Haute disponibilité

Les rubriques suivantes décrivent comment configurer le basculement entre actif et veille pour atteindre la haute disponibilité de Défense contre les menaces.

À propos de la haute disponibilité Cisco Secure Firewall Threat Defense

La configuration de la haute disponibilité, également appelée basculement, nécessite deux périphériques défense contre les menaces identiques connectés l'un à l'autre par un lien de basculement dédié et, éventuellement, un lien d'état. défense contre les menaces prend en charge le basculement entre actif/veille, où une unité est l'unité active et transmet le trafic. L'unité secondaire (en veille) ne transmet pas activement le trafic, mais synchronise la configuration et les autres renseignements d'état de l'unité active. Lors d'un basculement, l'unité active est remplacée par l'unité en veille, qui devient alors active.

L'intégrité de l'unité active (matériel, interfaces, logiciels et état environnemental) est surveillée pour déterminer si les conditions spécifiques au basculement sont respectées. Si ces conditions sont remplies, le basculement se produit.

Remarque La haute disponibilité n'est pas prise en charge sur défense contre les menaces virtuelles s'exécutant dans le nuage public.

Prise en charge de la haute disponibilité sur les périphériques Défense contre les menaces dans un déploiement dans une succursale distante

Dans le déploiement d'une succursale à distance, l'interface de données du périphérique défense contre les menaces est utilisée pour la gestion de Cisco Defense Orchestrator au lieu de l'interface de gestion sur le périphérique. Comme la plupart des succursales distantes ne disposent que d'une seule connexion Internet, l'accès CDO extérieur permet une gestion centralisée.

Vous pouvez utiliser *n'importe quelle* interface de données pour l'accès àCDO, par exemple, l'interface intérieure si vous avez un CDO interne. Cependant, ce guide aborde principalement l'accès à l'interface externe, car c'est le scénario le plus probable pour les succursales à distance.

CDO fournit une prise en charge de la haute disponibilité sur les périphériques défense contre les menaces qu'il gère par l'interface de données. Cette fonctionnalité est prise en charge sur les périphériques fonctionnant avec la version logicielle 7.2 ou ultérieure.

Pour en savoir plus, consultez *Déploiement de Firepower Threat Defense avec un FMC distant* dans le Guide de démarrage Cisco Firepower.

Configuration système requise pour High Availability (haute disponibilité)

Cette section décrit les exigences matérielles, logicielles et de licence pour les Défense contre les menaces dans une configuration High Availability (haute disponibilité).

Configuration matérielle requise

Les deux unités dans une configuration High Availability (haute disponibilité) doivent :

- être du même modèle. En outre, les instances de conteneur doivent utiliser les mêmes attributs de profil de ressource.

  Pour la Firepower 9300, la haute disponibilité est uniquement prise en charge entre les modules de même type; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute disponibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

  Si vous modifiez le profil de ressources après avoir ajouté la paire à haute disponibilité au CDO, mettez à jour l'inventaire de chaque unité dans la boîte de dialogue **Périphériques** > **Gestion des périphériques** > **Périphériques** > **Système** > **Inventaire**.

  Si vous affectez un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

  1. Rompre la haute disponibilité
  2. Attribuer le nouveau profil aux deux unités.
  3. Rétablir la haute disponibilité.

- Avoir le même nombre et les mêmes types d'interfaces.

  Pour le Châssis Firepower 4100/9300 , toutes les interfaces doivent être préconfigurées en FXOS de manière identique avant d'activer High Availability (haute disponibilité). Si vous modifiez les interfaces après avoir activé High Availability (haute disponibilité), modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

- Ayez les paramètres suivants dans un déploiement de succursale distante :
  - Ayez la même interface de gestion des données pour gérer le trafic de gestion dans un déploiement à distance.

    Par exemple, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.
  - Utilisez l'interface de gestion des données pour la gestion du trafic.

    Vous ne pouvez pas gérer une unité à l'aide d'une interface de données et l'autre à l'aide d'une interface de gestion.

Si vous utilisez des unités avec des tailles de mémoire flash différentes dans votre configuration High Availability (haute disponibilité), assurez-vous que l'unité dotée de la mémoire flash la plus faible dispose de suffisamment d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Si ce n'est pas le cas, la synchronisation de la configuration de l'unité ayant la plus grande mémoire flash vers l'unité ayant la plus faible mémoire flash échouera.

