Déployer une grappe pour Firewall Threat Defense sur le Cisco Secure Firewall 3100/4200

Dernière modification : 2026-05-25

Déployer une grappe pour Firewall Threat Defense sur le Cisco Secure Firewall 3100/4200

La mise en grappe vous permet de regrouper plusieurs nœuds Firewall Threat Defense 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 54.

À propos de la mise en grappe pour Cisco Secure Firewall 3100/4200

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

Intégration de la grappe dans votre réseau

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

- Réseau de fond de panier isolé à grande vitesse pour la communication intragrappe connu sous le nom de *liaison de commande de grappe*.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance.

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

- EtherChannel étendu (recommandé) : Les interfaces sur plusieurs membres de la grappe sont regroupées dans un seul EtherChannel; l'EtherChannel effectue l'équilibrage de la charge entre les unités.
- Routage basé sur les politiques (mode pare-feu routé uniquement) : Les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les unités à l'aide de cartes de routage et de listes de contrôle d'accès.
- Routage à chemins multiples à coût égal (mode pare-feu routé uniquement) : Les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les unités à l'aide de routages statiques ou dynamiques à coût égal.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité. La priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. Lorsque vous créez la grappe pour la première fois, vous spécifiez le nœud que vous souhaitez utiliser comme nœud de contrôle. Il deviendra le nœud de contrôle simplement parce qu'il s'agit du premier nœud ajouté à la grappe.

Tous les nœuds de la grappe partagent la même configuration. Le nœud que vous avez initialement spécifié comme nœud de contrôle remplacera la configuration sur les nœuds de données lorsqu'ils rejoindront la grappe. Vous n'avez donc qu'à effectuer la configuration initiale sur le nœud de contrôle avant de former la grappe.

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

Interfaces de la grappe

Vous pouvez configurer des interfaces de données soit ou en tant qu'interfaces individuelles . Toutes les interfaces de données de la grappe doivent être d'un seul type. Consultez À propos des interfaces de grappe, à la page 8 pour de plus amples renseignements.

Pour les EtherChannels étendus : vous pouvez utiliser des interfaces de pare-feu standard ou des interfaces IPS uniquement (ensembles en ligne ou interfaces passives). Pour les interfaces individuelles : les interfaces IPS uniquement ne sont pas prises en charge.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Consultez Liaison de commande de grappe, à la page 8 pour de plus amples renseignements.

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.

Le réseau de gestion

Vous devez gérer chaque nœud à l'aide de l'interface de gestion; la gestion à partir d'une interface de données n'est pas prise en charge avec la mise en 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 le nœud de contrôle au On-Prem Firewall Management Center, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Avant de créer la grappe, les licences attribuées aux nœuds de données importent peu; les paramètres de licence du nœud de contrôle sont répliqués sur chacun des nœuds de données. Vous pouvez modifier les licences pour la grappe en cliquant sur **Edit**

(Modifier). Licenses (Modifier les licences) dans **Système** (⚙) > **Licenses (Licences)** > **Smart Licenses (Licences Smart)** ou en choisissant **Devices (appareils)** > **Device Management (gestion des appareils)**, en cliquant sur **Modifier** (✎) pour la grappe, puis dans la zone **Licence**, en cliquant sur **Modifier** (✎).

Remarque Si vous ajoutez la grappe avant que le On-Prem Firewall Management Center ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le On-Prem Firewall Management Center, 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 grappes

Exigences du modèle

- Secure Firewall 3100 : maximum 16 nœuds
- Secure Firewall 4200 : maximum 16 nœuds

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration matérielle et logicielle requise

Pour toutes les unités d'une grappe :

- Il doit s'agir du même modèle.
- Doit inclure les mêmes interfaces.
- L'accès au On-Prem Firewall Management Center doit provenir de l'interface de gestion; la gestion de l'interface de données n'est pas prise en charge.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge.
- Doit utiliser le même mode de pare-feu (routage ou transparent).
- Doit appartenir au même domaine.
- Doit appartenir au même groupe.
- Ne doit avoir aucun déploiement en attente ou en cours.
- Le nœud de contrôle ne doit avoir aucune fonctionnalité non prise en charge configurée (voir Fonctionnalités non prises en charge par la mise en grappe, à la page 54).

- Aucun VPN ne doit être configuré sur les nœuds de données. Le nœud de contrôle peut être doté d'un VPN de site à site.

Exigences du commutateur

- Assurez-vous d'achever la configuration du commutateur avant de configurer la mise en grappe. Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. Par défaut, la MTU de la liaison de commande de grappe est supérieure de 100 octets aux interfaces de données. Si les commutateurs ont une incompatibilité MTU, la formation de la grappe échouera.

Lignes directrices de la mise en grappe

Mode pare-feu

Le mode de pare-feu doit correspondre sur toutes les unités.

Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

IPv6

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

Commutateurs

- 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. De plus, nous ne conseillons pas de définir la MTU de la liaison de commande de grappe entre 2 561 et 8 362. En raison de la gestion du groupe de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système. Lorsqu'un nœud rejoint la grappe, il vérifie la compatibilité MTU en envoyant un ping au nœud de contrôle avec une taille de paquet correspondant au MTU de la liaison de contrôle de grappe. Si le ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs connectés et réessayer.
- 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 conseillons d'utiliser l'un des algorithmes d'équilibrage de charges EtherChannel suivants : **source-dest-ip** or **src-dst-mixed-ip-port** (reportez-vous à la commande **port-channel load-balance** de Cisco Nexus OS et Cisco IOS-XE). 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 :

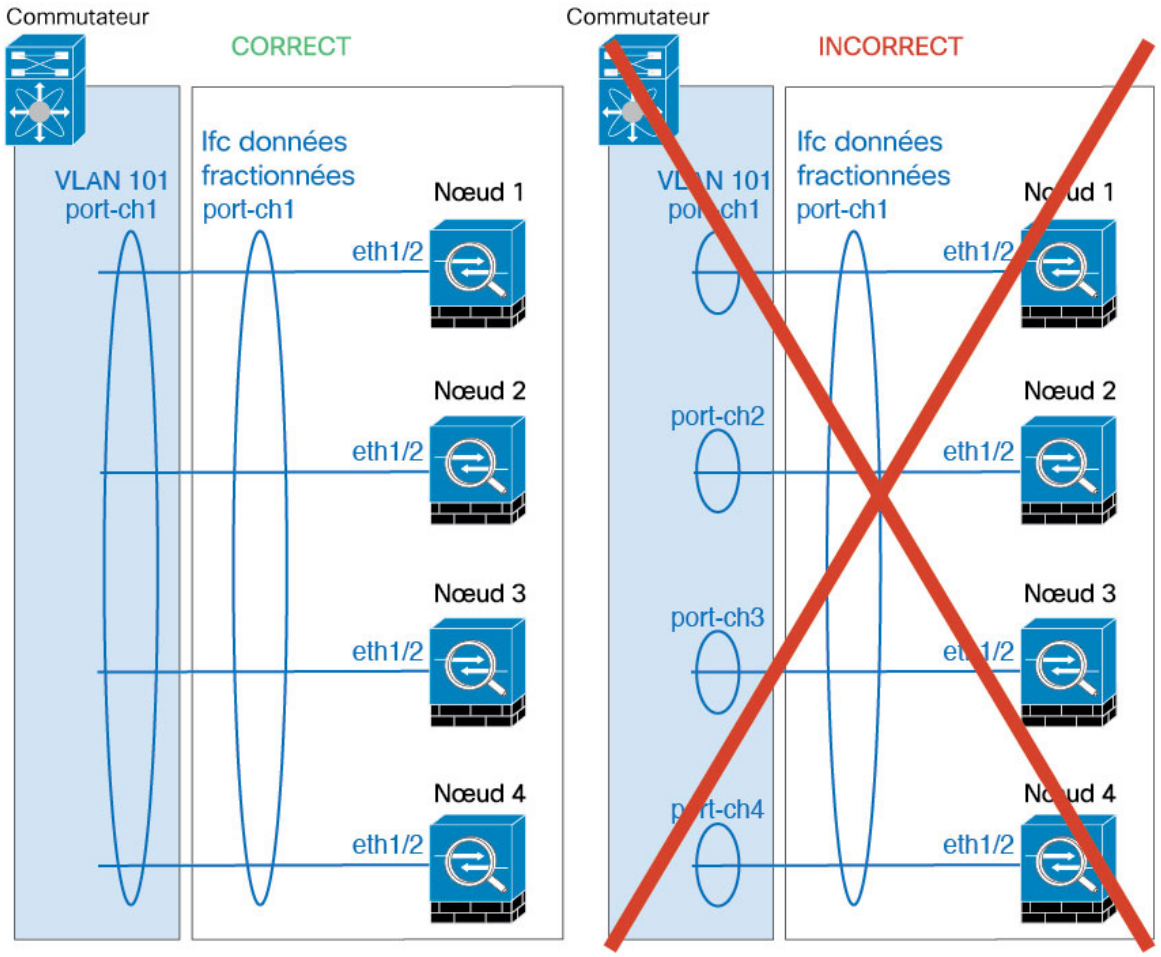
  router(config)# **port-channel** *id* **hash-distribution fixed**

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

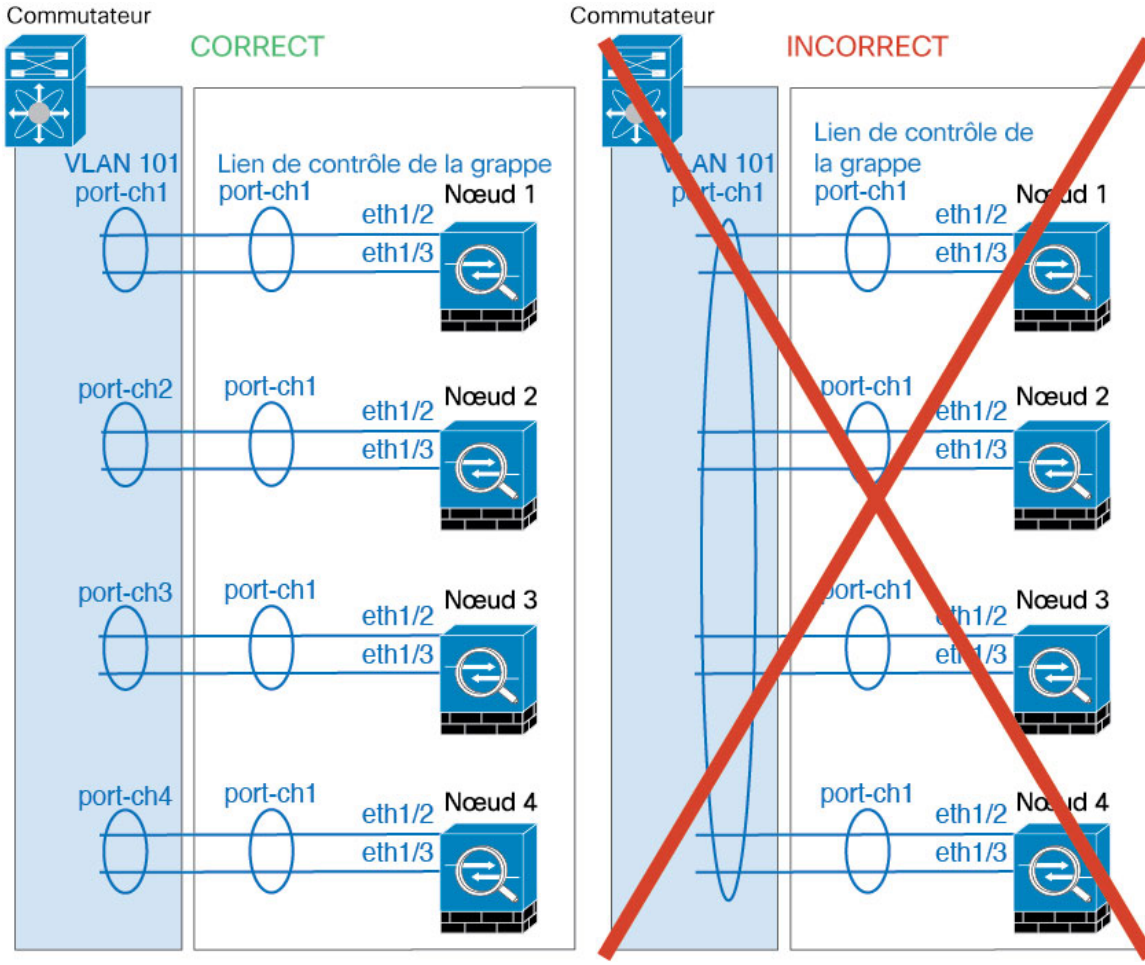
- Vous devez désactiver la fonctionnalité de convergence progressive LACP sur toutes les interfaces EtherChannel face à la grappe pour les commutateurs Cisco Nexus.

EtherChannels

- 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 Firewall Threat Defense ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- 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 bloquer votre connexion ; par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à un EtherChannel étendu, lorsque le port du serveur syslog est en panne et que le serveur ne gère pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe ASA. Ces messages peuvent faire en sorte que certaines unités de la grappe ASA connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.

- 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 pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 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 en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe

Pour ajouter une grappe au On-Prem Firewall Management Center, ajoutez chaque nœud au On-Prem Firewall Management Center en tant qu'unité autonome, configurez les interfaces sur l'unité que vous souhaitez utiliser comme nœud de contrôle, puis formez la grappe.

À propos des interfaces de grappe

Vous pouvez configurer des interfaces de données en tant que canaux EtherChannels étendus ou en tant qu'interfaces individuelles. Toutes les interfaces de données de la grappe doivent être à un seul type. Vous ne pouvez pas configurer Ethernet 1/1 comme EtherChannel étendu et configurer Ethernet 1/2 comme interface individuelle dans la même grappe, par exemple.

Pour les EtherChannels étendus : vous pouvez utiliser des interfaces de pare-feu standard ou des interfaces IPS uniquement (ensembles en ligne ou interfaces passives). Pour les interfaces individuelles : les interfaces IPS uniquement ne sont pas prises en charge.

Chaque unité doit également dédier au moins une interface matérielle comme liaison de commande de grappe.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Nous vous recommandons d'utiliser un EtherChannel pour le lien de commande de grappe, si disponible.

Présentation du trafic de liaison de commande de grappe

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

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.

- Surveillance de l'intégrité

Le trafic de données comprend :

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

Interfaces et réseau de la liaison de commande de grappe

Vous pouvez utiliser n’importe quelle interface physique ou EtherChannel pour la liaison de commande de grappe. Vous ne pouvez pas utiliser une sous-interface VLAN comme liaison de commande de grappe. Vous ne pouvez pas non plus utiliser l'interface.

Chaque liaison de commande de grappe possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Remarque Pour une grappe de deux membres, ne connectez pas directement la liaison de commande de grappe d’un nœud 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. Si vous devez connecter directement les unités (à des fins de test, par exemple), vous devez configurer et activer l’interface de liaison de commande de grappe sur les deux nœuds avant de former la grappe.

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.

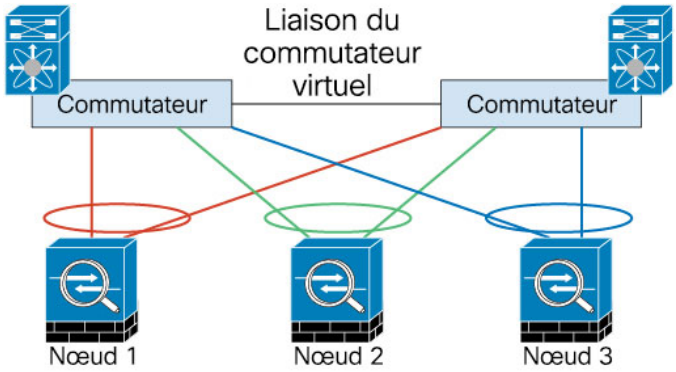
Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d’étranglement.

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 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.

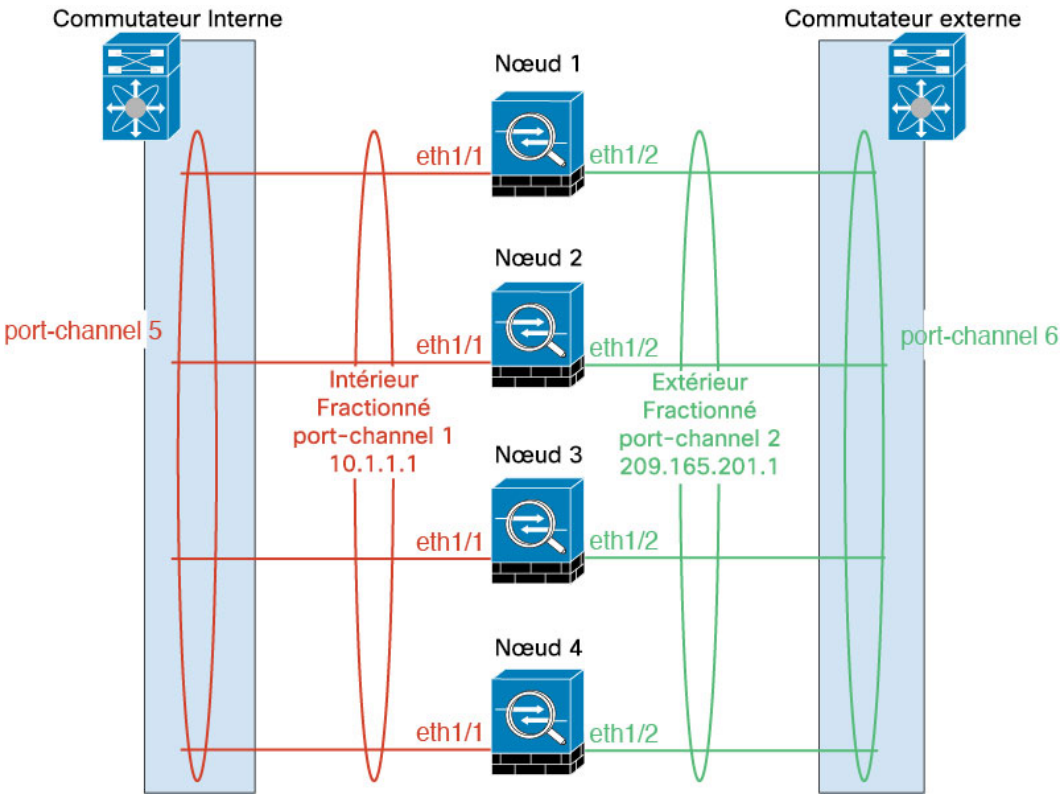
La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

EtherChannels étendus (recommandé)

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.

