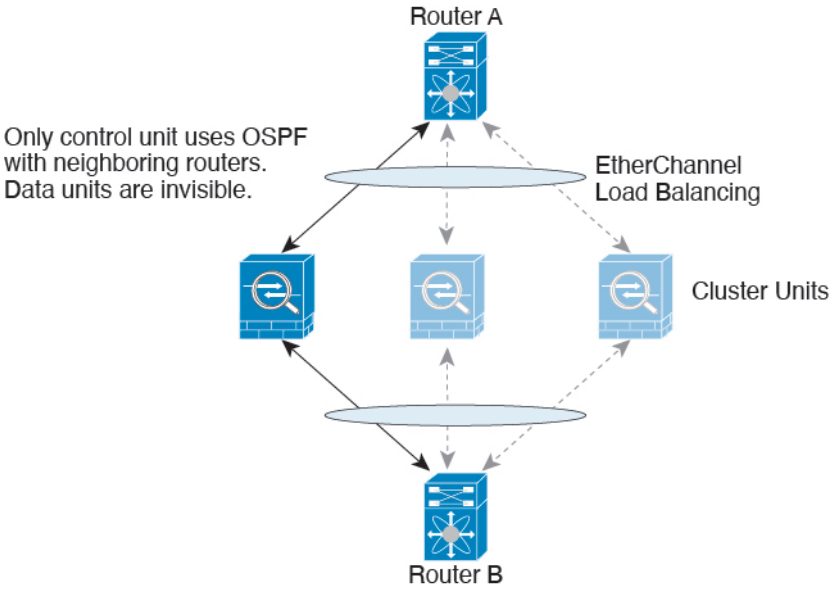
Paramètres de connexion

Les limites de connexion s'appliquent à l'ensemble de la grappe. 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

Le processus de routage ne s'exécute que sur l'unité de contrôle, et les routages sont appris par l'unité de contrôle et répliqués sur les serveurs secondaires. Si un paquet de routage arrive à une unité de données, il est redirigé vers l'unité de contrôle.

Illustration 13 : Routage dynamique



Une fois que les unités de données ont appris les routages de l'unité de contrôle, chaque unité prend les décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée entre l'unité de contrôle et les unités de données. S'il y a un basculement de l'unité de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

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.

Routage multidiffusion et mise en grappe

L'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

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 défense contre les menacesdans 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 défense contre les menaces 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 :

- 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, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau 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, le cluster 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.
- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface 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 (Round robin) : 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.
- Pas de PAT statique pour les inspections suivantes :
    - FTP
    - 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.

Inspection SIP et mise en grappes

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.

SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. 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 supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

Syslog et la mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. 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.

Connexions TLS/SSL et mise en grappe

Les états de déchiffrement des connexions TLS/SSL ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées seront réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.

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; Seule l'unité 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 à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les

utilisateurs de VPN verront une perturbation de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle.

Les clés et les certificats VPN sont répliqués sur toutes les unités.

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.

Par exemple, pour le débit TCP, le périphérique Firepower 9300 avec ses 3 modules SM-40 peut gérer environ 135 Gbit/s du trafic de pare-feu du monde réel lorsqu'il fonctionne seul. Pour le double châssis, le débit maximal combiné sera d'environ 80 % des 270 Gbit/s (2 châssis x 135 Gbit/s) : 216 Gbit/s.

Choix d'unité de contrôle

Les membres de la grappe communiquent sur le lien de commande de grappe pour élire une unité de contrôle comme suit :

1. Lorsque vous déployez la grappe, chaque unité diffuse une demande de sélection toutes les 3 secondes.
2. toute autre unité ayant un niveau de priorité plus élevée répondra à la demande de sélection; la priorité est définie lorsque vous déployez la grappe et n'est pas configurable.
3. Si, après 45 secondes, une unité ne reçoit pas de réponse d'une autre unité de priorité plus élevée, elle devient l'unité de contrôle.