Configuration logicielle requise

Les deux unités dans une configuration High Availability (haute disponibilité) doivent :

- : utilisez le même mode de pare-feu (routage ou transparent).
- Avoir la même version de logiciel;
- Faire partie du même domaine ou groupe sur centre de gestion.
- Ont la même configuration NTP. Consultez Configurer la synchronisation de l'heure NTP pour Threat Defense.
- Être entièrement déployé sur centre de gestion sans modifications non validées.
- DHCP ou PPPoE n'est configuré dans aucune de leurs interfaces.
- (Firepower 4100/9300) ont le même mode de déchargement de flux, activé ou désactivé.

Exigences de licence pour les périphériques Défense contre les menaces dans une paire à haute disponibilité

Les deux unités défense contre les menaces d'une configuration à haute disponibilité doivent avoir les mêmes licences.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire.

Avant que la haute disponibilité ne soit établie, les licences attribuées au périphérique secondaire ou en veille importent peu. Pendant la configuration à haute disponibilité, centre de gestion libère toutes les licences inutiles attribuées à l'unité de secours et les remplace par des licences identiques attribuées à l'unité principale ou active. Par exemple, si le périphérique actif dispose d'une licence Essentielle et d'une licence IPS et que le périphérique de veille n'a qu'une licence Essentielle , l'unité centre de gestion communique avec Cisco Smart Software Manager pour obtenir une licence IPS disponible pour votre compte, pour l'unité de veille Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, il devient non conforme jusqu'à ce que vous achetiez le nombre correct de licences.

Liens de basculement et de basculement avec état

Le lien de basculement et le lien de basculement dynamique facultatif sont des connexions dédiées entre les deux unités. Cisco recommande d'utiliser la même interface entre deux périphériques dans une liaison de basculement ou un lien de basculement avec état. Par exemple, dans un lien de basculement, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.

Lien de basculement

Les deux unités d'une paire de basculement communiquent en permanence sur une liaison de basculement pour déterminer l'état de fonctionnement de chaque unité.

Données de la liaison de basculement

Les informations suivantes sont transmises par la liaison de basculement :

- L'état de l'unité (actif ou en veille)
- Messages Hello (keep-alives)
- État de la liaison réseau
- Échange d'adresses MAC
- Réplication et synchronisation de la configuration

Interface de la liaison de basculement

Vous pouvez utiliser une interface de données inutilisée (physiqueinterface ou EtherChannel) comme liaison de basculement; cependant, vous ne pouvez pas spécifier une interface actuellement configurée avec un nom. Vous ne pouvez pas utiliser une interface de gestion des données si l'interface est configurée pour la communication avec CDO. Vous ne pouvez pas non plus utiliser une sous-interface, à l'exception d'une sous-interface définie sur le châssis pour le mode multi-instance. L'interface de liaison de basculement n'est pas configurée comme une interface réseau normale; il existe pour la communication de basculement uniquement. Cette interface ne peut être utilisée que pour la liaison de basculement (ainsi que pour le lien d'état).

Le défense contre les menaces ne prend pas en charge les interfaces de partage entre les données de l'utilisateur et le lien de basculement. Vous ne pouvez pas non plus utiliser des sous-interfaces distinctes sur le même parent pour la liaison de basculement et pour les données (sous-interfaces de châssis à instances multiples uniquement). Si vous utilisez une sous-interface de châssis pour le lien de basculement, toutes les sous-interfaces de ce parent, et le parent lui-même, sont restreintes pour utilisation en tant que liaisons de basculement.

Remarque Lorsque vous utilisez une comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec les mêmes interfaces membres existe sur les deux périphériques avant d'établir la haute disponibilité.

Consultez les consignes suivantes concernant la liaison de basculement :

- Firepower 4100/9300 : Nous vous recommandons d'utiliser une interface de données de 10 Go pour la combinaison de liaison de basculement et de liaison d'état.

- Tous les autres modèles : l'interface de 1 Go est suffisante pour une combinaison de liaison de basculement et d'état.

La fréquence d'alternance est égale au temps de maintien de l'unité.

Remarque Si vous avez une configuration importante et un temps d'attente d'unité faible, l'alternance entre les interfaces membres peut empêcher l'unité secondaire de se joindre ou de se joindre. Dans ce cas, désactivez l'une des interfaces membres jusqu'à ce que l'unité secondaire se soit jointe.