For regular firewall interfaces : Un EtherChannel étendu peut être configuré dans les modes de pare-feu avec routage 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.



Avantages de l'EtherChannel étendu

La méthode d'équilibrage de la charge EtherChannel est recommandée par rapport aux autres méthodes en raison des avantages suivants :

- Une détection plus rapide des défaillances.
- Un temps de convergence plus rapide. Les interfaces individuelles dépendent des protocoles de routage pour équilibrer la charge du trafic, et les protocoles de routage ont souvent une convergence lente lors d'une défaillance de liaison.
- Facile à configurer

Lignes directrices pour le débit maximal

Pour atteindre un débit maximal, nous vous recommandons ce qui suit :

- Utilisez un algorithme de hachage pour l'équilibrage de la charge qui est « symétrique », ce qui signifie que les paquets des deux directions auront le même hachage et seront envoyés au même Firewall Threat Defense dans l'EtherChannel étendu. Nous vous recommandons d'utiliser l'adresse IP source et de destination (par défaut) ou les ports source et destination comme algorithme de hachage.
- Utilisez le même type de cartes de ligne lors de la connexion des Firewall Threat Defenseau commutateur afin que les algorithmes de hachage appliqués à tous les paquets soient les mêmes.

Équilibrage de la charge

Le lien EtherChannel est sélectionné à l'aide d'un algorithme de hachage propriétaire, en fonction des adresses IP source ou de destination et des numéros de ports TCP et UDP.

Remarque Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes suivants : **source-dest-ip** ou **source-dest-ip-port** (consultez la commande **d'équilibrage de la charge du canal de port** du système d'exploitation Cisco Nexus ou Cisco IOS). N'utilisez pas le mot clé **vlan** dans l'algorithme d'équilibrage de charges, car cela pourrait entraîner une répartition inégale du trafic vers les nœuds d'une grappe.

Le nombre de liaisons dans l'EtherChannel affecte l'équilibrage de la charge.

L'équilibrage de charge symétrique n'est pas toujours possible. Si vous configurez la NAT, les paquets de transfert et de retour auront des adresses IP et/ou des ports différents. Le trafic de retour sera envoyé vers une autre unité en fonction du hachage, et la grappe devra rediriger la majeure partie du trafic de retour vers la bonne unité.

Redondance EtherChannel

L'EtherChannel a une redondance intégrée. Il surveille l'état du protocole de ligne de toutes les liaisons. Si une liaison échoue, le trafic est rééquilibré entre les liaisons restantes. Si tous les liens de l'EtherChannel échouent sur une unité particulière, mais que d'autres unités sont toujours actives, cette unité est supprimée de la grappe.

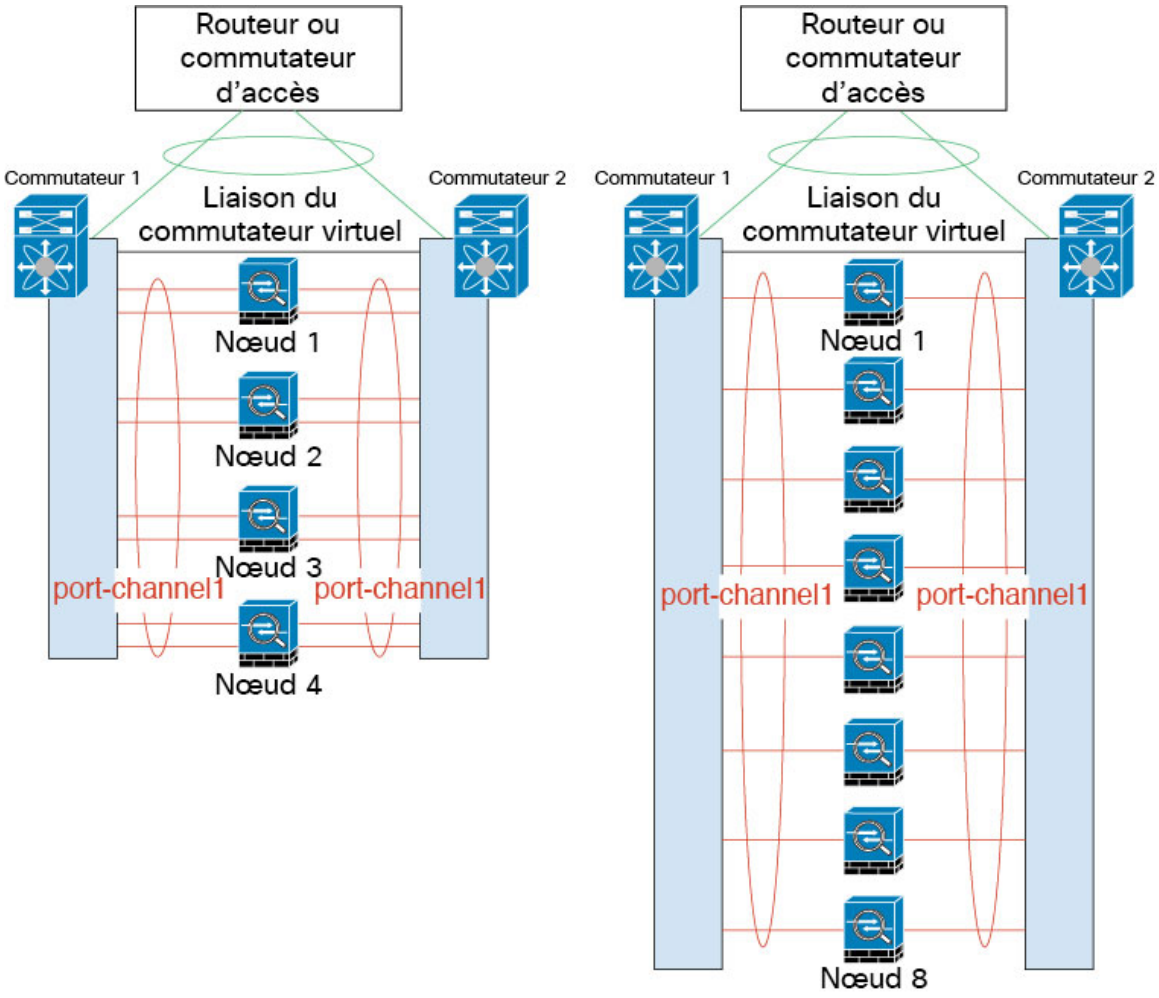
Connexion à un système de commutateurs redondants

Vous pouvez inclure plusieurs interfaces pour chaque Firewall Threat Defense dans l'EtherChannel étendu. Plusieurs interfaces par Firewall Threat Defense sont particulièrement utiles pour la connexion aux deux commutateurs dans un système VSS, vPC, StackWise ou StackWise Virtual.

Selon vos commutateurs, vous pouvez configurer jusqu'à 32 liens actifs dans l'EtherChannel étendu. Cette fonctionnalité nécessite que les deux commutateurs du vPC prennent en charge les canaux EtherChannels avec 16 liens actifs chacun (par exemple, le module Cisco Nexus 7000 avec le module Ethernet de 10 Gigabit de la gamme F2).

Pour les commutateurs qui prennent en charge 8 liens actifs dans l'EtherChannel, vous pouvez configurer jusqu'à 16 liens actifs dans l'EtherChannel étendu lors de la connexion à deux commutateurs dans un système redondant.

La figure suivante montre un EtherChannel de 16 liens actifs dans une grappe de 4 nœuds et une grappe de 8 nœuds.



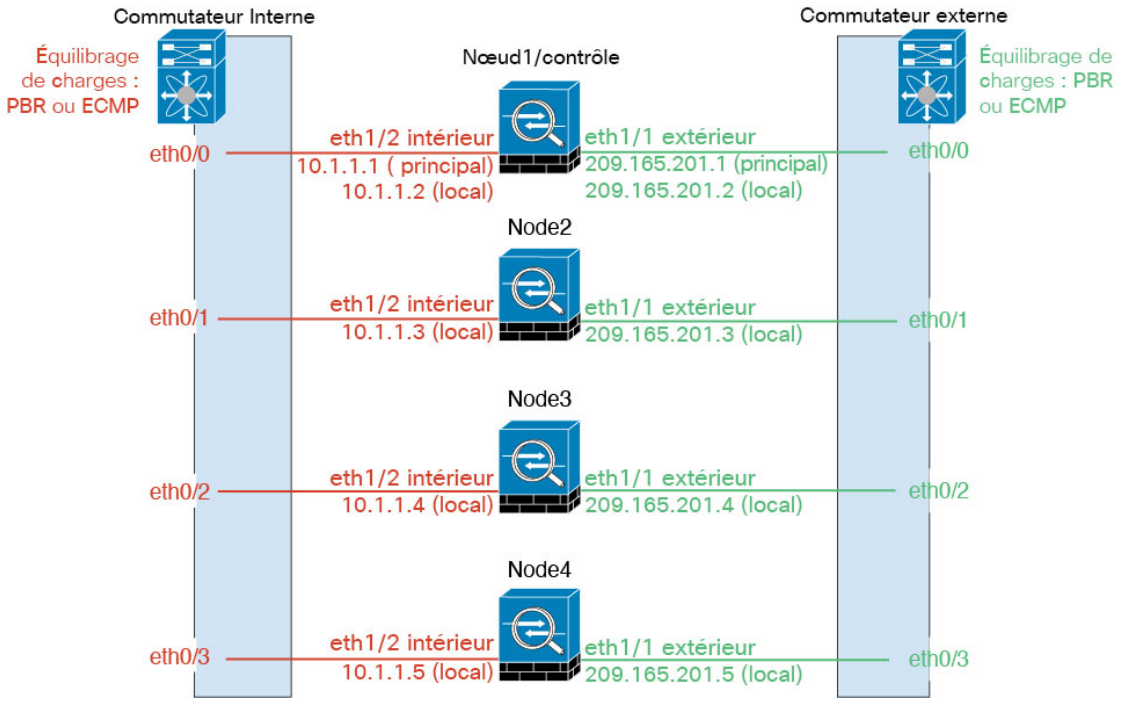
Interfaces individuelles (mode pare-feu routé uniquement)

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

Les interfaces IPS uniquement (ensembles en ligne et interfaces passives) ne sont pas prises en charge en tant qu'interfaces individuelles.

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

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



Routage basé sur les politiques

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

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

PBR prend des décisions de routage en fonction d'une carte de routage et d'une ACL. Vous devez répartir manuellement le trafic entre toutes les Firewall Threat Defense d'une grappe. Comme PBR est statique, il se peut qu'il ne permette pas d'atteindre un résultat d'équilibrage de la charge optimale à tout moment. Pour obtenir les meilleures performances, nous vous recommandons de configurer la politique PBR de sorte que les paquets d'acheminement et de retour d'une connexion soient dirigés vers la même Firewall Threat Defense. Par exemple, si vous avez un routeur Cisco, la redondance peut être obtenue en utilisant Cisco IOS PBR avec Object Tracking. Le suivi d'objets Cisco IOS surveille chaque Firewall Threat Defense à l'aide d'un ping ICMP. PBR peut ensuite activer ou désactiver les cartes de routage en fonction de l'accessibilité d'un Firewall Threat Defense. Consultez les URL suivantes pour en savoir plus :

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

Routage à chemins multiples à coût égal

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

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

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de Firewall Threat Defense peut provoquer des problèmes. Le routage continue d'être utilisé et le trafic vers le Firewall Threat Defense défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque Firewall Threat Defense pour qu'il participe au routage dynamique.

Cisco Intelligent Traffic Director (mode pare-feu routé seulement)

Lorsque vous utilisez des interfaces individuelles, chaque interface Firewall Threat Defense conserve ses propres adresses IP et MAC. Intelligent Traffic Director (ITD) est une solution d'équilibrage de la charge matérielle haut débit pour les commutateurs Nexus 5000, 6000, 7000 et 9000. En plus de couvrir entièrement les capacités fonctionnelles du PBR traditionnel, il offre un flux de travail de configuration simplifié et plusieurs fonctionnalités supplémentaires pour une répartition de la charge plus fine.

L'ITD prend en charge la permanence des adresses IP, le hachage cohérent pour la symétrie des flux bidirectionnels, les adresses IP virtuelles, la surveillance de l'intégrité, les politiques sophistiquées de gestion des défaillances avec redondance N+M, l'équilibrage de la charge pondérée et les sondes d'ANS d'applications IP, y compris le DNS. En raison de la nature dynamique de l'équilibrage de la charge, il permet une répartition du trafic plus uniforme sur tous les nœuds de la grappe par rapport à PBR. Afin de parvenir à une symétrie de flux bidirectionnelle, nous vous recommandons de configurer l'ITD de manière à ce que les paquets d'aller et de retour d'une connexion soient dirigés vers la même Firewall Threat Defense. Consultez l'URL suivante pour en savoir plus :

https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd_deployment/ITD_ASA_Deployment_Guide.pdf

Câbler et ajouter des périphériques au On-Prem Firewall Management Center

Avant de configurer la mise en grappe, vous devez préparer vos périphériques. En particulier, la grappe ne sera pas créée si tous les nœuds ne peuvent pas communiquer sur la liaison de commande de grappe. Par conséquent, avant de former la grappe, la liaison de commande de grappe doit être prête à fonctionner.

Procédure

Étape 1 Câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Étape 2 Configurez les équipements en amont et en aval.

a) Pour le réseau de liaison de commande de grappe, définissez la MTU pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données.

Par défaut, la MTU de l'interface de données est de 1500 octets, donc la MTU de la liaison de commande de grappe sur le nœud de la grappe sera fixée à 1600 octets. Si vous utilisez des MTU plus élevées sur vos interfaces de données, augmentez en conséquence la MTU de la liaison de commande de grappe sur les commutateurs de connexion.

b) Configurez les interfaces de liaison de commande de grappe sur l'équipement en amont et en aval, y compris pour un EtherChannel facultatif.

Consultez Interfaces et réseau de la liaison de commande de grappe, à la page 9 pour connaître les exigences de liaison de commande de grappe.

c) Configurez les interfaces de données sur les équipements en amont et en aval, y compris les EtherChannels étendus, si vous choisissez ce mode d'interface de grappe.

Consultez À propos des interfaces de grappe, à la page 8 pour obtenir des renseignements sur le câblage des EtherChannels étendus.

Étape 3 Ajoutez chaque nœud à On-Prem Firewall Management Center en tant que périphérique autonome dans le même domaine et groupe.

Vous pouvez créer une grappe avec un seul périphérique, puis ajouter d'autres nœuds ultérieurement. Les paramètres initiaux (licence, politique de contrôle d'accès) que vous définissez lorsque vous ajoutez un périphérique seront hérités par tous les nœuds de la grappe à partir du nœud de contrôle. Vous choisirez le nœud de contrôle lors de la formation de la grappe.

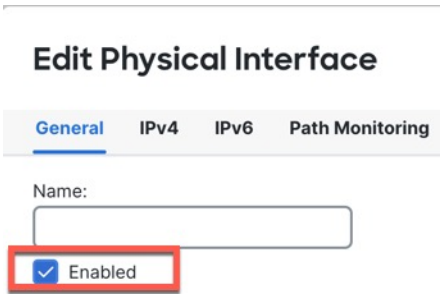
Étape 4 Activez la liaison de commande de grappe sur l'appareil que vous souhaitez utiliser comme nœud de contrôle.

Lorsque vous ajoutez les autres nœuds, ils héritent de la configuration de la liaison de commande de grappe.

Remarque
Ne configurez *pas* le nom ou l'adressage IP pour la liaison de commande de grappe. La MTU de l'interface de liaison de commande de grappe est automatiquement définie à 100 octets de plus que la MTU d'interface de données la plus élevée lorsque vous créez la grappe. Vous n'avez donc pas besoin de la définir maintenant. Cependant, nous ne recommandons pas de régler la MTU du lien de contrôle de la grappe entre 2561 et 8362. En raison de la gestion des groupes de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système. Si la MTU est réglée dans cette plage lorsque vous ajoutez la grappe, nous vous recommandons de revenir à la page **Interfaces** et de l'augmenter manuellement au-delà de 8362. Lorsqu'un nœud rejoint la grappe, il vérifie la compatibilité MTU en envoyant un ping au nœud de contrôle avec une taille de paquet correspondant au MTU de la liaison de contrôle de grappe. Si le ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs connectés et réessayer.

a) Sur le périphérique que vous souhaitez désigner comme nœud de contrôle, choisissez Devices (Périphériques) > Device Management (Gestion des périphériques), puis cliquez sur**Devices (appareils) > Device Management (gestion des appareils)**.**Modifier** (✎)
b) Cliquez sur **Interfaces**.
c) Activez l'interface. Si vous souhaitez utiliser un EtherChannel pour la liaison de commande de grappe, activez tous les membres.

Illustration 1 : Activer l'interface de liaison de commande de grappe



d) (Facultatif) Ajoutez un canal EtherChannel.

Nous vous recommandons d'utiliser le mode activé pour les interfaces membres de la liaison de commande de grappe afin de réduire le trafic inutile sur la liaison de commande de grappe (le mode actif est l'option par défaut). La liaison de commande de grappe n'a pas besoin du surdébit du trafic LACP, car il s'agit d'un réseau isolé et stable. **Remarque :** nous vous recommandons de régler les EtherChannels de *données* en mode actif.

e) Cliquez sur **Save** (Enregistrer), puis sur **Deploy** (déployer) pour déployer les modifications d'interface sur le nœud de contrôle.