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

4. Si une unité se joint ultérieurement à la grappe avec une priorité plus élevée, elle ne devient pas automatiquement l'unité de contrôle; l'unité de contrôle existante conserve toujours ses fonctions d'unité de contrôle, sauf si elle arrête de répondre, auquel cas une nouvelle unité de contrôle est élue.
5. Dans un scénario de « split-brain » (processeur partagé), où il y a temporairement plusieurs unités de contrôle, l'unité ayant la priorité la plus élevée conserve le rôle tandis que les autres unités retournent aux rôles d'unité de données.

Remarque Vous pouvez forcer manuellement une unité à devenir l'unité de contrôle. Pour les fonctions centralisées, si vous forcez le changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité du châssis, des unités et de l'interface, et en reproduisant les états de connexion entre les unités.

Surveillance des applications du châssis

La surveillance de l'intégrité de l'application du châssis est toujours activée. Le superviseur Châssis Firepower 4100/9300 vérifie l'application défense contre les menaces régulièrement (à chaque seconde). Si l'appareil de défense contre les menaces est opérationnel et ne peut pas communiquer avec le superviseur Châssis Firepower 4100/9300 pendant 3 secondes, l'appareil de défense contre les menaces génère un message syslog et quitte la grappe.

Si le superviseur Châssis Firepower 4100/9300 ne peut pas communiquer avec l'application après 45 secondes, il recharge l'appareil de défense contre les menaces . Si l'appareil de défense contre les menaces ne peut pas communiquer avec le superviseur, il se supprime de la grappe.

Surveillance de l'intégrité de l'unité

Chaque unité envoie périodiquement un paquet de diffusion keepaliveheartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet keepaliveheartbeat ou autre paquet d'un nœud de données au cours de la période 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 choisi parmi le nœud restant.

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. Consultez la Choix d'unité de contrôle, à la page 63 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles utilisées et signale les modifications d'état au nœud de contrôle. Pour la mise en grappe sur plusieurs châssis, les EtherChannels étendus utilisent le protocole cLACP (Link Aggregation Control Protocol). Chaque châssis surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel et informe l'application défense contre les menaces si l'interface est en panne. Lorsque vous activez la surveillance de l'intégrité, les interfaces physiques sont surveillées par défaut (y compris l'interface principale EtherChannel pour les interfaces EtherChannel). Seules les interfaces nommées qui sont dans un état activé peuvent être surveillées. Par exemple, tous les ports membres d'un EtherChannel doivent tomber en panne avant qu'un EtherChannel *nommé* ne soit supprimé de la grappe. Vous pouvez éventuellement désactiver la surveillance par interface.

Si une interface surveillée tombe en panne sur un nœud particulier, mais qu'elle est active sur d'autres nœuds, ce nœud est supprimé de la grappe. Le délai avant la suppression par appareil de défense contre les menaces d'un nœud de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'appareil de défense contre les menaces ne surveille 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

appareil de défense contre les menaces de la grappe. Pour un membre établi, le nœud est supprimé après 500 ms.

Pour la mise en grappe sur plusieurs châssis, si vous ajoutez ou supprimez un EtherChannel de la grappe, la surveillance de l'intégrité de l'interface est suspendue pendant 95 secondes pour que vous ayez le temps d'effectuer les modifications sur chaque châssis.

Surveillance de l'application Decorator

Lorsque vous installez une application décorateur sur une interface, comme l'application Radware DefensePro, appareil de défense contre les menaces et l'application décorateur doivent être opérationnels pour rester dans la grappe. L'unité ne rejoint pas la grappe tant que les deux applications ne sont pas opérationnelles. Une fois dans la grappe, l'unité surveille l'intégrité de l'application du séparateur toutes les 3 secondes. Si l'application décorateur est en panne, l'unité est supprimée de la grappe.

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.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

Rejoindre la grappe

Après le retrait d'un membre 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 : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- 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 le lien de commande de grappe soit actif. L'application défense contre les menaces 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.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.
- Échec de la communication Châssis-Application : lorsque l'application défense contre les menaces détecte que l'intégrité de l'application de châssis a été récupérée, elle essaie de rejoindre la grappe automatiquement.

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 3 : 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	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—

Gestion des connexions par la grappe

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 du 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 .
- 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.

  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.
- Forwarder (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. 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.