Pour un EtherChannel utilisé comme liaison de basculement, pour éviter les paquets dans le désordre, une seule interface dans l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'il est utilisé comme liaison de basculement.

Connexion de la liaison de basculement

Connectez le lien de basculement de l'une des deux manières suivantes :

- À l'aide d'un commutateur, sans autre périphérique sur le même segment de réseau (domaine de diffusion ou VLAN) que les interfaces de basculement du périphérique.
- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe.

Si vous n'utilisez pas de commutateur entre les unités, et en cas de défaillance de l'interface, la liaison est interrompue sur les deux homologues. Cette condition peut nuire aux efforts de dépannage, car vous ne pouvez pas facilement déterminer quelle unité a l'interface défaillante qui a entraîné la défaillance du lien.

Lien de basculement dynamique

Pour utiliser le basculement avec état, vous devez configurer un lien de basculement avec état (également appelé lien d'état) pour transmettre les informations sur l'état de la connexion.

Partagé avec la liaison de basculement

Le partage d'un lien de basculement est le meilleur moyen de conserver les interfaces. Cependant, vous devez envisager une interface dédiée pour le lien d'état et le lien de basculement, si votre configuration est importante et que le trafic sur le réseau est élevé.

Interface dédiée à la liaison de basculement dynamique

Vous pouvez utiliser une interface de données dédiée (physique ou EtherChannel) pour la liaison d'état. Consultez Interface de la liaison de basculement, à la page 4 pour connaître les exigences relatives à une lien liaison d'état dédiée et Connexion de la liaison de basculement, à la page 5 pour obtenir des renseignements sur la façon de connecter la liaison d'état.

Pour des performances optimales lors de l'utilisation du basculement longue distance, la latence de la liaison d'état doit être inférieure à 10 millisecondes et non supérieure à 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une certaine dégradation des performances se produit en raison de la retransmission des messages de basculement.

Éviter le basculement interrompu et les liaisons de données

Nous recommandons que les liens de basculement et les interfaces de données empruntent différentes voies pour réduire le risque d'échec de toutes les interfaces en même temps. Si le lien de basculement est arrêté, l'appareil défense contre les menaces peut utiliser les interfaces de données pour déterminer si un basculement est requis. Ensuite, l'opération de basculement est suspendue jusqu'à ce que l'intégrité du lien de basculement soit restaurée.

Consultez les scénarios de connexion suivants pour concevoir un réseau de basculement résilient.

Scénario 1 (non recommandé)

Si un seul commutateur ou un ensemble de commutateurs est utilisé pour connecter les interfaces de basculement et de données entre deux périphériques défense contre les menaces , quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux périphériques deviennent actifs.défense contre les menaces Par conséquent, les deux méthodes de connexion indiquées dans les figures suivantes ne sont **pas** recommandées.

Illustration 1 : Connexion avec un commutateur unique Non recommandée

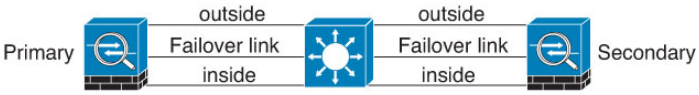
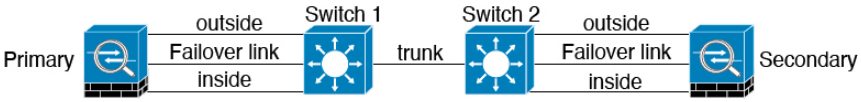


Illustration 2 : Connexion avec un double commutateur : non recommandée



Scénario 2 (recommandé)

Nous recommandons que les liens de basculement n'utilisent pas le même commutateur que les interfaces de données. Au lieu de cela, utilisez un commutateur différent ou utilisez un câble direct pour connecter le lien de basculement, comme le montrent les figures suivantes.

Illustration 3 : Connexion avec un autre commutateur

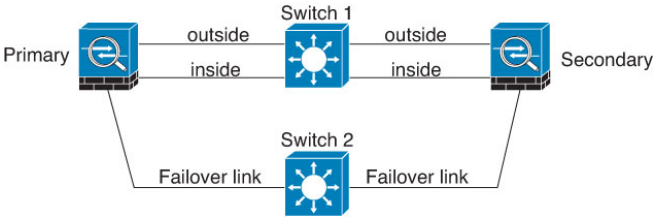
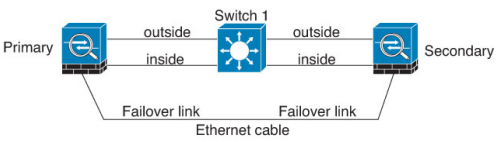