Créer une grappe

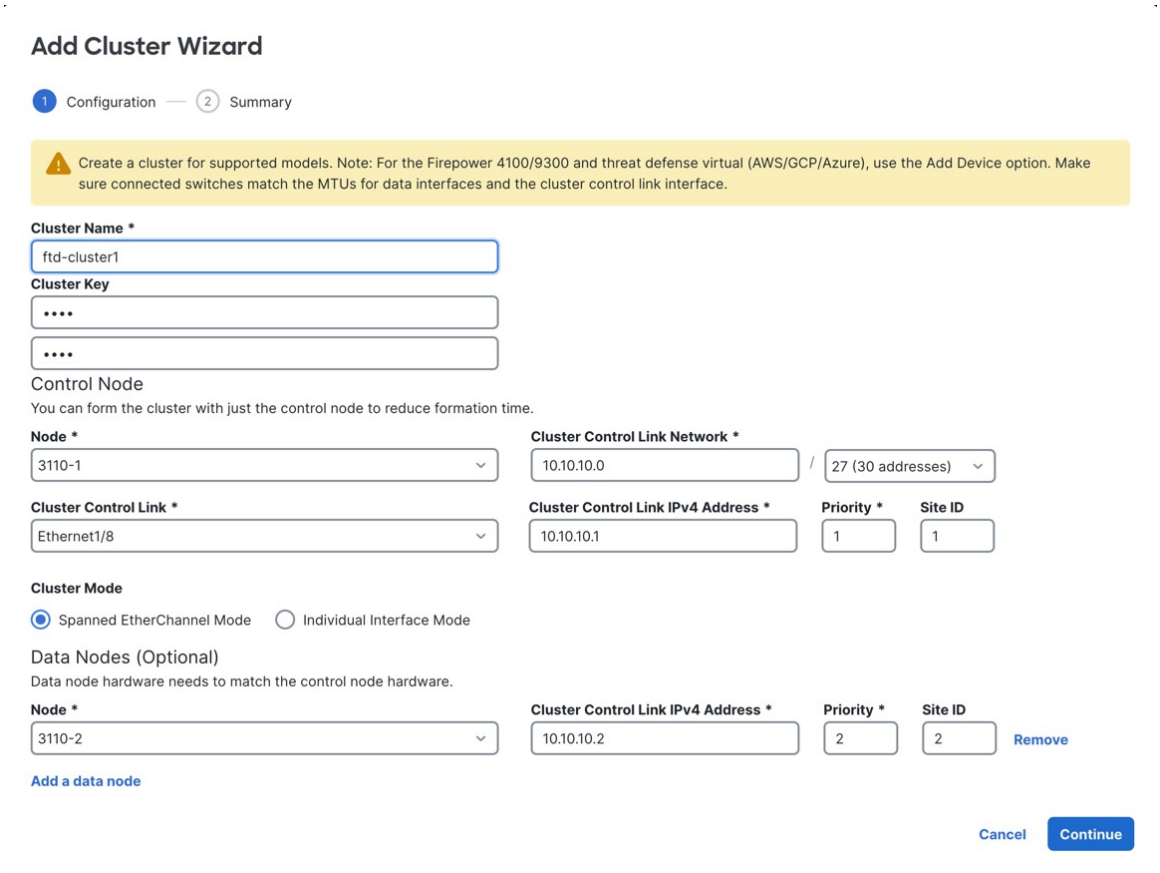
Créer une grappe à partir d'un ou de plusieurs périphériques dans On-Prem Firewall Management Center.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, puis sélectionnez **Add (Ajouter)** > **Cluster (Grappe)**.

L'**assistant d'ajout de grappe** apparaît.

Illustration 2 : Ajout de Cluster Wizard (Assistant Grappe)



Étape 2 Spécifiez un **nom de grappe** et une **clé de grappe** d'authentification pour le trafic de contrôle.

- **Nom de la grappe** : chaîne ASCII de 1 à 38 caractères.
- **Clé de la grappe** : chaîne ASCII de 1 à 38 caractères. La valeur de la **clé de la grappe** est utilisée pour générer la clé de chiffrement. Ce chiffrement 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.

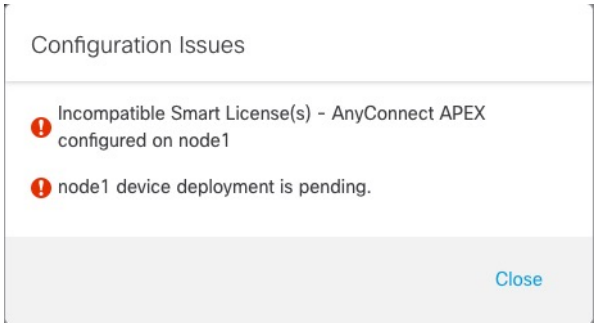
Étape 3 Pour le **nœud de contrôle**, définissez les paramètres suivants :

- **Nœud** : choisissez le périphérique que vous souhaitez utiliser comme nœud de contrôle initialement. Lorsque le On-Prem Firewall Management Center forme la grappe, il ajoute d'abord ce nœud à cette dernière pour qu'il devienne le nœud de contrôle.

  Remarque

  Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes. Par exemple :

  Illustration 3 : Problèmes de configuration

  Pour résoudre les problèmes ci-dessus, supprimez la licence VPN non prise en charge et déployez les modifications de configuration en attente sur le périphérique.

- Réseau de liaisons **de contrôle de grappe** : Précisez un sous-réseau IPv4; IPv6 n'est pas pris en charge pour cette interface. Précisez un sous-réseau **24**, **25**, **26** ou **27**.
- **Cluster Control Link (liaison de commande de grappe)** : Choisissez l'interface physique ou l'EtherChannel que vous souhaitez utiliser pour la liaison de commande de grappe.

  Remarque
  La MTU de l'interface de liaison de commande de grappe est automatiquement réglée à 100 octets de plus que la MTU de l'interface de données la plus élevée; par défaut, la MTU est de 1600 octets. Nous ne recommandons pas de définir la MTU de la liaison de commande de grappe entre 2561 et 8362. En raison de la gestion du groupe de blocs, cette taille MTU n'est pas optimale pour le fonctionnement du système. Si la MTU est réglée dans cette plage lorsque vous ajoutez la grappe, nous recommandons d'augmenter la MTU au-delà de 8362 sur le **Devices (appareils)** > **Device Management (gestion des appareils)**, puis de cliquer sur la page **Interfaces**.

  Assurez-vous de configurer les commutateurs connectés à la liaison de commande de grappe sur la MTU (supérieure) appropriée; sinon, la formation de la grappe échouera. Lorsqu'un nœud rejoint la grappe, il vérifie la compatibilité MTU en envoyant un ping au nœud de contrôle avec une taille de paquet correspondant au MTU de la liaison de contrôle de grappe. Si le ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs connectés et réessayer.

- **Cluster Control Link IPv4 Address** (adresse IPv4 de la liaison de commande de grappe) : ce champ sera rempli automatiquement avec la première adresse du réseau de liaison de commande de grappe. Vous pouvez modifier l'adresse hôte si vous le souhaitez.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée. Même si vous définissez la priorité sur une valeur inférieure à celle des autres nœuds, ce nœud sera toujours le nœud de contrôle lors de la formation de la grappe.
- **Site ID** (ID de site) : (fonctionnalité FlexConfig) Saisissez l'ID de site pour ce nœud entre 1 et 8. La valeur 0 désactive la mise en grappe intersites. Les personnalisations supplémentaires de grappe intersites afin d'améliorer la redondance et la stabilité, comme la localisation des directeurs, la redondance de sites et la mobilité du flux de grappe, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig.

Étape 4 Pour le **mode de grappe**, choisissez **Mode EtherChannel étendu** ou le mode **d'interface individuelle**.

Étape 5 Pour **les nœuds de données (facultatif)**, cliquez sur **Add a data node** (Ajouter un nœud de données) pour ajouter un nœud à la grappe.

Vous pouvez former la grappe uniquement avec le nœud de contrôle pour accélérer la formation de cette dernière, ou vous pouvez ajouter tous les nœuds maintenant. Définissez les éléments suivants pour chaque nœud de données :

- **Nœud** : choisissez le périphérique que vous souhaitez ajouter.

  Remarque

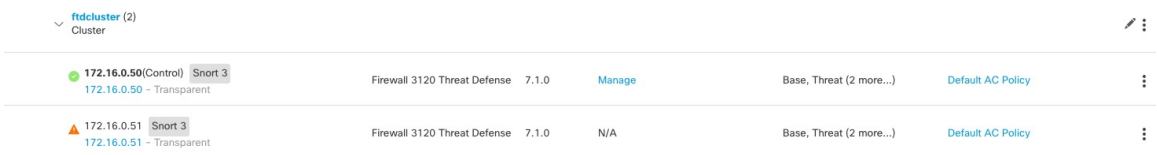
  Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes.

- **Cluster Control Link IPv4 Address** (adresse IPv4 de la liaison de commande de grappe) : ce champ sera rempli automatiquement avec la prochaine adresse du réseau de liaison de commande de grappe. Vous pouvez modifier l'adresse hôte si vous le souhaitez.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.
- **Site ID** (ID de site) : (fonctionnalité FlexConfig) Saisissez l'ID de site pour ce nœud entre 1 et 8. La valeur 0 désactive la mise en grappe intersites. Les personnalisations supplémentaires de grappe intersites afin d'améliorer la redondance et la stabilité, comme la localisation des directeurs, la redondance de sites et la mobilité du flux de grappe, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig.

Étape 6 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save** (Enregistrer).

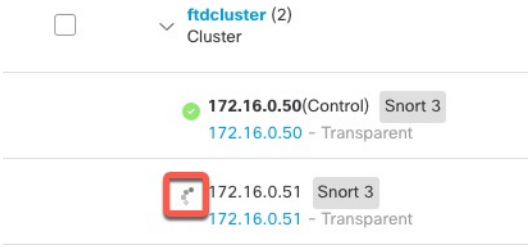
Le nom de la grappe s'affiche sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** ; développez la grappe pour voir ses nœuds.

Illustration 4 : Gestion des grappes

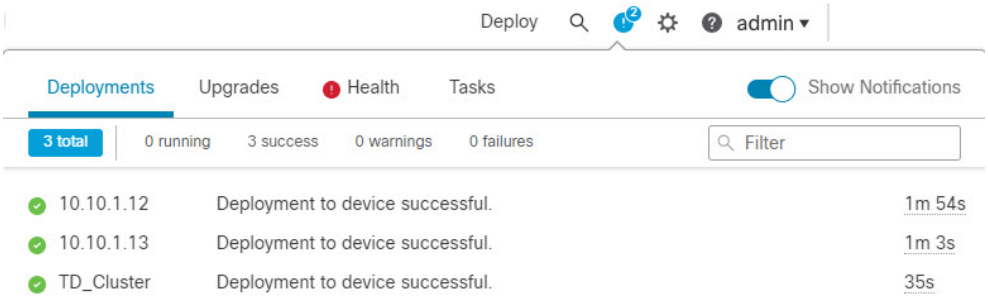


Un nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 5 : Inscription des nœuds



Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches). Le On-Prem Firewall Management Center met à jour la tâche d'enregistrement de grappe à mesure que chaque nœud s'enregistre.

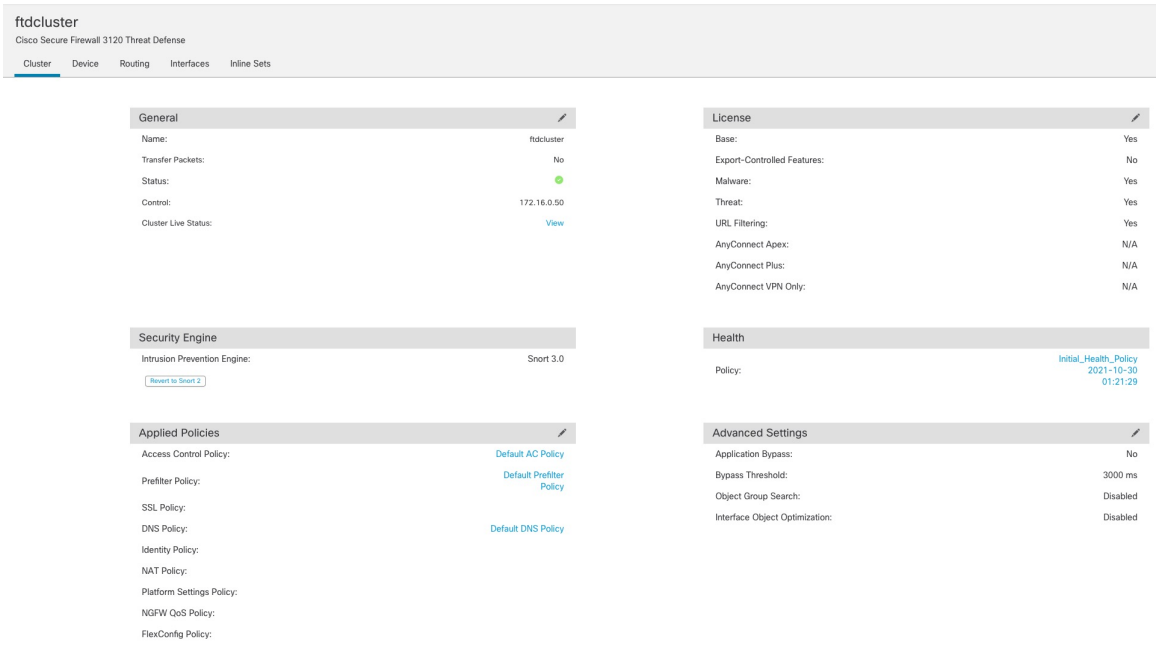


Étape 7 Configurez les paramètres spécifiques au périphérique en cliquant sur **Modifier** (✎) de la grappe.

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

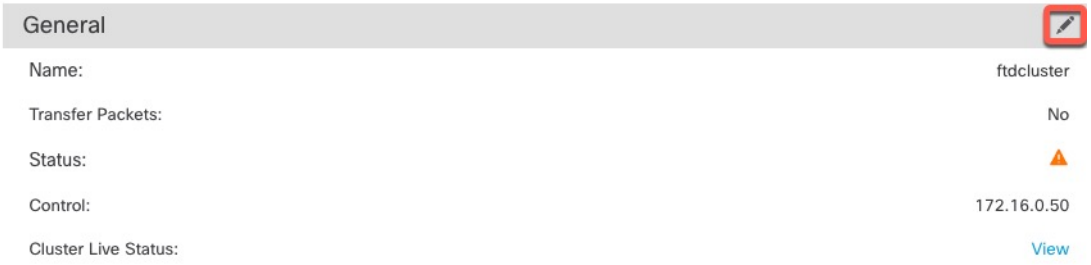
Étape 8 Sur l'écran **Devices (appareils)** > **Device Management (gestion des appareils)** et ensuite choisissez **Add**, **Cluster**, vous voyez **General** et d'autres paramètres pour la grappe.

Illustration 6 : Paramètres de la grappe

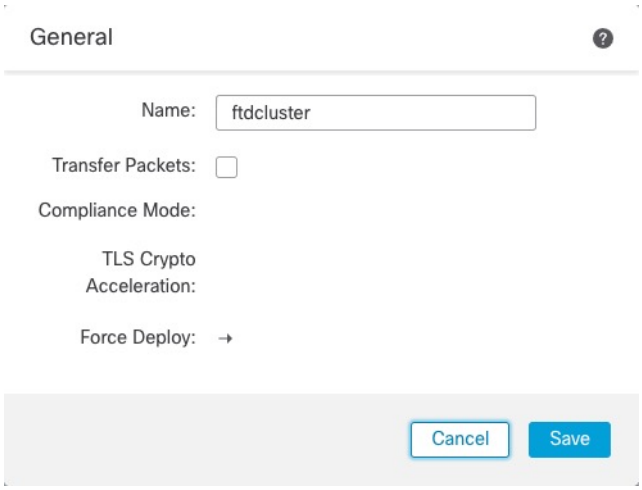


Consultez les éléments suivants, propres à la grappe, dans la zone **General** (Général) :

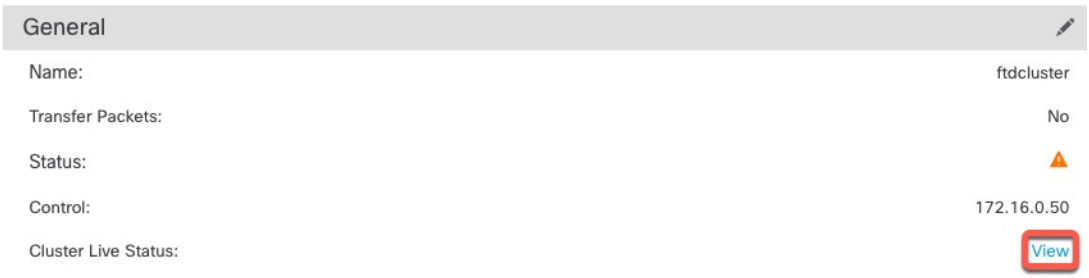
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Modifier** (✎).