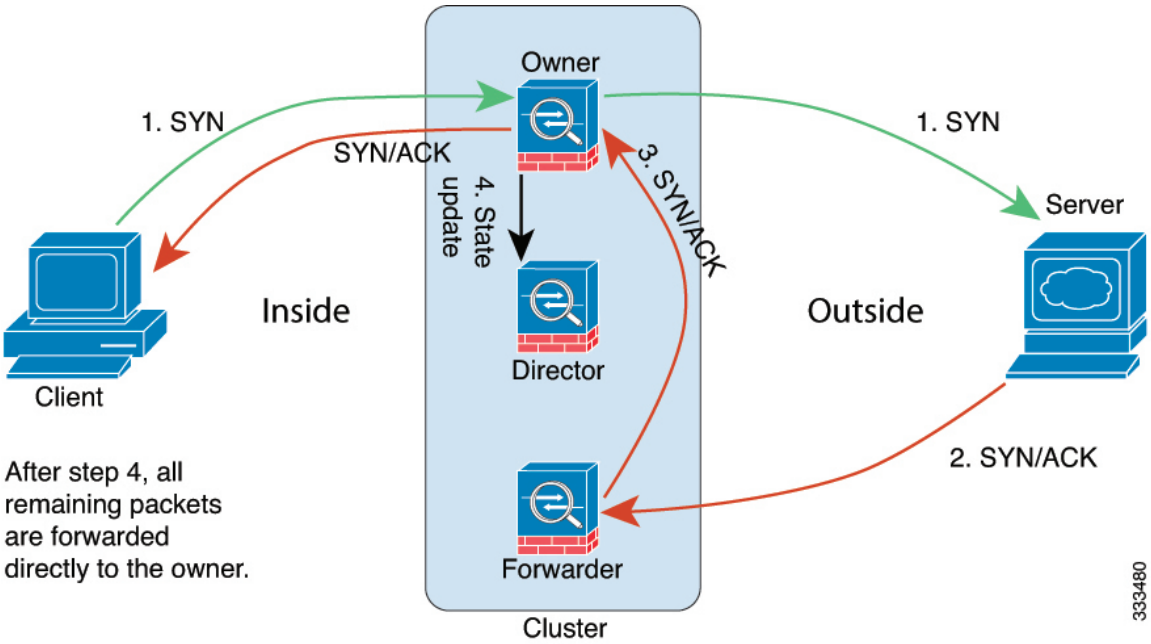
- Propriétaire de fragment : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés 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.

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. 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.