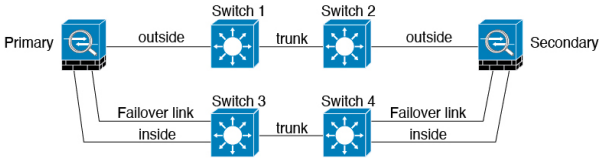
Illustration 4 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données défense contre les menaces sont connectées à plusieurs ensembles de commutateurs, un lien de basculement peut être connecté à l'un des commutateurs, de préférence le commutateur du côté sécurisé (interne) du réseau, comme le montre la figure suivante.

Illustration 5 : Connexion avec un commutateur sécurisé



Scénario 4 (recommandé)

Les configurations de basculement les plus fiables utilisent une interface redondante au niveau du lien de basculement, comme le montrent les figures suivantes.

Illustration 6 : Connexion avec des interfaces redondantes

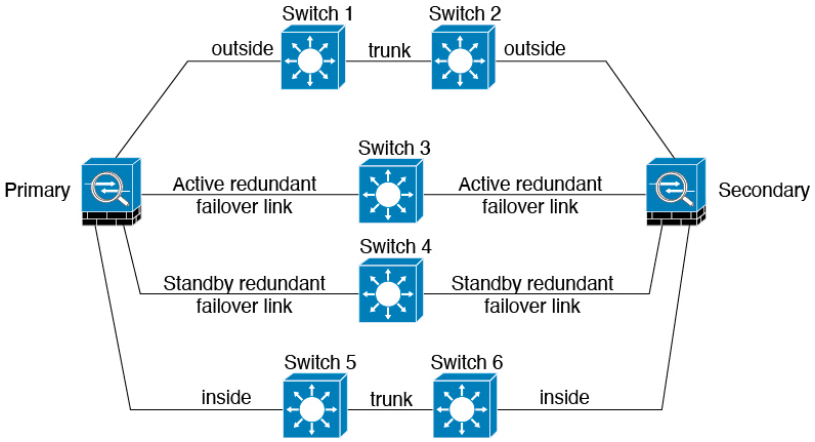
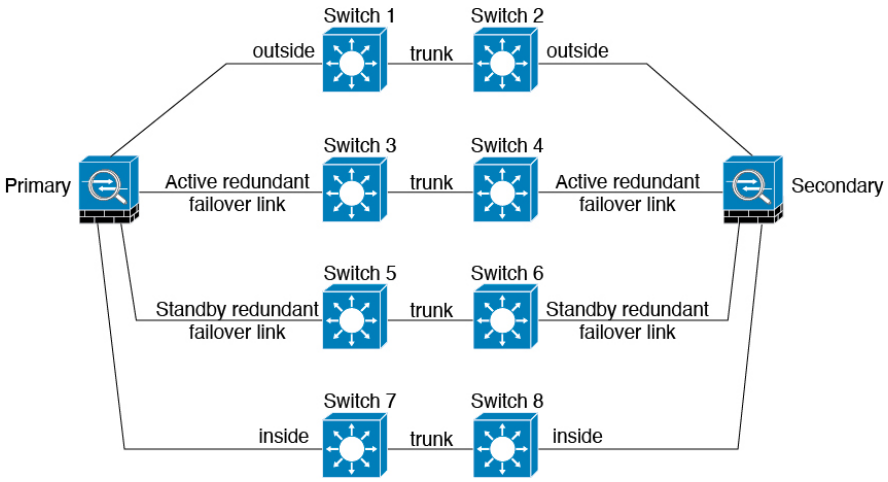


Illustration 7 : Connexion avec des liaisons inter-commutateurs



Les adresses MAC et les adresses IP en High Availability (haute disponibilité)

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. En général, lors d'un basculement, la nouvelle unité active prend en charge les adresses IP et MAC actives. Étant donné que les périphériques réseau ne constatent aucun changement dans l'association d'adresses MAC à l'adresse IP, aucune entrée ARP ne change et n'expire sur le réseau.

Remarque Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien. Vous ne pouvez pas non plus vous connecter à l'unité de secours sur cette interface à des fins de gestion.

L'adresse IP et l'adresse MAC du lien d'état ne changent pas lors du basculement.