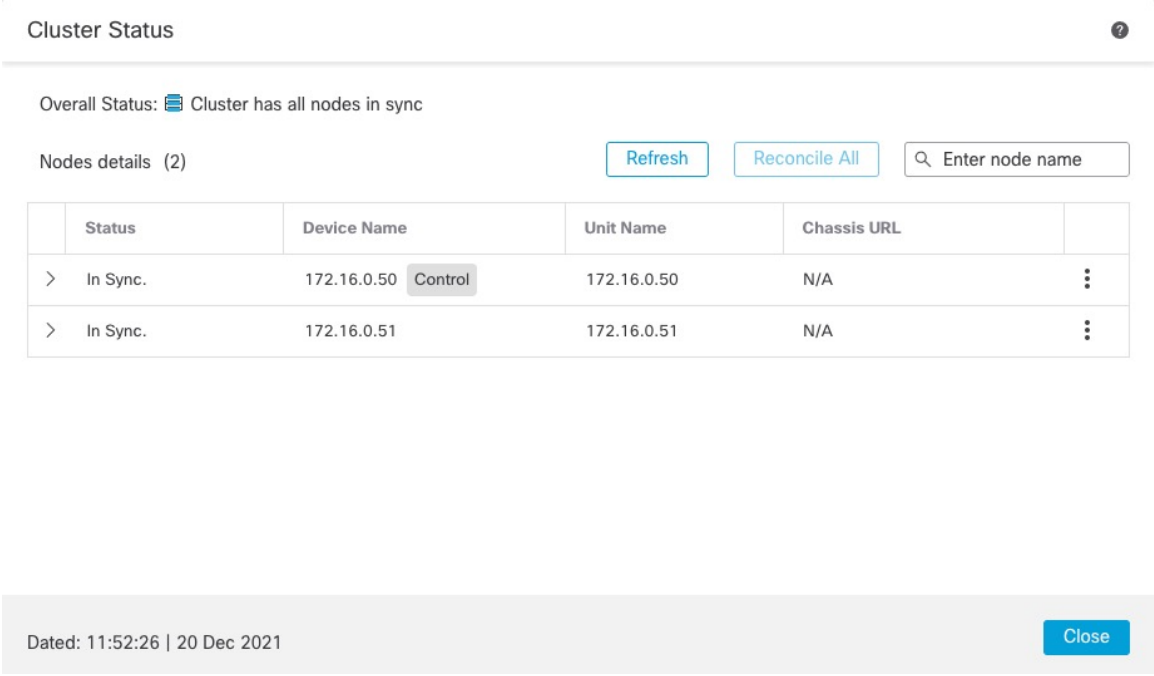
Définissez ensuite le champ **Name** (Nom).



- **General > Cluster Live Status**(Général > État de la grappe en direct) : cliquez sur le lien **View** (afficher) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).

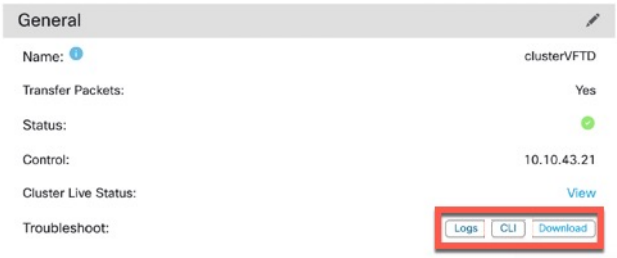


La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de relancer l'enregistrement de l'unité de données en cliquant sur **Reconcile All** (Rapprocher tout). Vous pouvez également envoyer un message Ping à la liaison de commande de grappe à partir d'un nœud. Consultez Effectuer un ping sur la liaison de commande de grappe, à la page 50.



- **General > Troubleshoot** (Général > Dépannage) : vous pouvez générer et télécharger des journaux de dépannage, et vous pouvez afficher les interfaces de ligne de commande des grappes. Consultez Dépannage de la grappe, à la page 49.

Illustration 7 : Dépanner



Étape 9 Sur **Devices (appareils)** > **Device Management (gestion des appareils)**, puis **Add** (Ajouter), **Device** (Périphérique), vous pouvez sélectionner chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

Illustration 8 : Paramètres du périphérique

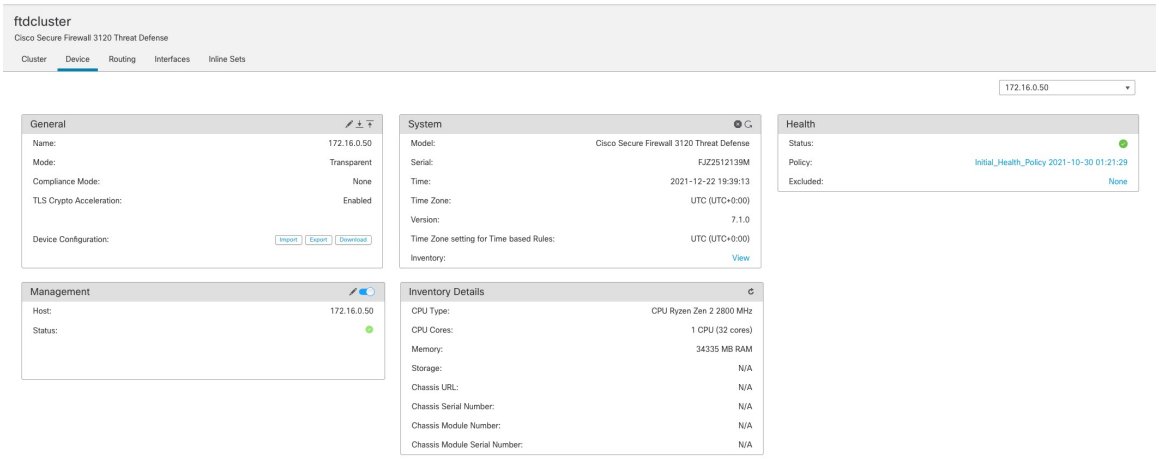
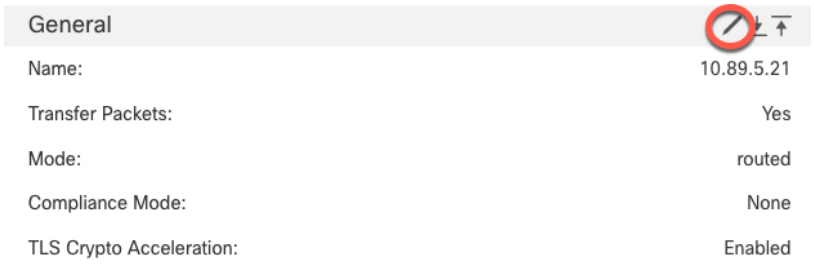
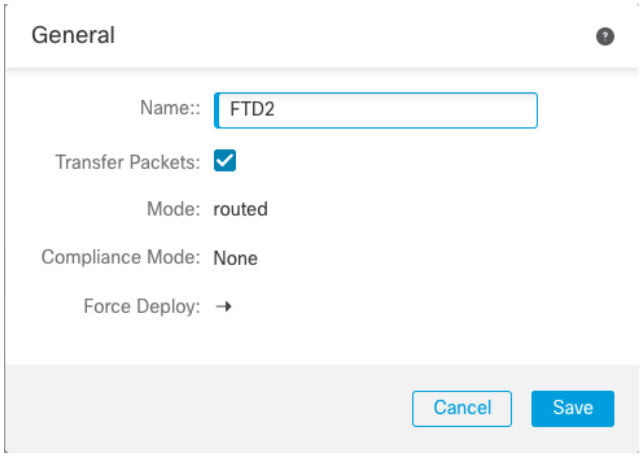


Illustration 9 : Choisir un nœud

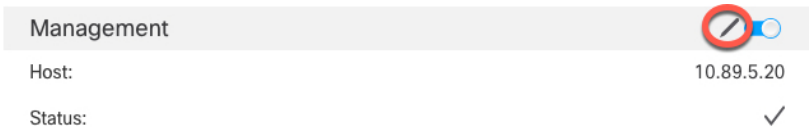
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Modifier** (✎).



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



- **Gestion > Hôte** : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, vous devez correspondre à la nouvelle adresse dans On-Prem Firewall Management Center pour qu'elle puisse atteindre le périphérique sur le réseau. Désactivez d'abord la connexion, modifiez l'adresse de l'**hôte** dans la zone **Management** (gestion), puis réactivez la connexion.



Interfaces de configuration

Vous pouvez configurer des interfaces de données en tant que canaux EtherChannels étendus ou en tant qu'interfaces individuelles. Chaque méthode utilise un mécanisme différent d'équilibrage de charge. Vous ne pouvez pas configurer les deux types dans la même configuration.

Configurer des EtherChannel étendus

Configurez les interfaces de données en tant qu'EtherChannels étendus.

Procédure

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

Étape 2 Cliquez sur **Interfaces**.

Étape 3 Configurez les interfaces de données de l'EtherChannel étendu.

a) Configurez un ou plusieurs EtherChannels.

Vous pouvez inclure une ou plusieurs interfaces membres dans l'EtherChannel. Comme cet EtherChannel s'étend sur tous les nœuds, vous n'avez besoin que d'une interface membre par nœud. Cependant, pour un débit et une redondance supérieurs, il est recommandé d'utiliser plusieurs membres.

b) (Facultatif) Pour les interfaces de pare-feu standard, configurez les sous-interfaces VLAN sur l'EtherChannel. Le reste de cette procédure s'applique aux sous-interfaces.

c) Cliquez sur **Modifier** (✎) pour l'interface EtherChannel.

d) Configurez le nom et les autres paramètres.

- 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. Par défaut, la MTU de la liaison de commande de grappe est de 1600 octets. Si vous souhaitez augmenter la MTU des interfaces de données, augmentez d'abord la MTU de la liaison de commande de grappe. Nous ne recommandons pas de définir la MTU de la liaison de contrôle de la grappe entre 2561 et 8362 ; en raison de la gestion du pool de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.
- Pour le mode routé, DHCP, PPPoE, la configuration automatique IPv6 et les adresses de liaison locales manuelles ne sont pas prises en charge. Pour les connexions point à point, vous pouvez

spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion.

e) 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 unique non utilisée actuellement sur votre réseau pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité 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.

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

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Déployer** > **Déployer** et déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les interfaces individuelles

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle.

Les interfaces de gestion individuelles vous permettent de connecter SSH directement à chaque unité si nécessaire, tandis qu'une interface EtherChannel étendue permet uniquement la connexion au nœud de contrôle.

Les interfaces IPS uniquement (ensembles en ligne et interfaces passives) ne sont pas prises en charge en tant qu'interfaces individuelles.

Avant de commencer

- Vous devez être en mode interface individuelle.
- Les interfaces individuelles nécessitent que vous configuriez l'équilibrage de charge sur les périphériques voisins. L'équilibrage de charge externe n'est pas requis pour l'interface de gestion.
- (Facultatif) Configurez l'interface en tant qu'interface EtherChannel locale du périphérique ou configurez les sous-interfaces.

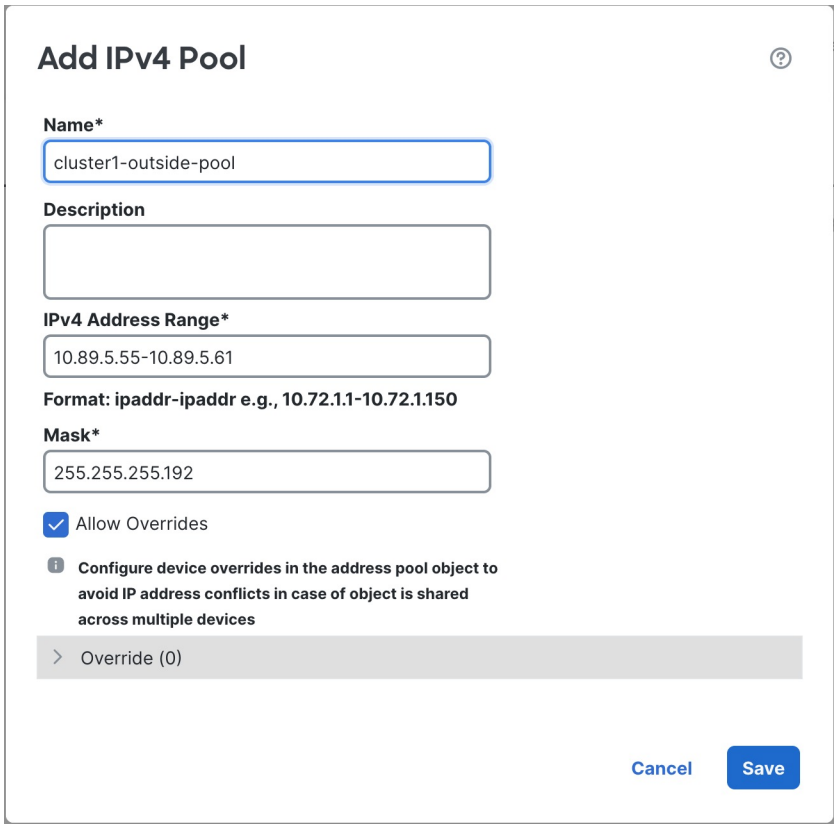
  Dans le cas d'un EtherChannel, celui-ci est local à l'unité et n'est pas un EtherChannel étendu.

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)** > **Address Pools (Ensembles d'adresses)** pour ajouter un ensemble d'adresses IPv4 et/ou IPv6.

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. L'adresse IP principale 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.

Illustration 10 : Add Address Pool (ajouter un ensemble d'adresses)



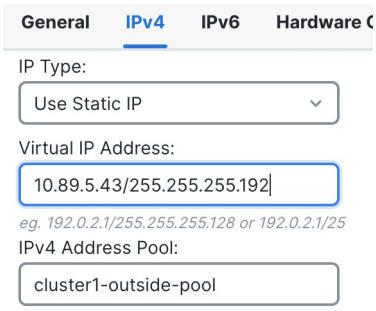
Remarque
Bien que cela ne soit pas courant, si vous souhaitez définir les adresses MAC manuellement, vous pouvez également ajouter un objet de regroupement d'adresses MAC.

Étape 2 Dans **Devices (appareils)** > **Device Management (gestion des appareils)**, puis choisissez **Interfaces**, cliquez sur **Modifier** (✎) pour l'interface que vous souhaitez configurer.

Étape 3 Dans la page **IPv4**, entrez **l'adresse IP virtuelle** et le masque. Cette adresse IP principale (« virtuelle ») est une adresse fixe pour la grappe et appartient toujours au nœud de contrôle.

Les protocoles DHCP et PPPoE ne sont pas pris en charge. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion.

Illustration 11 : Page IPv4



Étape 4 Dans la liste déroulante **IPv4 Address Pool** (ensemble d'adresses IPv4), choisissez l'ensemble d'adresses que vous avez créé.

Étape 5 Sur **IPv6 > Basic**, dans la liste déroulante **IPv6 Address Pool** (ensemble d'adresses IPv6), choisissez l'ensemble d'adresses que vous avez créées.

La configuration automatique IPv6 et les adresses de liaison manuelles ne sont pas prises en charge.

Étape 6 Configurez les autres paramètres de l'interface normalement.

Pour définir les adresses MAC manuellement, vous pouvez sélectionner l'ensemble d'adresses MAC dans la page **Advanced** (Advanced) de l'interface.

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. Par défaut, la MTU de la liaison de contrôle de la grappe est de 1600 octets. Si vous souhaitez augmenter la MTU des interfaces de données, augmentez d'abord la MTU de la liaison de commande de grappe. Nous ne recommandons pas de définir la MTU de la liaison de contrôle de la grappe entre 2561 et 8362 ; en raison de la gestion du pool de blocs, cette taille de MTU n'est pas optimale pour le fonctionnement du système.

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 12 : Paramètres de surveillance de l'intégrité de la grappe

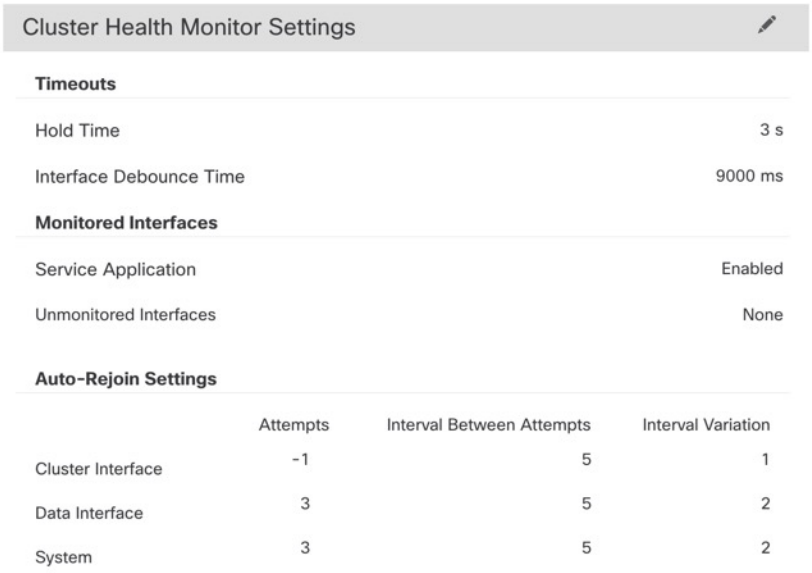


Tableau 1 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Entre 0,3 et 45 secondes; la valeur par défaut est de 3 secondes. 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	Entre 300 et 9 000 ms. La valeur par défaut est 500ms. 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	

Champ	Description
Interface de la grappe	Affiche les paramètres de jonction automatique après un échec de la liaison de commande de grappe.
Tentatives	Entre -1 et 65535. La valeur par défaut est -1 (illimité). Définit le nombre de tentatives de jonction.
Intervalle entre les tentatives	Entre 2 et 60. La valeur par défaut est 5 minutes. Définit la durée de l'intervalle en minutes entre les tentatives de jonction.
Variation de l'intervalle	Entre 1 et 3. La valeur par défaut est de 1x la durée de l'intervalle. Définit si la durée de l'intervalle augmente entre chaque tentative.
Interfaces de données	Affiche les paramètres de jonction automatique après la défaillance de l'interface de données.
Tentatives	Entre -1 et 65535. La valeur par défaut est de 3. Définit le nombre de tentatives de jonction.
Intervalle entre les tentatives	Entre 2 et 60. La valeur par défaut est 5 minutes. Définit la durée de l'intervalle en minutes entre les tentatives de jonction.
Variation de l'intervalle	Entre 1 et 3. La valeur par défaut est de 2x la durée de l'intervalle. Définit si la durée de l'intervalle augmente entre chaque tentative.
Système	Affiche les paramètres de jonction automatique après les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.
Tentatives	Entre -1 et 65535. La valeur par défaut est de 3. Définit le nombre de tentatives de jonction.
Intervalle entre les tentatives	Entre 2 et 60. La valeur par défaut est 5 minutes. Définit la durée de l'intervalle en minutes entre les tentatives de jonction.
Variation de l'intervalle	Entre 1 et 3. La valeur par défaut est de 2x la durée de l'intervalle. Définit si la durée de l'intervalle augmente entre chaque tentative.