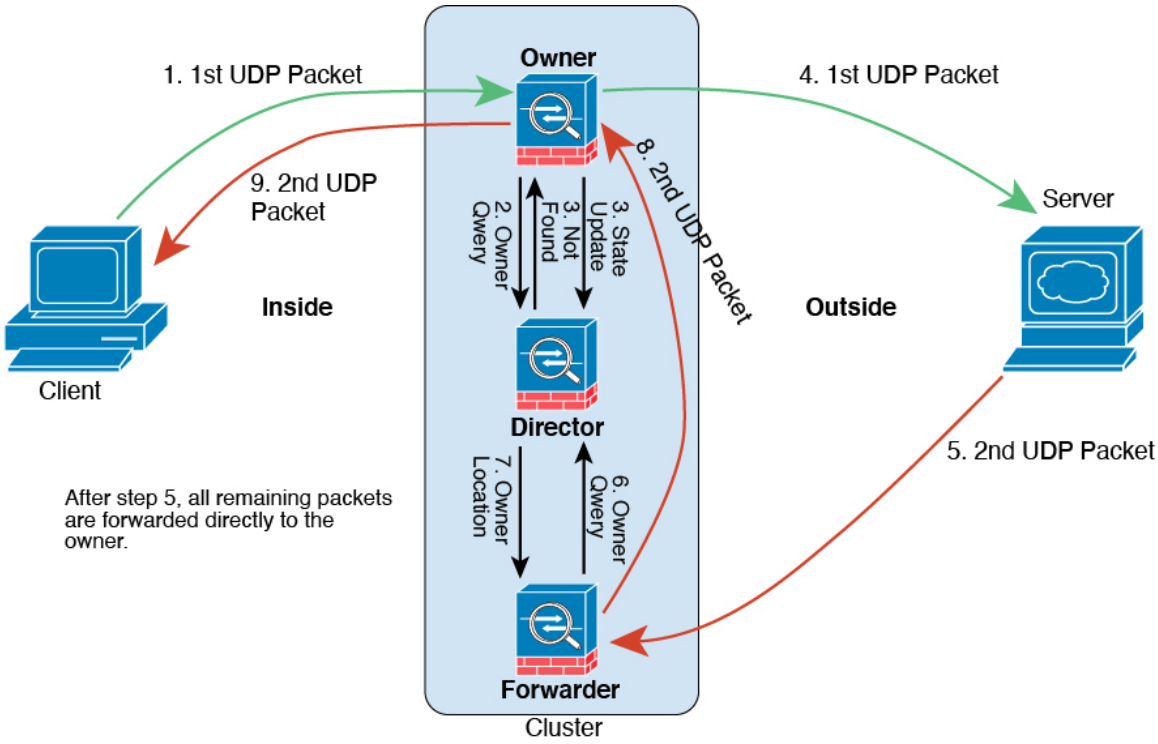


1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces 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 14 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un défense contre les menaces (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.

Historique de la mise en grappe

Tableau 4 :

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)** **Remarque** Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.
Le tableau de bord du moniteur d'intégrité de la grappe.	20221213	N'importe lequel	Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes. Écrans nouveaux ou modifiés : **System** (⚙) > **Moniteur** > **d'intégrité**