Adresses IP et adresses MAC actives/en attente

Pour le High Availability (haute disponibilité)(actif/veille) consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité active utilise toujours les adresses IP et MAC de l'unité principale.
2. Lorsque l'unité active bascule, l'unité en veille adopte les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.
3. Lorsque l'unité défaillante est remise en ligne, elle est maintenant en état de veille et prend le relais des adresses IP et MAC de secours.

Toutefois, si l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC, car elle ne connaît pas les adresses MAC de l'unité principale. Lorsque l'unité principale devient disponible, les adresses MAC de l'unité secondaire (active) changent pour celles de l'unité principale, ce qui peut entraîner une interruption de votre trafic réseau. De même, si vous remplacez l'unité principale par un nouveau matériel, une nouvelle adresse MAC est utilisée.

Si vous rechargez l'unité de secours avec la configuration de basculement désactivée, l'unité de secours démarre en tant qu'unité active et utilise les adresses IP et MAC de l'unité principale. Cela conduit à des adresses IP en double et entraîne des perturbations du trafic réseau. Utilisez la commande **configure high-availability resume** pour activer le basculement et restaurer le flux de trafic.

Les adresses MAC virtuelles empêchent cette perturbation, car les adresses MAC actives sont connues de l'unité secondaire au démarrage et restent les mêmes dans le cas du nouveau matériel de l'unité principale. Nous vous recommandons de configurer l'adresse MAC virtuelle sur les unités principale et secondaire pour vous assurer que l'unité secondaire utilise les adresses MAC correctes lorsqu'il s'agit de l'unité active, même si elle est mise en ligne avant l'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devrez peut-être effacer les tableaux ARP sur les routeurs connectés pour restaurer le flux de trafic. appareil de défense contre les menaces n'envoie pas d'ARP gratuits pour les adresses NAT statiques lorsque l'adresse MAC change, de sorte que les routeurs connectés n'apprennent pas le changement d'adresse MAC pour ces adresses.

Adresses MAC virtuelles

L'appareil de défense contre les menaces comporte plusieurs méthodes pour configurer les adresses MAC virtuelles. Nous vous recommandons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible.

Pour la capacité multi-instance, le châssis FXOS génère automatiquement uniquement les adresses MAC principales pour toutes les interfaces. Vous pouvez remplacer l'adresse MAC générée par une adresse MAC virtuelle avec les adresses MAC principale et secondaire, mais la prédéfinition de l'adresse MAC secondaire n'est pas essentielle; la définition de l'adresse MAC secondaire garantit que le trafic de gestion vers le périphérique ne sera pas interrompu dans le cas d'une nouvelle unité secondaire matérielle.

Basculement avec état

pendant le basculement dynamique, l'unité active transmet en permanence des informations sur l'état de la connexion à l'unité en veille. Après un basculement, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications de l'utilisateur final prises en charge ne sont pas tenues de se reconnecter pour conserver la même session de communication.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis au appareil de défense contre les menaces de secours :

- table de traduction NAT
- Les connexions et les états TCP et UDP, y compris les états des connexions HTTP. Les autres types de protocoles IP et ICMP ne sont pas analysés par l'unité active, car ils sont établis sur la nouvelle unité active à l'arrivée d'un nouveau paquet.
- États de connexion Snort, résultats d'inspection et informations sur les trous d'épingle, y compris une application stricte du protocole TCP.
- La table ARP
- La table des ponts de couche 2 (pour les groupes de ponts)
- La table ISAKMP et IPsec SA
- La base de données sur les connexions GTP-PDP
- Sessions de signalisation SIP et trous d'épingle.
- Tables de routage statiques et dynamiques : le basculement dynamique participe aux protocoles de routage dynamiques, tels que OSPF et EIGRP, de sorte que les itinéraires appris par les protocoles de routage dynamiques sur l'unité active sont conservés dans une table RIB (Routing Information Base) sur l'unité en attente. Lors d'un basculement, les paquets se déplacent normalement avec une perturbation minimale du trafic, car l'unité secondaire active est initialement soumise à des règles qui reflètent l'unité principale. Immédiatement après le basculement, le délai de reconvergence démarre sur l'unité nouvellement active. Ensuite, le numéro de la période pour la table RIB est incrémenté. Pendant la reconvergence, les routes OSPF et EIGRP sont mises à jour avec un nouveau numéro de période. Une fois la minuterie expirée, les entrées de route périmées (déterminées par le numéro de période) sont supprimées du tableau. Le RIB contient ensuite les informations de transfert les plus récentes du protocole de routage sur la nouvelle unité active.