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 changer 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)**.

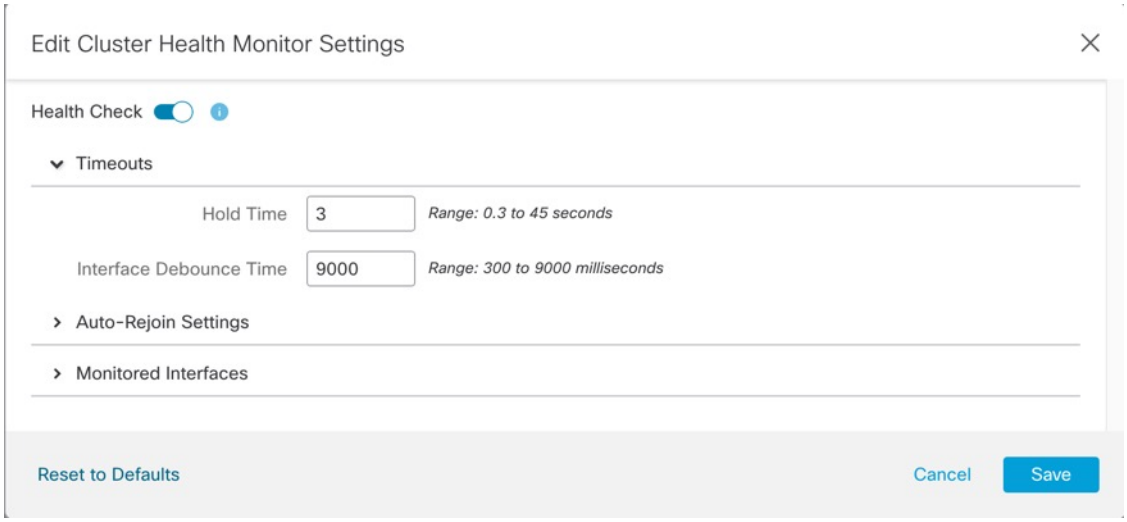
Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Modifier** (✎).

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 **Modifier** (✎).

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

Illustration 13 : 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 ou un VNet), 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.

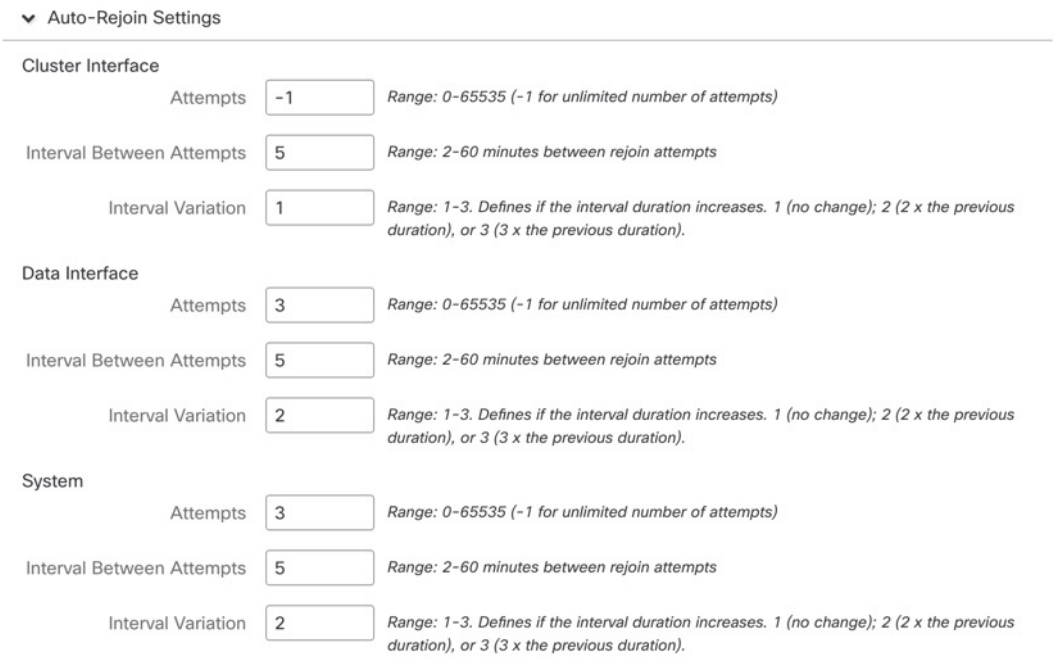
Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **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 14 : Configurer les paramètres de jonction automatique

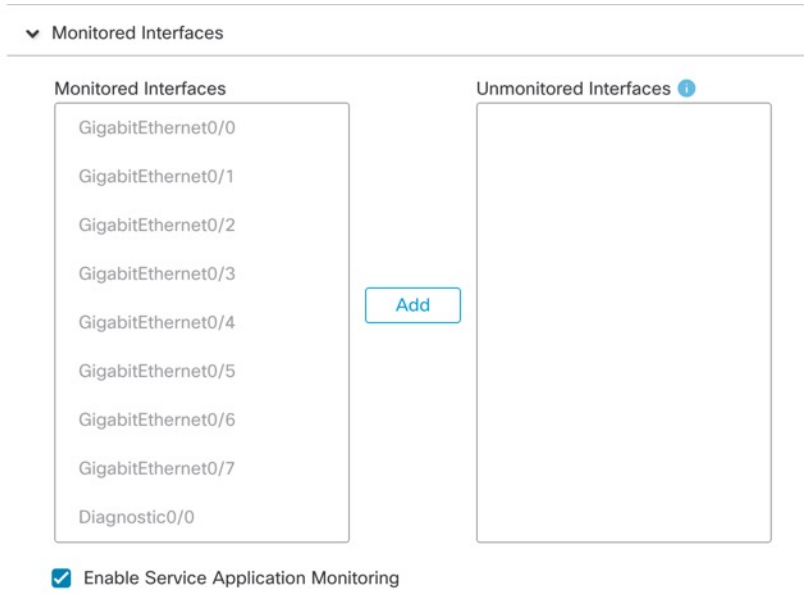


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **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 15 : 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.

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 ou un VNet), 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.

Gérer les nœuds de la grappe

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

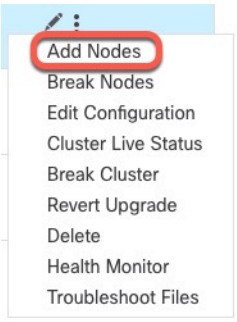
Ajouter un nouveau nœud de grappe

Vous pouvez ajouter un ou plusieurs nouveaux nœuds de grappe à une grappe existante.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮) pour la grappe, et choisissez **Add Nodes** (Ajouter des nœuds).

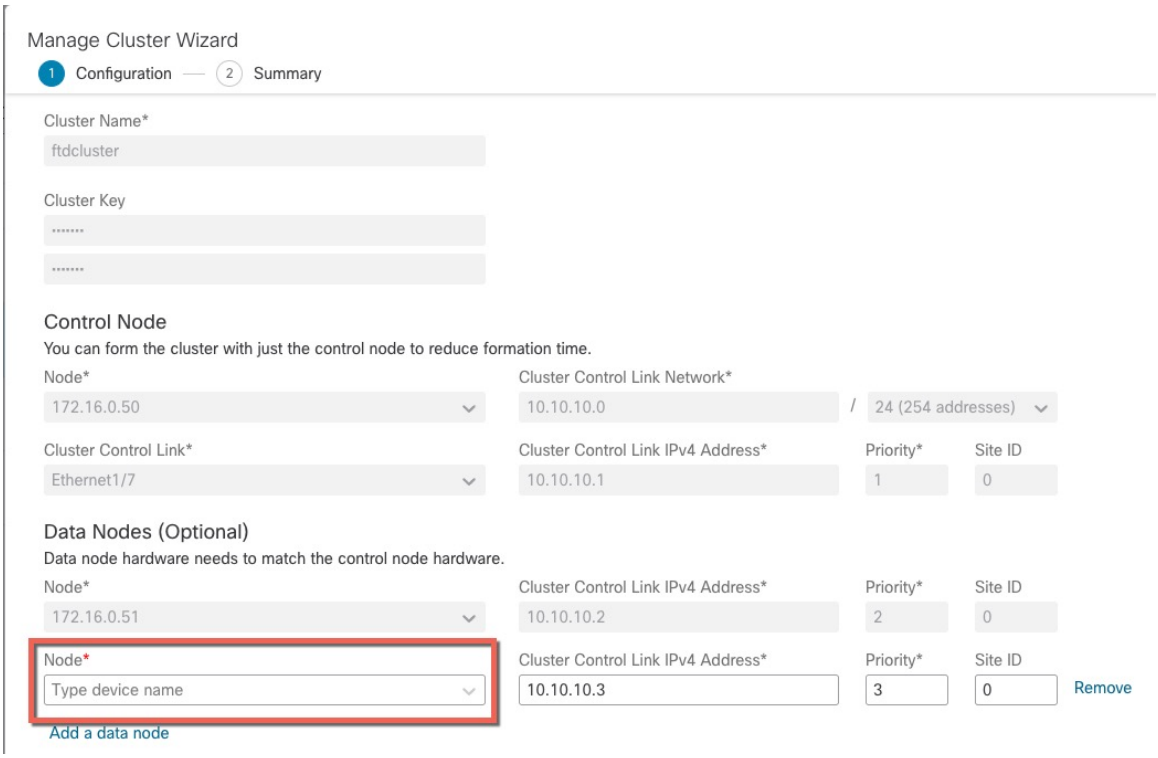
Illustration 16 : Ajouter des nœuds



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Dans le menu **Nœud**, choisissez un périphérique, ajustez l'adresse IP, la priorité et l'ID de site si vous le souhaitez.

Illustration 17 : Assistant de gestion des grappes

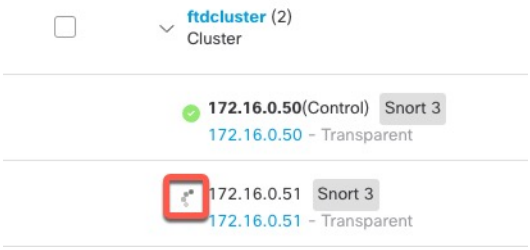


Étape 3 Pour ajouter des nœuds supplémentaires, cliquez sur **Add a data node** (Ajouter un nœud de données).

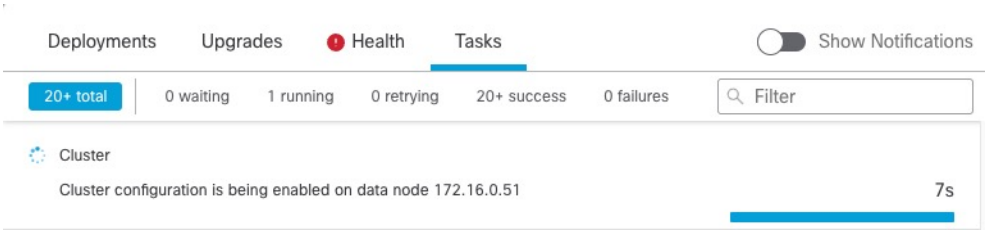
Étape 4 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save** (Enregistrer).

Le nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 18 : Inscription des nœuds



Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches).



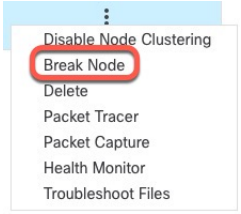
Séparer le nœud

Vous pouvez supprimer un nœud de la grappe pour qu'il devienne un périphérique autonome. Vous ne pouvez pas rompre le nœud de contrôle à moins de rompre la grappe entière. La configuration du nœud de données a été effacée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮) pour le nœud que vous souhaitez rompre, puis choisissez **Break Node** (Dissocier le nœud).

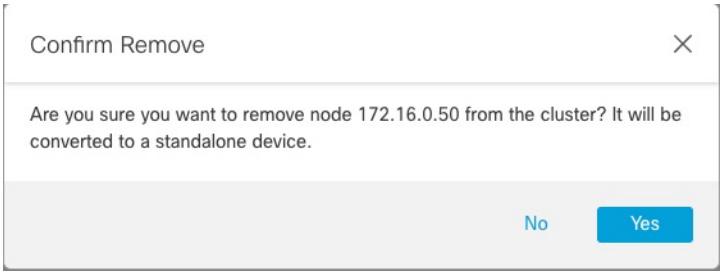
Illustration 19 : Séparer le nœud



Vous pouvez éventuellement séparer un ou plusieurs nœuds à partir du menu Plus de la grappe en sélectionnant **Break Nodes** (Séparer les nœuds).

Étape 2 Vous êtes invité à confirmer la séparation; cliquez sur **Yes**(oui).

Illustration 20 : Confirmer la rupture



Vous pouvez surveiller la rupture du nœud de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches).

Rompre la grappe

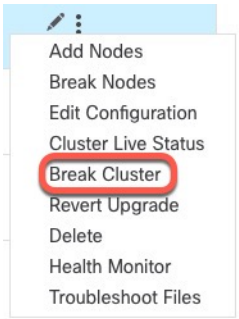
Vous pouvez rompre la grappe et convertir tous les nœuds en périphériques autonomes. Le nœud de contrôle conserve la configuration de l'interface et de la politique de sécurité, tandis que la configuration des nœuds de données est effacée.

Procédure

Étape 1 Vérifiez que tous les nœuds de la grappe sont gérés par On-Prem Firewall Management Center lors du rapprochement des nœuds. Consultez Rapprocher les nœuds de la grappe, à la page 40.

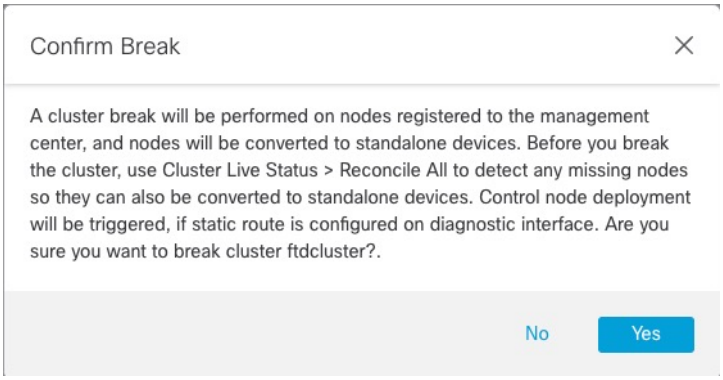
Étape 2 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮) pour la grappe, puis choisissez **Break Cluster** (Rupture de grappe).

Illustration 21 : Rompre la grappe



Étape 3 Vous êtes invité à rompre la grappe ; cliquez sur **Yes** (oui).

Illustration 22 : Confirmer la rupture



Vous pouvez surveiller l'interruption de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**.

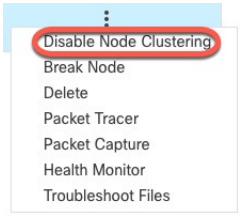
Désactiver la mise en grappe

Vous pouvez désactiver un nœud en préparation de sa suppression, ou temporairement pour la maintenance. Cette procédure vise à désactiver temporairement un nœud; le nœud continuera de s'afficher dans la liste des périphériques On-Prem Firewall Management Center. Lorsqu'un nœud devient inactif, toutes les interfaces de données sont fermées.

Procédure

Étape 1 Pour l'unité que vous souhaitez désactiver, sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮), et choisissez **Disable Node Clustering** (Désactiver la mise en grappe de nœuds).

Illustration 23 : Désactiver la mise en grappe



Si vous désactivez la mise en grappe sur le nœud de contrôle, l'un des nœuds de données deviendra le nouveau nœud de contrôle. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle. Vous ne pouvez pas désactiver la mise en grappe sur le nœud de contrôle s'il s'agit du seul nœud de la grappe.

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur le nœud.

Le nœud affichera **(Disabled)** (Désactivé) à côté de son nom dans la liste **Devices (appareils)** > **Device Management (gestion des appareils)** .

Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 38.

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe. Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe. Consultez Rejoindre la grappe, à la page 62 pour savoir pourquoi un nœud peut être supprimé d'une grappe.

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮), et sélectionnez **Enable Node Clustering** (Activer la mise en grappe de nœuds).

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

Modifier le nœud de contrôle

⚠

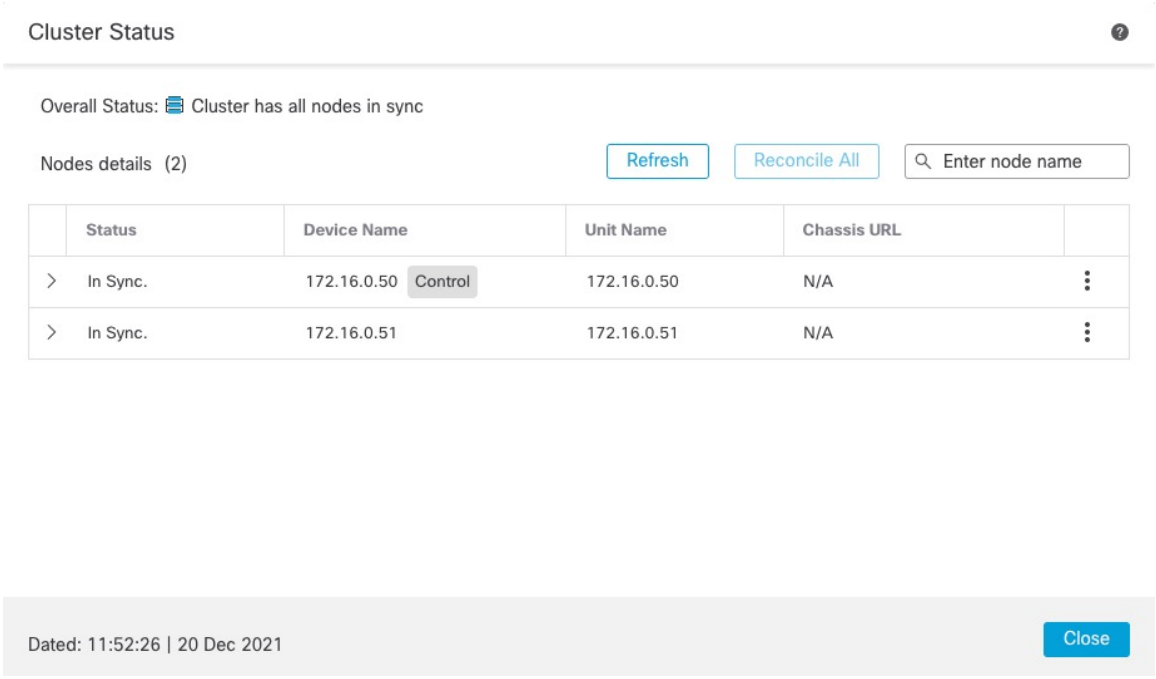
Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez préciser l'unité *exacte* que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle en utilisant l'une ou l'autre de ces méthodes, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Étape 1 Ouvrez la boîte de dialogue **Cluster Status** (État de la grappe) en sélectionnant **Devices (appareils)** > **Device Management (gestion des appareils) Plus** (⋮) **Cluster Live Status** (État en direct de la grappe).