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Prise en charge des grappes de 16 nœuds.	20220609	7.2.0	Vous pouvez maintenant configurer des grappes de 16 nœuds pour les modèles Firepower 4100/9300. Auparavant, le maximum était de 6 unités. Nouveaux écrans ou modifiés : aucun. Plateformes prises en charge : Firepower 4100/9300
Le déploiement en grappe des modifications de pare-feu se termine plus rapidement.	20220609	7.2.0	Le déploiement en grappe des modifications de pare-feu se termine désormais plus rapidement. Nouveaux écrans ou modifiés : aucun.
Amélioration de l'attribution des blocs de ports PAT pour la mise en grappe.	20220609	7.0.3	L'allocation améliorée des blocs de ports PAT garantit que l'unité de contrôle conserve des ports en réserve pour les nœuds en cours de jonction et récupère de manière proactive les ports inutilisés. Pour optimiser au mieux l'allocation, vous pouvez définir le nombre maximal de nœuds que vous prévoyez avoir dans la grappe à l'aide de la commande **cluster-member-limit** à l'aide de FlexConfig. L'unité de contrôle peut ensuite allouer des blocs de ports au nombre de nœuds planifié sans avoir à réserver des ports pour des nœuds supplémentaires que vous ne comptez pas utiliser. La valeur par défaut est de 16 nœuds. Vous pouvez également surveiller le journal système 747046 pour vous assurer qu'il y a suffisamment de ports disponibles pour un nouveau nœud. Commandes nouvelles ou modifiées : **cluster-member-limit** (FlexConfig), **show nat pool cluster** [**summary**], **show nat pool ip detail**
Le déploiement en grappe Snort se termine plus rapidement et échoue plus rapidement lorsqu'un événement se produit.	20220609	7.0.3	Le déploiement en grappe des modifications Snort se termine plus rapidement. En outre, lorsqu'une grappe connaît un événement qui fait échouer un déploiement centre de gestion, l'échec se produit plus rapidement. Nouveaux écrans ou modifiés : aucun.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Amélioration de la gestion des grappes.	20220609	7.0.3	Centre de gestion comporte des fonctionnalités de gestion des grappes améliorées que vous ne pouviez auparavant réaliser qu'à l'aide de la CLI, notamment : • Activer et désactiver les unités de la grappe • Afficher l'état de la grappe à partir de la page Device Management (gestion des périphériques), y compris l'historique et le résumé par unité • Changer le rôle de l'unité de contrôle. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques), menu** > **More** (Plus) • **Périphériques** > **Gestion des périphériques** > **Grappe** > **zone Général > Lien État de la grappe en direct État de la grappe** Plateformes prises en charge : Firepower 4100/9300
Mise en grappe multi-instances.	20220609	7.0.3	Vous pouvez maintenant créer une grappe à l'aide d'instances de conteneur. Sur le périphérique Firepower 9300, vous devez inclure une instance de conteneur sur chaque module de la grappe. Vous ne pouvez pas ajouter plusieurs instances de conteneur à la grappe par moteur/module de sécurité. Nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Commandes FXOS nouvelles ou modifiées : **set port-type cluster** Écrans nouveaux ou modifiés de Firepower Chassis Manager : • **Périphériques logiques** > **Ajouter une grappe** • Menu déroulant **Interfaces** > **All Interfaces(Toutes les interfaces)** > **Add New (Ajouter une nouvelle) > champ Subinterface (sous-interface) > Type** Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Synchronisation de la configuration avec les unités de données en parallèle.	20220609	7.0.3	L'unité de contrôle synchronise maintenant les changements de configuration avec les unités de données en parallèle par défaut. Auparavant, la synchronisation se produisait de manière séquence. Nouveaux écrans ou modifiés : aucun.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Messages pour un échec de jonction de grappe ou une éviction ajoutés à **show cluster history**.	20220609	7.0.3	De nouveaux messages ont été ajoutés à la commande **show cluster history** lorsqu'une unité de grappe ne parvient pas à rejoindre la grappe ou la quitter. Commandes nouvelles ou modifiées : **show cluster history** Nouveaux écrans ou modifiés : aucun.
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	20220609	7.0.3	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Commandes nouvelles ou modifiées : **show conn** (sortie uniquement). Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
L'ajout de grappes est plus facile.	20220609	7.0.3	Vous pouvez maintenant ajouter n'importe quelle unité d'une grappe à centre de gestionet les autres unités de la grappe sont détectées automatiquement. Auparavant, vous deviez ajouter chaque unité de grappe en tant que périphérique distinct, puis les regrouper dans une grappe. L'ajout d'une unité de grappe est également désormais automatique. Notez que vous devez supprimer une unité manuellement. Écrans Nouveaux ou modifiés : Boîte de dialogue **Périphériques** > **Gestion des périphériques** menu déroulant **> Ajouter > Périphérique > Ajouter un périphérique** **Périphériques** > **Gestion des périphériques** – onglet **Grappe > zone Général 1 état de l'enregistrement de la grappe > lien Résumé de la grappe actuelle** boîte de dialogue **> Cluster Status** (état de la grappe) Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Prise en charge du VPN de site à site avec mise en grappe comme fonctionnalité centralisée.	20220609	7.0.3	Vous pouvez maintenant configurer le VPN de site à site avec mise en grappe. Le VPN de site à site est une fonctionnalité centralisée; Seule l'unité de contrôle prend en charge les connexions VPN. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Rejoindre automatiquement la grappe après une défaillance interne.	20220609	7.0.3	Auparavant, de nombreuses conditions d'erreur internes entraînaient le retrait d'une unité de la grappe et vous deviez rejoindre manuellement la grappe après avoir résolu le problème. Désormais, une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite. Nouvelle commande ou commande modifiée : **show cluster info auto-join** Aucun écran modifié. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Mise en grappe sur plusieurs châssis pour 6 modules; Prise en charge de Firepower 4100.	20220609	7.0.3	Avec FXOS 2.1.1, vous pouvez désormais activer la mise en grappe sur plusieurs châssis de périphériques Firepower 9300 et 4100. Pour le périphérique Firepower 9300, vous pouvez inclure jusqu'à six modules. Par exemple, vous pouvez utiliser 1 module dans 6 châssis, ou 2 modules dans 3 châssis, ou toute combinaison fournissant un maximum de 6 modules. Pour le périphérique Firepower 4100, vous pouvez inclure jusqu'à 6 châssis. **Remarque** La mise en grappe inter-sites est également prise en charge. Toutefois, les personnalisations visant à améliorer la redondance et la stabilité, comme les adresses IP et MAC spécifiques au site, la localisation des directeurs, la redondance du site et la mobilité du flux de grappes, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig. Aucun écran modifié. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Mise en grappe sur plusieurs modules avec un châssis Firepower 9300.	20220609	7.0.3	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Écrans Nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Ajouter** > **Ajouter une grappe** **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : défense contre les menaces sur le périphérique Firepower 9300

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.