Remarque Les routages ne sont synchronisés que pour les événements de connexion ou de déconnexion sur une unité active. Si le lien est actif ou inactif sur l'unité de secours, les routages dynamiques envoyés à partir de l'unité active peuvent être perdus. Ce comportement est tout à fait normal et attendu.

- Serveur DHCP : les baux d'adresses DHCP ne sont pas répliqués. Cependant, un serveur DHCP configuré sur une interface enverra un message ping pour s'assurer qu'une adresse n'est pas utilisée avant d'accorder l'adresse à un client DHCP, donc il n'y a pas d'incidence sur le service. Les informations d'état ne sont pas pertinentes pour le relais DHCP ou DDNS.
- Décisions relatives à la politique de contrôle d'accès : les décisions relatives à la correspondance du trafic (y compris l'URL, la catégorie d'URL, la géolocalisation, etc.), la détection des intrusions, les programmes malveillants et le type de fichier sont conservées pendant le basculement. Cependant, pour les connexions évaluées au moment du basculement, les mises en garde suivantes doivent être apportées :
  - AVC : Les verdicts d'ID d'application sont répliqués, mais pas les états de détection. Une synchronisation appropriée a lieu tant que les verdicts App-ID sont complets et synchronisés avant le basculement.
  - État de la détection d'intrusion : lors du basculement, une fois que le prélèvement en milieu de flux se produit, de nouvelles inspections sont effectuées, mais les anciens états sont perdus.
  - Blocage des programmes malveillants : l'élimination des fichiers doit être disponible avant le basculement.
  - Détection et blocage du type de fichier : le type de fichier doit être identifié avant le basculement. Si le basculement se produit pendant que le périphérique actif d'origine identifie le fichier, le type de fichier n'est pas synchronisé. Même si votre politique de fichiers bloque ce type de fichier, le nouveau périphérique actif télécharge le fichier.
- Décisions relatives à l'identité de l'utilisateur à partir de la politique d'identité, y compris les correspondances entre l'utilisateur et l'adresse IP recueillies passivement par l'intermédiaire de et de l'annuaire des sessions ISE, ainsi que l'authentification active par le biais du portail captif. Les utilisateurs qui sont en train de s'authentifier activement au moment du basculement peuvent être invités à s'authentifier à nouveau.
- Network AMP : les recherches au sein du nuage sont indépendantes de chaque périphérique, de sorte que le basculement n'affecte pas cette fonctionnalité en général. Plus précisément :
  - Recherche de signature : si le basculement se produit au milieu d'une transmission de fichier, aucun événement de fichier n'est généré et aucune détection ne se produit.
  - Stockage de fichiers : si le basculement se produit lors du stockage du fichier, il est stocké sur le périphérique actif d'origine. Si le périphérique actif d'origine est tombé en panne pendant le stockage du fichier, le fichier n'est pas stocké.
  - Pré-classification de fichier (analyse locale) : si le basculement se produit au milieu de la pré-classification, la détection échoue.
  - Analyse dynamique de fichier (connectivité au nuage) : en cas de basculement, le système peut transmettre le fichier au nuage.

- Prise en charge des fichiers d'archive : si le basculement se produit au milieu d'une analyse, le système perd de la visibilité sur le fichier ou l'archive.
- Blocage personnalisé : en cas de basculement, aucun événement n'est généré.

- Décisions en matière de renseignements sur la sécurité. Cependant, les décisions basées sur le DNS qui sont en cours au moment du basculement ne sont pas prises.
- VPN d'accès à distance : les utilisateurs finaux du VPN d'accès à distance n'ont pas à s'authentifier ou à reconnecter la session VPN après un basculement. Cependant, les applications fonctionnant sur la connexion VPN pourraient perdre des paquets pendant le processus de basculement et ne pas se rétablir après la perte de paquets.
- De toutes les connexions, seules celles établies seront répliquées sur l'ASA de secours.