Illustration 24 : État de la grappe (cluster)



Étape 2 Pour l'unité que vous souhaitez voir devenir l'unité de contrôle, sélectionnez (**Plus** (⋮) > **Change Role to Control (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**.

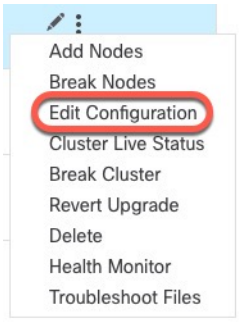
Modifier la configuration de grappe

Vous pouvez modifier la configuration de la grappe. Si vous modifiez la clé de grappe, l'interface de liaison de commande de grappe ou le réseau de liaison de commande de grappe, la grappe sera rompue et reconstituée automatiquement. Jusqu'à ce que la grappe soit reconstituée, vous pouvez subir des perturbations de trafic. Si vous modifiez l'adresse IP de la liaison de commande de grappe pour un nœud, une priorité de nœud ou un ID de site, seuls les nœuds concernés sont rompus et rajoutés à la grappe.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez **Plus** (⋮) pour la grappe, et choisissez **Edit Configuration** (Modifier la configuration).

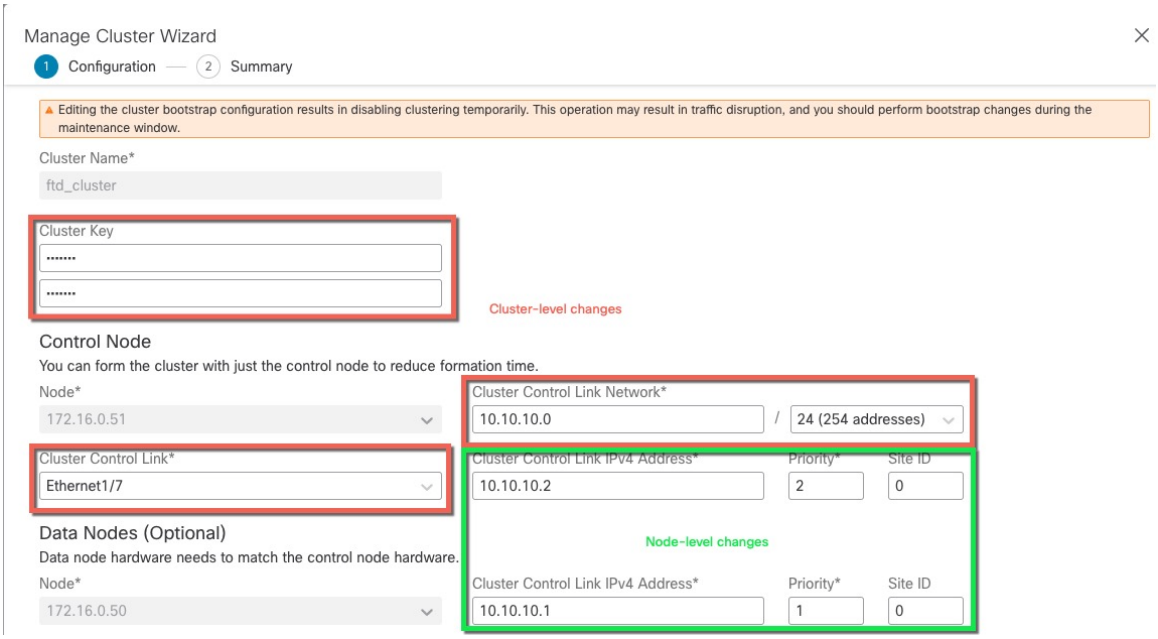
Illustration 25 : Modifier la configuration



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Mettre à jour la configuration de grappe

Illustration 26 : Assistant de gestion des grappes



Si la liaison de commande de grappe est un EtherChannel, vous pouvez modifier l'appartenance à l'interface et la configuration du protocole LACP en cliquant sur **Modifier** (✎) à côté du menu déroulant de l'interface.

Étape 3 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save** (Enregistrer).

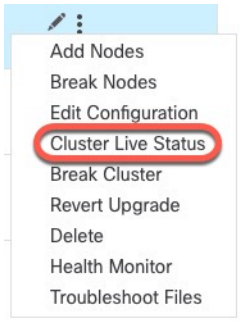
Rapprocher les nœuds de la grappe

Si un nœud de grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du périphérique avec On-Prem Firewall Management Center. Par exemple, un nœud de données peut ne pas s'enregistrer si On-Prem Firewall Management Center est occupé par certains processus ou en cas de problème de réseau.

Procédure

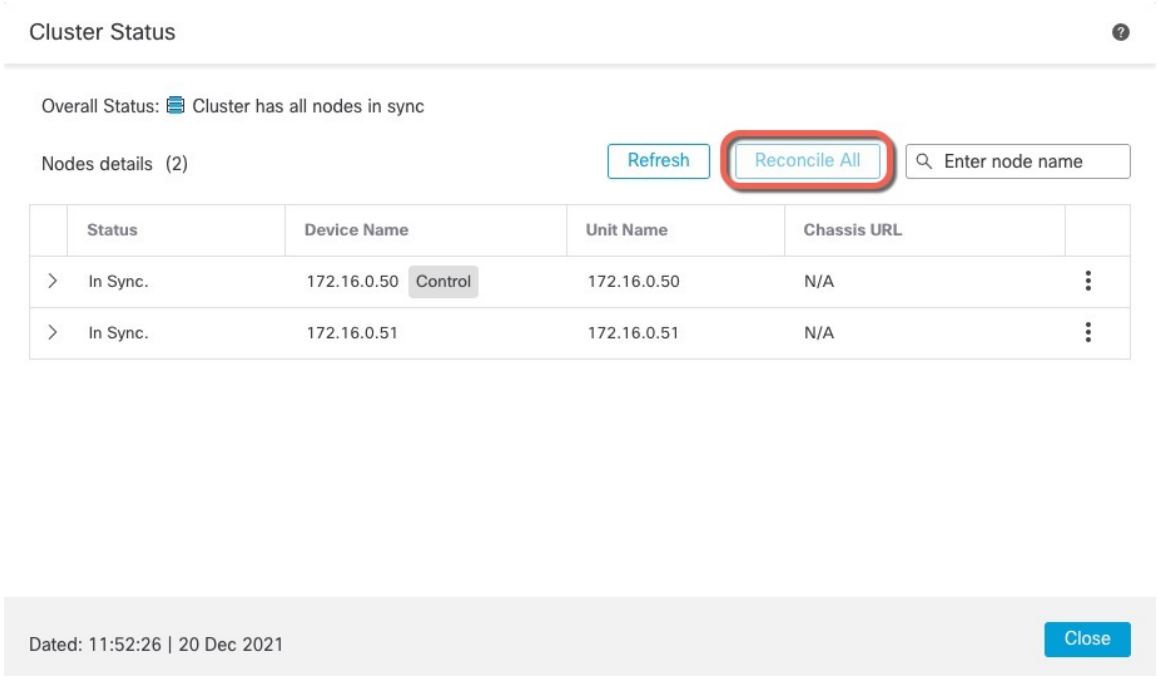
Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils) Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en temps réel de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Illustration 27 : État actuel de la grappe



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

Illustration 28 : Tout faire concorder



Pour plus d'informations sur l'état de la grappe, consultez Surveillance de la grappe, à la page 43.

Désenregistrer la grappe ou les nœuds et enregistrer dans un nouveau On-Prem Firewall Management Center

Vous pouvez annuler l'enregistrement de la grappe à partir de On-Prem Firewall Management Center, ce qui conserve la grappe inchangée. Vous souhaiterez peut-être annuler l'enregistrement de la grappe si vous souhaitez l'ajouter à un nouveau On-Prem Firewall Management Center.

Vous pouvez également désinscrire un nœud du On-Prem Firewall Management Center sans le dissocier de la grappe. Bien que le nœud ne soit pas visible dans le On-Prem Firewall Management Center, il fait tout de même partie de la grappe et continuera de transmettre le trafic et pourrait même devenir le nœud de contrôle. Vous ne pouvez pas annuler l'enregistrement du nœud de contrôle actuel. Il se peut que vous souhaitiez désenregistrer le nœud s'il n'est plus accessible depuis le On-Prem Firewall Management Center, mais que vous souhaitiez le conserver dans la grappe pendant que vous dépannez la connectivité de gestion.

Désinscription d'une grappe :

- Rompt toutes les communications entre le On-Prem Firewall Management Center et la grappe.
- Supprime la grappe de la page **Device Management** (gestion des périphériques).
- Rétablit la gestion locale de l'heure de la grappe si la politique de paramétrage de la plateforme de la grappe est configurée pour synchroniser l'heure à partir du On-Prem Firewall Management Center au moyen du protocole NTP.
- Laisse la configuration telle quelle, de sorte que la grappe continue de traiter le trafic.

  Les politiques, telles que la NAT et le VPN, les listes de contrôle d'accès et les configurations d'interface, demeurent inchangées.

Si vous enregistrez de nouveau la grappe sur le même On-Prem Firewall Management Center, ou sur un autre fichier, la configuration sera supprimée, de sorte que la grappe cessera de traiter le trafic à ce moment-là; la configuration de la grappe demeure inchangée, vous pouvez donc ajouter la grappe dans son ensemble. Vous pouvez choisir une politique de contrôle d'accès lors de l'inscription, mais vous devrez réappliquer les autres politiques après l'inscription, puis déployer la configuration avant de traiter à nouveau le trafic.

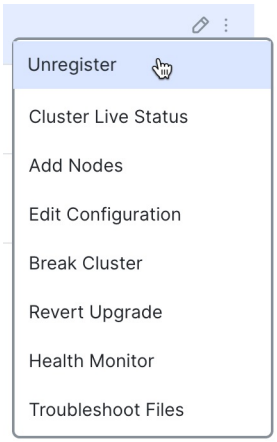
Avant de commencer

Cette procédure nécessite un accès de l'interface de ligne de commande à l'un des nœuds.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur **Plus** (⋮) pour la grappe ou le nœud, et choisissez **Unregister (Désinscrire)**.

Illustration 29 : Annuler l'enregistrement de la grappe ou du nœud



Étape 2 Vous êtes invité à annuler l'enregistrement et à la grappe ou le nœud; cliquez sur **Yes**(oui).

Étape 3 Vous pouvez enregistrer la grappe sur un nouveau (ou le même) On-Prem Firewall Management Center en ajoutant l'un des membres de la grappe en tant que nouveau périphérique.

Il vous suffit d'ajouter un des nœuds de la grappe en tant que périphérique et les autres nœuds de la grappe seront détectés.

a) Connectez-vous à l'interface de ligne de commande d'un nœud de la grappe et identifiez le nouveau On-Prem Firewall Management Center à l'aide de la commande **configure manager add**.
b) Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, et puis cliquez sur **Add (Ajouter)** > **Device (Périphérique)**.

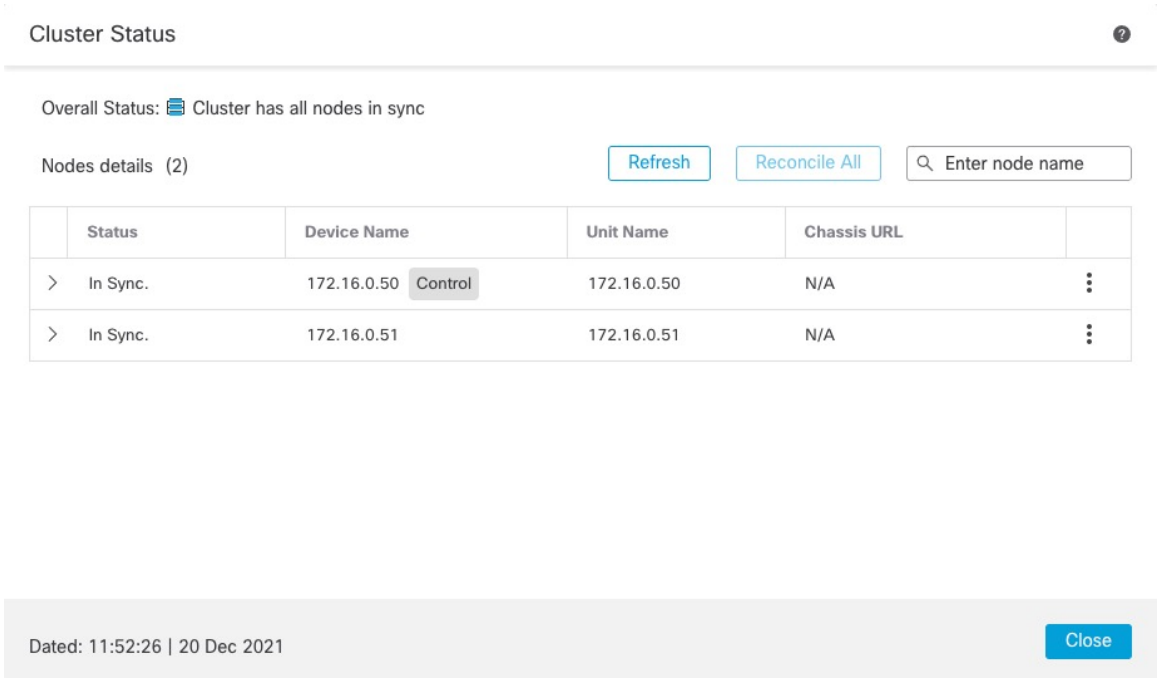
Étape 4 Pour rajouter un nœud non enregistré, consultez Rapprocher les nœuds de la grappe, à la page 40.

Surveillance de la grappe

Vous pouvez surveiller la grappe dans On-Prem Firewall Management Center et l'interface de ligne de commande Firewall Threat Defense.

- Boîte de dialogue **Cluster Status (État de la grappe**, accessible depuis l'icône **Devices (appareils)** > **Device Management (gestion des appareils) Plus** (⋮) ou depuis la zone General (Général) de la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe),** au moyen du lien **Cluster Live Status** (État en direct de la grappe).

Illustration 30 : État de la grappe (cluster)



Le nœud de contrôle est doté d'un indicateur graphique identifiant son rôle.

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

- En synchronisation : le nœud est enregistré auprès de On-Prem Firewall Management Center.
- En attente d'enregistrement : le nœud fait partie de la grappe, mais ne s'est pas encore enregistré auprès de On-Prem Firewall Management Center. Si un nœud ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- La mise en grappe est désactivée : le nœud est enregistré auprès de On-Prem Firewall Management Center, 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 le nœud de la grappe.
- Grappe en cours de jonction... : le nœud se joint à la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de On-Prem Firewall Management Center.

Pour chaque nœud, vous pouvez afficher le **résumé** ou l'**historique**.

Illustration 31 : Résumé du nœud

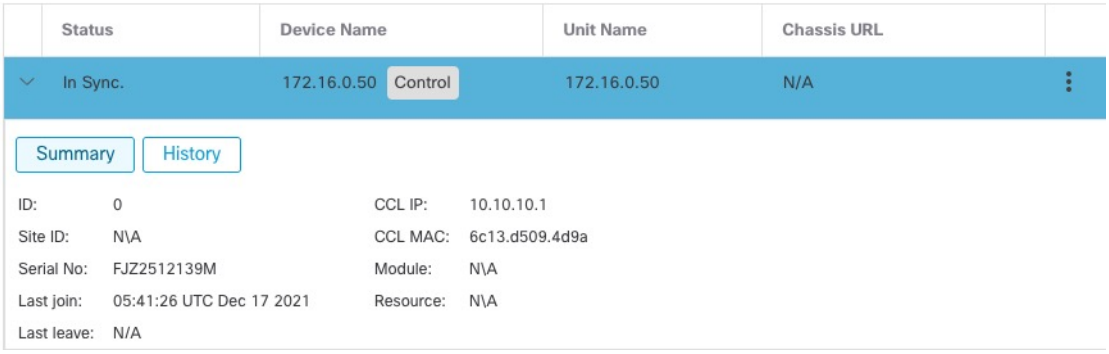
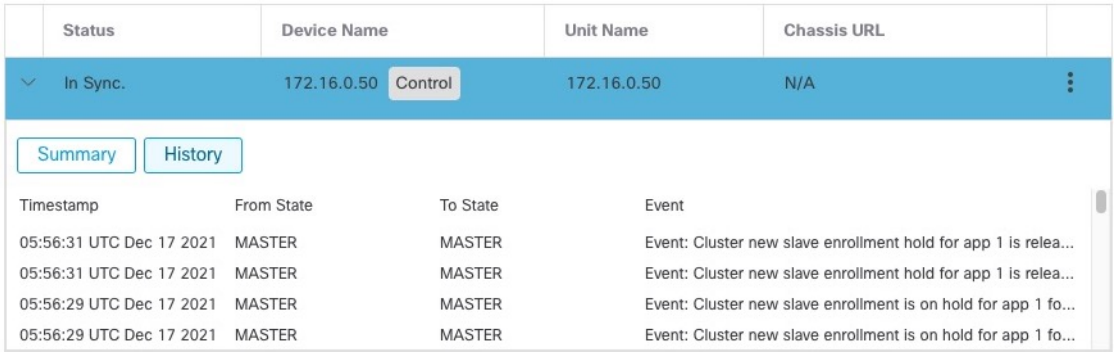


Illustration 32 : Historique du nœud



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

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

- **Devices (appareils)** > **Device Management (gestion des appareils)***cluster_name*

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir tous les nœuds membres, y compris le nœud de contrôle affiché avec son rôle à côté de l'adresse IP. L'icône de chargement s'affiche pour les nœuds 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** (afficher le 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 Firewall Threat Defense est le nœud de contrôle d'une grappe, On-Prem Firewall Management Center 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 On-Prem Firewall Management Center) 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 On-Prem Firewall Management Center.

Procédure

Étape 1 Choisissez **Système** (⚙) > **Health (Intégrité)** > **Monitor (Moniteur)**.

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 : Utilisation 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 **Ajouter un nouveau tableau de bord**( ) 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
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

Dépannage de la grappe

Vous pouvez utiliser l'outil **Ping CCL** pour vous assurer que la liaison de commande de grappe fonctionne correctement. Vous pouvez également utiliser les outils suivants, qui sont disponibles pour les périphériques et les grappes :

- Fichiers de dépannage : Si un nœud ne parvient pas à rejoindre la grappe, un fichier de dépannage est automatiquement généré. Vous pouvez également générer et télécharger des fichiers de dépannage à partir de **Devices (appareils)** > **Device Management (gestion des appareils)** et ensuite choisir **Add (Ajouter)**, **Cluster (Grappe)General (Général)** .

  Vous pouvez également générer des fichiers à partir de la page **Device Management** (gestion des périphériques) en cliquant sur **Plus** (⋮) et en sélectionnant **Dépannage des fichiers**.

- Sortie CLI : dans la zone **Devices (appareils)** > **Device Management (gestion des appareils)**, puis choisissez **Add (Ajouter)**, **Cluster (Grappe)General (Général)**, vous pouvez afficher un ensemble de sorties CLI prédéfinies pour dépanner la grappe. Les commandes suivantes sont automatiquement exécutées pour la grappe :

  - **show running-config cluster**

- **afficher l'information sur la grappe**
- **show cluster info health**
- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp (afficher le protocole arp)**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

Vous pouvez également saisir n'importe quelle commande **show** dans le champ Command.

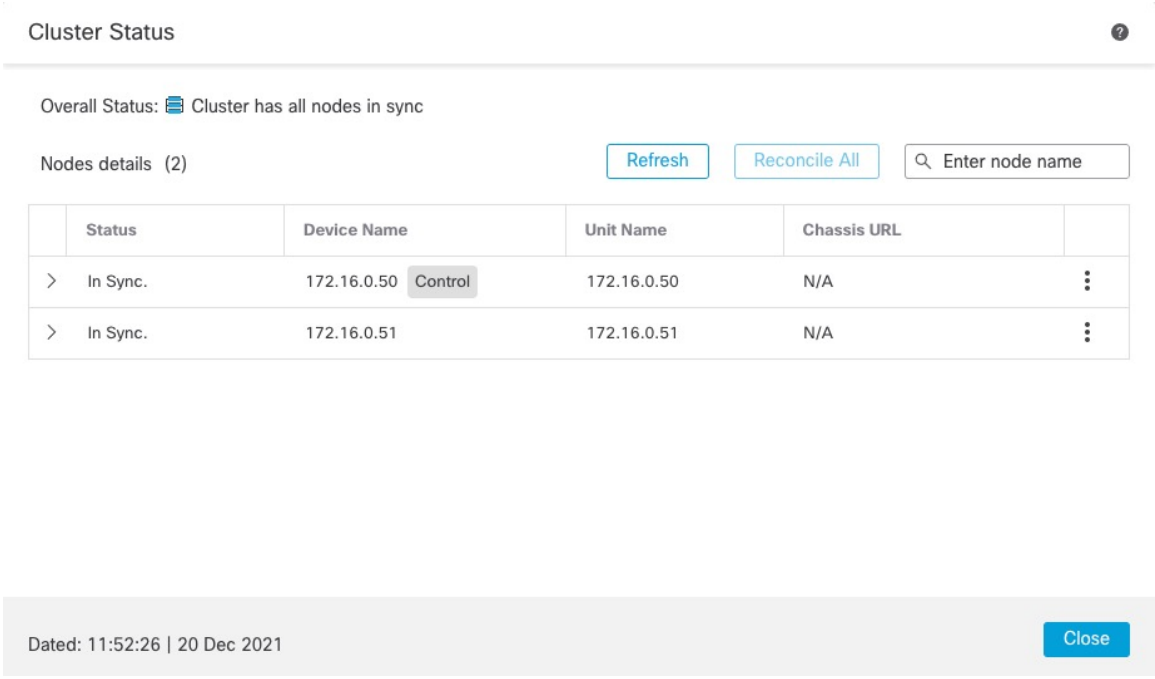
Effectuer un ping sur la liaison de commande de grappe

Lorsqu'un nœud rejoint la grappe, il vérifie la compatibilité MTU en envoyant un ping au nœud de contrôle avec une taille de paquet correspondant au MTU de la liaison de contrôle de grappe. Si le ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs connectés et réessayer. Cet outil vous permet d'envoyer un message ping manuel à tous les nœuds qui ont déjà rejoint la grappe au cas où vous auriez des problèmes de connectivité de liaison de commande de grappe.

Procédure

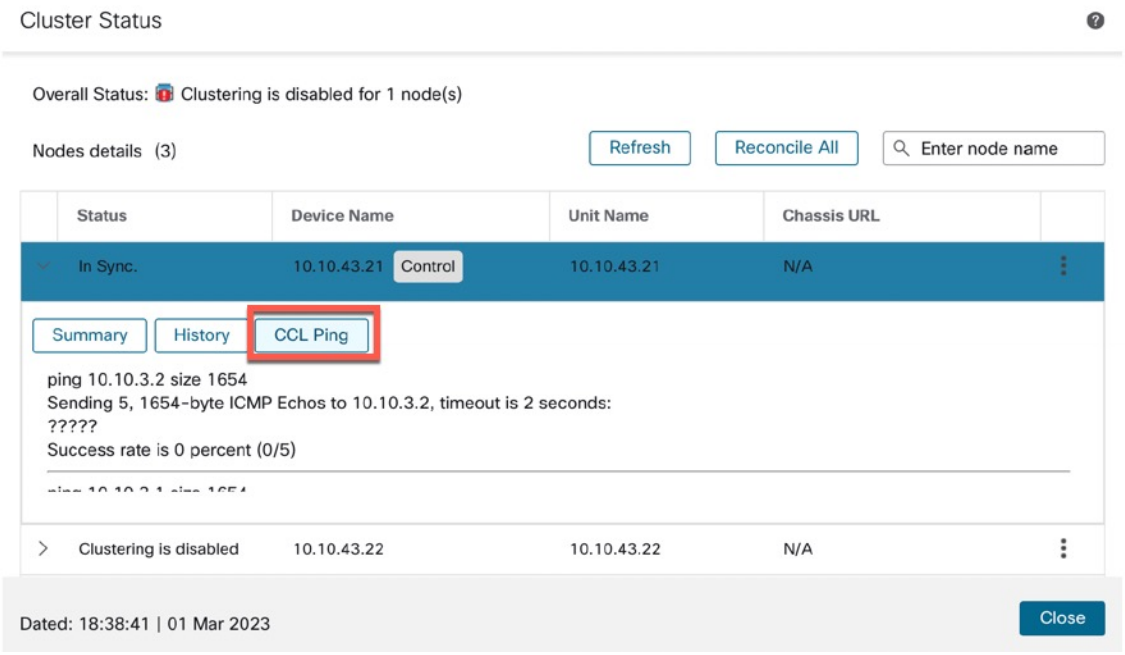
Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, cliquez sur l'icône **Plus** (⋮) à côté de la grappe et choisissez **Cluster Live Status** (État en temps réel de la grappe).

Illustration 33 : État de la grappe (cluster)



Étape 2 Développez l'un des nœuds et cliquez sur **CCL Ping**.

Illustration 34 : Ping CCL

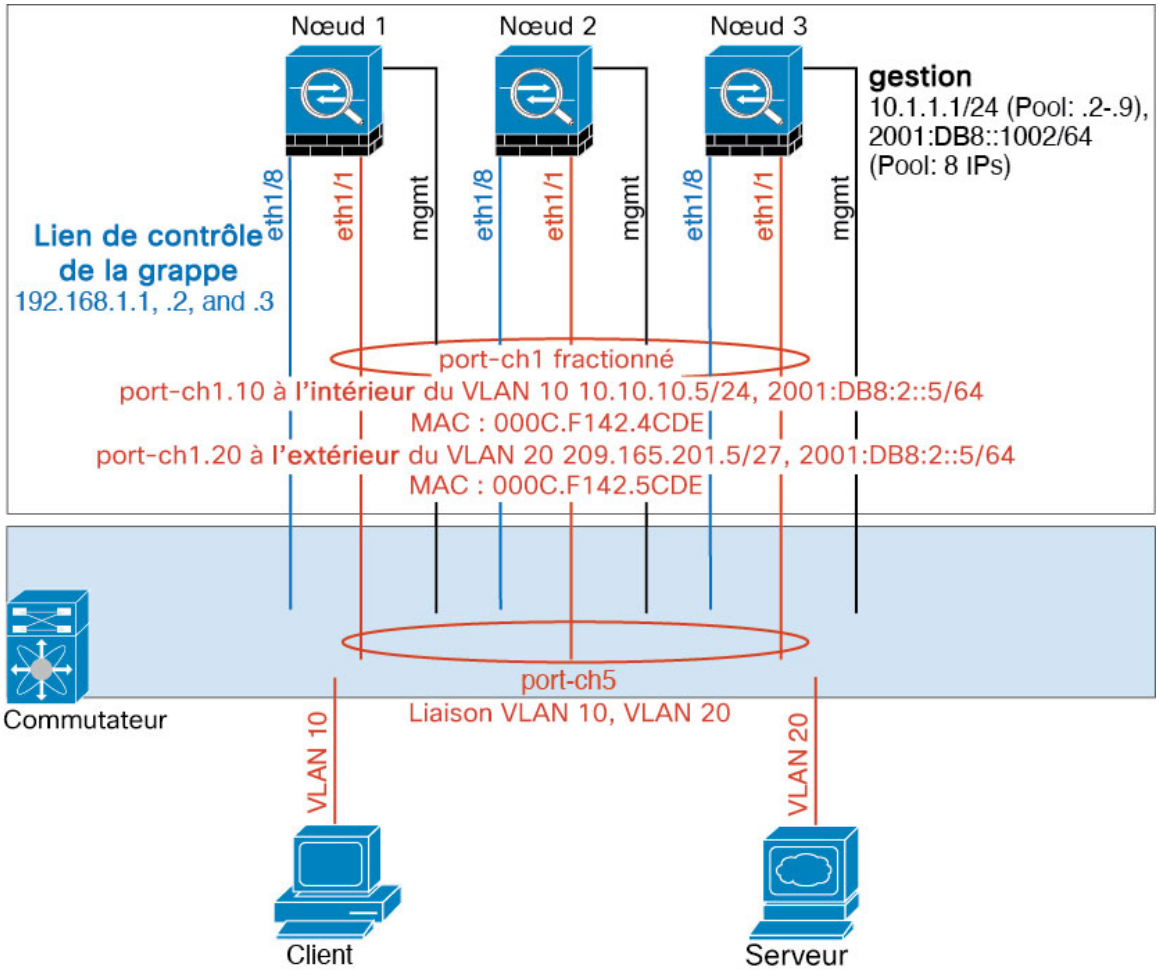


Le nœud envoie un message Ping sur la liaison de commande de grappe à tous les autres nœuds en utilisant une taille de paquet qui correspond à la MTU maximale.

Exemples de mise en grappe

Ces exemples comprennent des exemples de déploiements typiques.

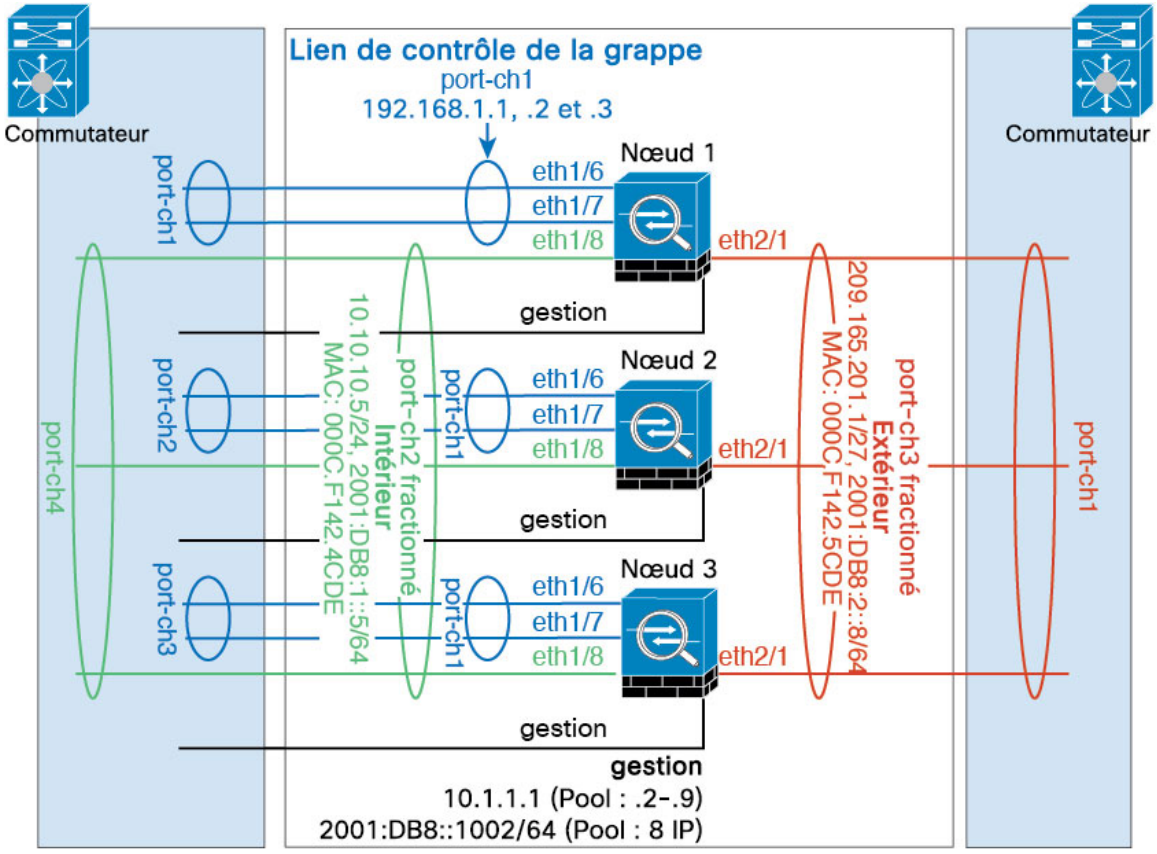
Pare-feu sur clé



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. Il 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. S'il 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 Firewall Threat Defense

Certaines fonctions Firewall Threat Defense 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 On-Prem Firewall Management Center.

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Le VPN de site à site (basé sur des politiques et basé sur des routes) n'est pas pris en charge dans les nuages publics.
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute accessibilité
- Routage et pont intégrés
- Mode UCAPL/CC On-Prem Firewall Management Center
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.

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 On-Prem Firewall Management Center.

- 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 (mode EtherChannel étendu uniquement)

Paramètres de connexion et mise en grappe

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.

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 en multidiffusion en mode d'interface individuelle

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

Routage en multidiffusion en mode d'interface individuelle

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

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents Firewall Threat Defensedans 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 Firewall Threat Defense qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

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

- No Proxy ARP (Pas de serveur mandataire ARP) : Pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un nœud qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale. Ce n'est pas un problème pour un EtherChannel étendu, car il n'y a qu'une seule adresse IP associée à l'interface de grappe.
- No interface PAT on an Individual interface (Pas de PAT d'interface sur une interface individuelle) Le PAT d'interface n'est pas pris en charge pour les interfaces individuelles.
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouvel ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.
- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, 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

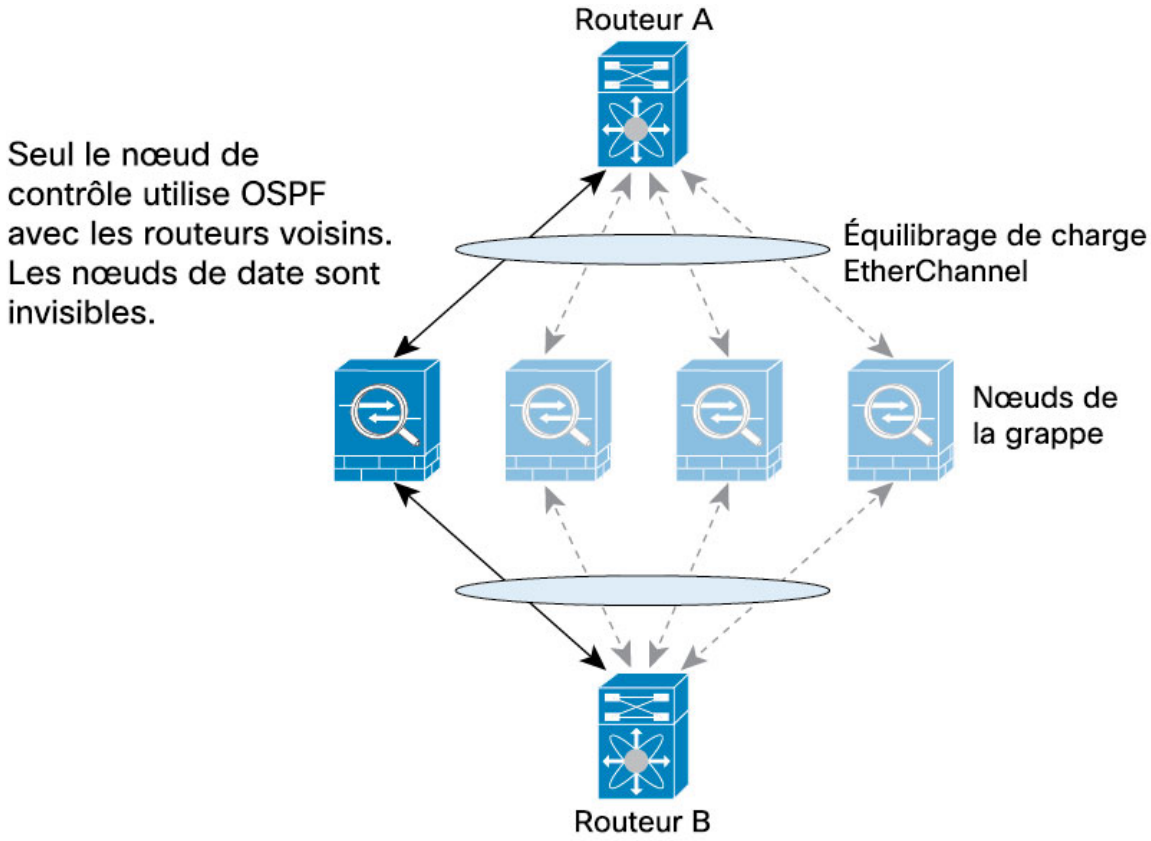
de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est 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.