Fonctionnalités non prises en charge

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises au appareil de défense contre les menaces de secours :

- Sessions dans des tunnels en texte brut autres que GREv0 et IPv4-en-IP. Les sessions à l'intérieur des tunnels ne sont pas répliquées et le nouveau nœud actif ne pourra pas réutiliser les verdicts d'inspection existants pour faire correspondre les règles de politique correctes.
- Connexions TLS/SSL déchiffrées : les états de déchiffrement ne sont pas synchronisés et si l'unité active échoue, les connexions déchiffrées seront réinitialisées. De nouvelles connexions devront être établies avec la nouvelle unité active. Les connexions qui ne sont pas déchiffrées (c'est-à-dire celles qui correspondent à une action de règle Ne pas déchiffrer de TLS/SSL) ne sont pas affectées et sont répliquées correctement.
- Les connexions de contournement d'état TCP
- Le routage de multidiffusion

Exigences du groupe de ponts pour la haute disponibilité

Il y a des considérations particulières à prendre en matière de haute disponibilité lors de l'utilisation de groupes de ponts.

Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter les pertes de trafic sur les interfaces membres du groupe de ponts lorsque le port est dans un état bloquant, vous pouvez configurer l'une des solutions de contournement suivantes :

- Le port du commutateur est en mode d'accès : activez la fonctionnalité STP PortFast sur le commutateur :

  ```
  interface interface_id
    spanning-tree portfast
  ```

  La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- Si le port de commutation est en mode Trunk, ou si vous ne pouvez pas activer STP PortFast, vous pouvez utiliser l'une des solutions de contournement moins souhaitables suivantes qui a une incidence sur la fonctionnalité de basculement ou la stabilité STP :
  - Désactivez la surveillance sur le groupe de ponts et les interfaces membres.
  - Augmentez le temps d'attente de l'interface dans les critères de basculement à une valeur élevée qui permettra au protocole STP de converger avant que l'unité ne bascule.
  - Réduisez les minuteurs STP sur le commutateur pour permettre au STP de converger plus rapidement que le temps d'attente de l'interface.

Surveillance de l'intégrité du basculement

Le périphérique Défense contre les menaces surveille l'intégrité générale et l'intégrité de l'interface de chaque unité. Cette section comprend des informations sur la façon dont lepériphérique Défense contre les menaces effectue les tests pour déterminer l'état de chaque unité.

Surveillance de l'intégrité de l'unité

Le périphérique défense contre les menaces détermine l'intégrité de l'autre unité en surveillant le lien de basculement à l'aide de messages Hello. Lorsqu'une unité ne reçoit pas trois messages Hello consécutifs sur la liaison de basculement, l'unité envoie des messages LANTEST sur chaque interface de données, y compris la liaison de basculement, pour valider si l'homologue réagit ou non. L'action du périphérique défense contre les menaces dépend de la réponse de l'autre unité. Consultez les exemples d'actions suivantes :

- Si le périphérique défense contre les menaces reçoit une réponse sur le lien de basculement, il ne bascule pas.
- Si le périphérique défense contre les menaces ne reçoit pas de réponse sur la liaison de basculement, mais qu'il reçoit une réponse sur une interface de données, l'unité ne bascule pas. Le lien de basculement est marqué comme ayant échoué. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer sur l'unité de secours lorsque le lien de basculement est inactif.
- Si le périphérique défense contre les menaces ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Surveillance d'interfaces

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes, elle exécute des tests d'interface. Si l'un des tests d'interface échoue pour une interface, mais que cette même interface sur l'autre unité continue de transmettre le trafic avec succès, l'interface est considérée comme ayant échoué et lepériphérique arrête d'exécuter les tests.

Si le seuil que vous avez défini pour le nombre d'interfaces défaillantes est atteint (voir **Périphériques** > **Gestion des périphériques** > **Haute disponibilité** > **Critères de déclenchement du basculement**) et que l'unité active a plus d'interfaces défaillantes que l'unité en attente, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Inconnu » et ne sont pas prises en compte dans la limite de basculement définie par la politique d'interface de basculement.

Une interface devient de nouveau opérationnelle si elle reçoit du trafic. Un périphérique défaillant passe en mode veille si le seuil de défaillance de l'interface n'est plus atteint.

Si une interface a des adresses IPv4 et IPv6 configurées, le périphérique utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité. Si une interface n'a que des adresses IPv6 configurées, le périphérique utilise la découverte des voisins IPv6 au lieu d'ARP pour effectuer les tests de surveillance de l'intégrité. Pour le test de ping de diffusion, le périphérique utilise l'adresse de tous les nœuds IPv6 (FE02::1).

Tests d'interface

Lepériphérique Défense contre les menaces utilise les tests d'interface suivants. La durée de chaque test est d'environ 1,5 seconde.