Routage dynamique

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 35 : Routage dynamique en mode EtherChannel étendu



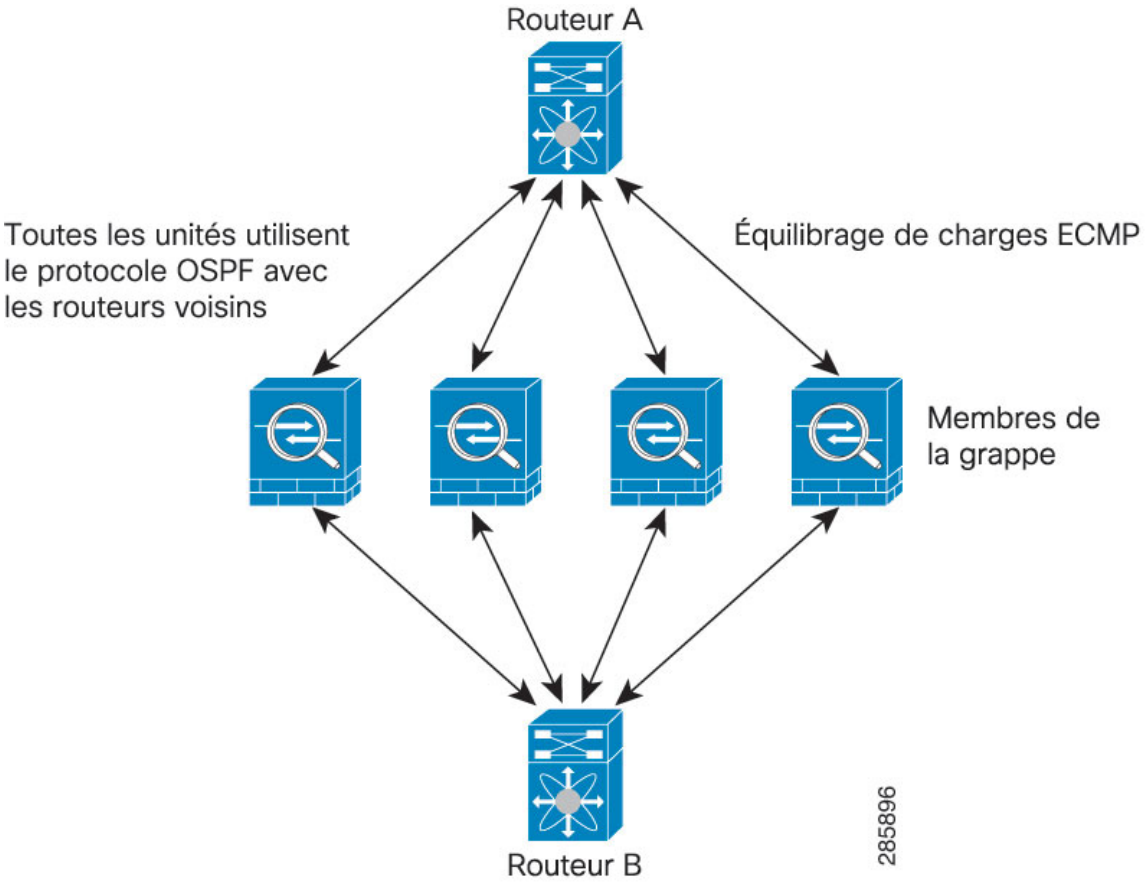
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud 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.

Routage dynamique en mode d'interface individuelle

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

Illustration 36 : Routage dynamique en mode d'interface individuelle



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

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

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

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

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

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.

Cisco TrustSec et la mise en grappe

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

VPN et mise en grappe

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

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

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

Lorsque vous connectez un tunnel VPN à une adresse EtherChannel étendu, les connexions sont automatiquement transférées au nœud de contrôle. Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

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

Facteur d'évolutivité de rendement

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

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

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

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

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

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

Haute disponibilité au sein de la grappe

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

Surveillance de l'intégrité du nœud

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

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 restaurée, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Consultez Choix du nœud de contrôle, à la page 61 pour de plus amples renseignements.

Surveillance d'interfaces

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

- Spanned EtherChannel (EtherChannel étendu) : Utilise le protocole cLACP (cluster Link Aggregation Control Protocol). Chaque nœud surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel. L'état est signalé au nœud de contrôle.
- Interfaces individuelles (mode routage uniquement) : chaque nœud surveille automatiquement ses interfaces et signale l'état des interfaces au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, ales interfaces physiques (y compris le canal EtherChannel principal) sont surveillées par défaut. Vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées. Par exemple, l'EtherChannel désigné doit échouer pour être considéré comme en échec, ce qui signifie que tous les ports membres d'un EtherChannel doivent échouer à déclencher la suppression de la grappe.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant que Firewall Threat Defense ne supprime un membre de la grappe dépend du type d'interface et dépend du fait que le nœud est un membre établi ou en train de se joindre à la grappe. Pour les EtherChannels (étendus ou non) : si l'interface est en panne sur un membre établi, le Firewall Threat Defense supprime le membre après 9 secondes. Le Firewall Threat Defense 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 Firewall Threat Defense de la grappe. Pour les non-EtherChannels, le nœud est supprimé après 500 ms, quel que soit l'état membre.

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.

Firewall Threat Defense tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque Firewall Threat Defense devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion 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 : Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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.

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	—

Trafic	Soutien relatif à l'état	Notes
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 de la sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

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

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

Connexions par traduction d'adresse de port

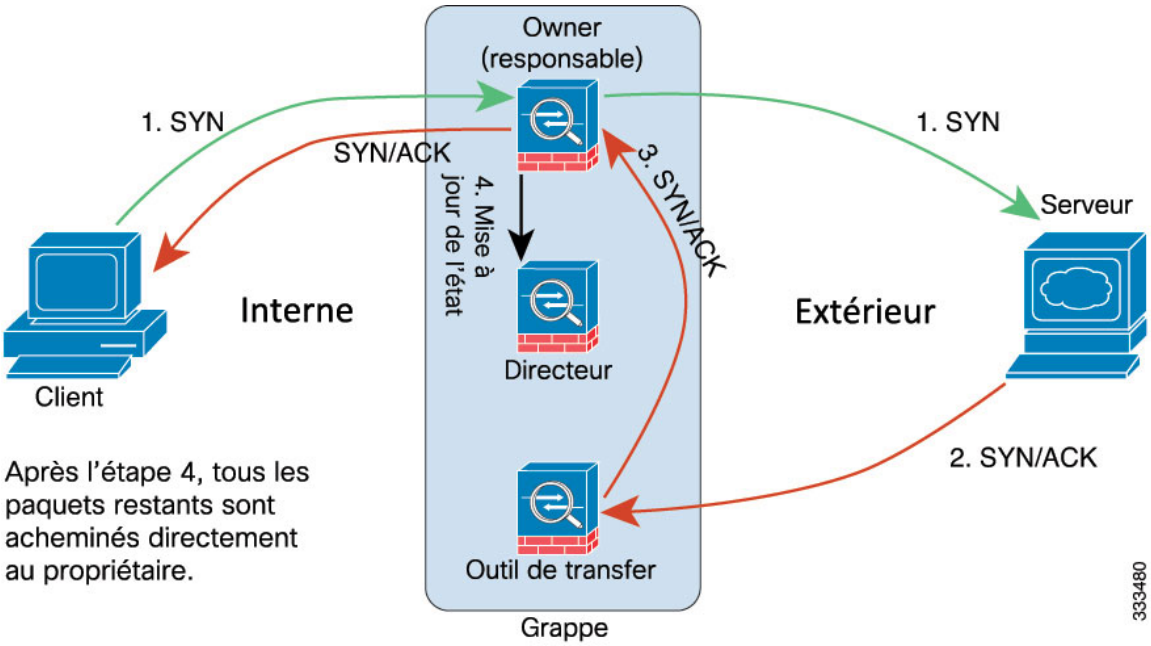
Nouvelle propriété de connexion

La redirection du trafic n'est pas prise en charge dans cette version. 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. Tous les paquets suivants pour la même connexion doivent arriver au même nœud. Si des paquets de connexion atteignent un autre nœud, ils seront abandonnés. Si un flux inverse arrive à un nœud différent, il sera également abandonné. Pour les fonctionnalités centralisées, si les connexions n'atteignent pas le nœud de contrôle, elles seront abandonnées.

Par défaut, AWS GWLB utilise le quintuple pour maintenir la rémanence du flux. Il est conseillé d'activer la rémanence de 2 ou 3 tuples sur AWS GWLB pour vous assurer que les mêmes flux sont envoyés au même nœud.

Exemple de flux de données pour TCP

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

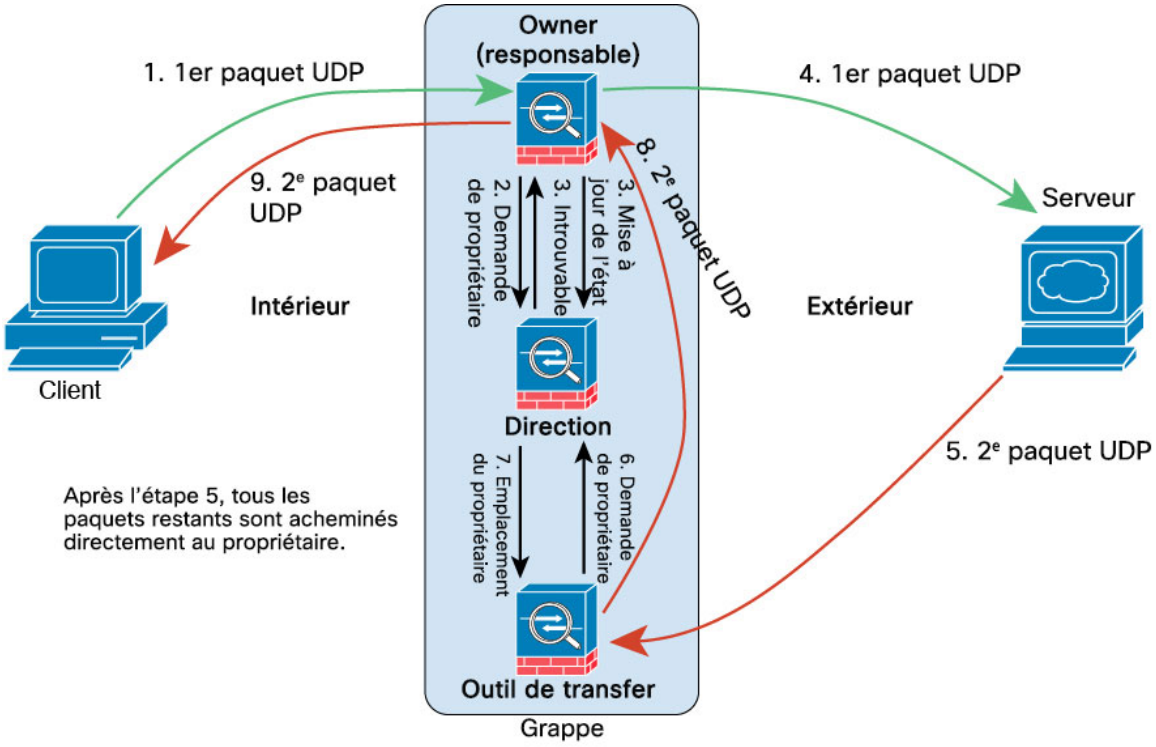


1. Le paquet SYN provient du client et est livré à un Firewall Threat Defense (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un Firewall Threat Defense différent (selon la méthode d'équilibrage de la charge). Ce Firewall Threat Defense 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 37 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un Firewall Threat Defense (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

Fonctionnalités	On-Prem Firewall Management Center Minimum	Firewall Threat Defense Minimum	Détails
Grappes de 16 nœuds pour Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0	Pour Cisco Secure Firewall 3100 et 4200, le nombre maximal de nœuds est passé de 8 à 16.
Mode d'interface individuelle pour les grappes Cisco Secure Firewall 3100/4200.	7.6.0	7.6.0	Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP locale utilisée pour le routage. L'adresse IP de la grappe principale pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente. L'équilibrage de charge doit être configuré séparément sur le commutateur en amont. Restrictions : instances de contenant non prises en charge. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **Cluster (grappe)** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objets** > **Gestion des objets** > **Ensemble des adresses** > **Ensemble des adresses MAC**
Test de ping MTU lors de l'adhésion d'un nœud à une grappe	7.6.0	7.6.0	Lorsqu'un nœud rejoint la grappe, il vérifie la compatibilité MTU en envoyant un ping au nœud de contrôle avec une taille de paquet correspondant au MTU de la liaison de contrôle de grappe. Si le ping échoue, une notification est générée afin que vous puissiez corriger l'incompatibilité MTU sur les commutateurs connectés et réessayer.
Outil de ping de liaison de commande de grappe.	7.2.6 7.4.1	N'importe lequel	Vous pouvez vérifier que tous les nœuds de la grappe peuvent communiquer entre eux sur la liaison de commande de grappe en effectuant un ping. L'une des principales causes de l'échec d'un nœud à rejoindre la grappe est une configuration incorrecte de la liaison de commande de la grappe; par exemple, la MTU de la liaison de commande de la grappe peut être plus élevée que les MTU des commutateurs de connexion. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **More (Plus)** > **Cluster Live Status (État en direct de la grappe).**

Fonctionnalités	On-Prem Firewall Management Center Minimum	Firewall Threat Defense Minimum	Détails
La génération et le téléchargement du fichier de dépannage sont disponibles à partir des pages Périphériques et Grappes.	7.4.1	7.4.1	Vous pouvez générer et télécharger des fichiers de dépannage pour chaque périphérique sur la page Périphérique, ainsi que pour tous les nœuds de la grappe sur la page Grappe. Pour une grappe, vous pouvez télécharger tous les fichiers en un seul fichier compressé. Vous pouvez également inclure les journaux de grappe de la grappe pour les nœuds de grappe. Vous pouvez également déclencher la génération de fichiers à partir du menu **Devices (Périphériques)** > **Devices (Gestion des périphériques) More (Plus) Troubleshoot Files (Fichiers de dépannage)**. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device (Périphérique)** > **General (Général)** • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **General (Général)**
Génération automatique d'un fichier de dépannage sur un nœud lorsque celui-ci ne parvient pas à rejoindre la grappe.	7.4.1	7.4.1	Si un nœud ne parvient pas à rejoindre la grappe, un fichier de dépannage est automatiquement généré pour ce dernier. Vous pouvez télécharger le fichier à partir de **Tâches** ou de la page **Grappe**.
Afficher la sortie de l'interface de ligne de commande pour un périphérique ou une grappe de périphériques.	7.4.1	N'importe lequel	Vous pouvez afficher un ensemble de sorties prédéfinies de l'interface de ligne de commande qui peuvent vous aider à dépanner le périphérique ou la grappe. Vous pouvez également saisir n'importe quelle commande **show** et voir le résultat. Écrans nouveaux ou modifiés :**Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **General (Général)**
Mise en grappe pour Cisco Secure Firewall 4200	7.4.0	7.4.0	Cisco Secure Firewall 4200 prend en charge la mise en grappe étendue sur l'EtherChannel pour jusqu'à 8 nœuds.
Paramètres de surveillance de l'intégrité de la grappe	7.3.0	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.

Fonctionnalités	On-Prem Firewall Management Center Minimum	Firewall Threat Defense Minimum	Détails
Tableau de bord de surveillance de l'intégrité de la grappe	7.3.0	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 (système)** > **Health** > **Monitor (surveillance de l'intégrité)**
Configuration automatique de la MTU de la liaison de commande de grappe	7.2.0	7.2.0	La MTU de l'interface de liaison de commande de grappe est maintenant automatiquement définie à 100 octets de plus que la MTU de l'interface de données la plus élevée; par défaut, la MTU est de 1600 octets.
Mise en grappe pour Cisco Secure Firewall 3100	7.1.0	7.1.0	Cisco Secure Firewall 3100 prend en charge la mise en grappe étendue sur l'EtherChannel pour jusqu'à 8 nœuds. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **More (Plus)**menu • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : Cisco Secure Firewall 3100

À propos de la traduction

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

À propos de la traduction

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