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test de liaison active/désactivée indique que l'interface est en panne, lepériphérique la considère comme ayant échoué et les tests s'arrêtent. Si l'état est Activé, lepériphérique effectue le test d'activité réseau.
2. Test d'activité réseau : test d'activité réseau reçu. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets admissibles pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, lepériphérique démarre le test ARP.
3. Test ARP : Un test des réponses ARP réussies. Chaque unité envoie une seule requête ARP pour l'adresse IP dans l'entrée la plus récente de son tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si l'unité ne reçoit pas de réponse ARP, lepériphérique envoie une seule requête ARP pour l'adresse IP dans l'entrée *suivante* du tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, lepériphérique démarre le test ping de diffusion.
4. Test de ping de diffusion : un test de réponses au ping réussies. Chaque unité envoie un message Ping de diffusion, puis compte tous les paquets reçus. Si l'unité reçoit des paquets pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, les tests recommencent avec le test ARP. Si les deux unités continuent de ne recevoir aucun trafic venant des tests ARP et de ping de diffusion, ces tests continueront à se dérouler à l'infini.

État d'interface

Les interfaces surveillées peuvent avoir l'état suivant :

- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- Normal (en attente) : l'interface est opérationnelle, mais n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Normal (Non surveillée) : l'interface est opérationnelle, mais n'est pas surveillée par le processus de basculement.
- En test : les messages Hello ne sont pas entendus sur l'interface pendant cinq cycles d'interrogation.
- Liaison en panne : l'interface ou le VLAN est administrativement inactif.

- Liaison en panne (en attente) : l'interface ou le VLAN est en panne administrative et n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Liaison en panne (non surveillée) : l'interface ou le VLAN est en panne administrative, mais n'est pas surveillée par le processus de basculement.
- Aucune liaison : le lien physique de l'interface est inactif.
- Pas de liaison (en attente) : le lien physique de l'interface est inactif et n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Pas de liaison (non surveillée) : le lien physique de l'interface est inactif, mais n'est pas surveillé par le processus de basculement.
- Échec : aucun trafic n'est reçu sur l'interface, mais le trafic est diffusé sur l'interface homologue.

Déclencheurs de basculement et heures de

Les événements suivants déclenchent le basculement dans une paire à haute disponibilité Firepower :

- Plus de 50 % des instances Snort sur l'unité active sont en panne.
- L'espace disque de l'unité active est plein à plus de 90 %.
- La commande **no failover active** est exécutée sur l'unité active ou la commande **failover active** est exécutée sur l'unité de secours.
- L'unité active comporte plus d'interfaces défaillantes que l'unité en veille.
- La défaillance d'interface sur le périphérique actif dépasse le seuil configuré.

  Par défaut, la défaillance d'une seule interface entraîne le basculement. Vous pouvez modifier la valeur par défaut en configurant un seuil pour le nombre d'interfaces ou un pourcentage d'interfaces surveillées qui doivent échouer pour que le basculement se produise. Si le seuil est dépassé sur le périphérique actif, le basculement se produit. Si le seuil est dépassé sur le périphérique en veille, l'unité passe à l'état **Fail** (échec).

  Pour modifier les critères de basculement par défaut, saisissez la commande suivante en mode de configuration globale :

Tableau 1 :

Commande	Objectif
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	Modifie les critères de basculement par défaut. Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 250. Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.

Le tableau suivant présente les événements déclencheurs de basculement et la synchronisation de détection des défaillances. En cas de basculement, vous pouvez afficher la raison du basculement dans le centre de

messages, ainsi que les diverses opérations relatives à la paire à haute disponibilité. Vous pouvez configurer ces seuils sur une valeur comprise dans la plage minimale et maximale spécifiée.

Tableau 2 : Défense contre les menaces Heures de basculement de l'

Événement déclenchant la de basculement	Minimum	Par défaut	Maximum
L'unité active n'est plus alimentée, le matériel tombe en panne, le logiciel est rechargé ou se bloque. Lorsque l'un de ces événements se produit, les interfaces surveillées ou le lien de basculement ne reçoivent aucun message Hello.	800 milliseconde	15 secondes	45 secondes
Lien physique de l'interface de la unité active en panne.	500 millisecondes	5 secondes	15 secondes
L'interface de l'unité active est active, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un appareil de défense contre les menaces de secours pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, l'unité en veille devient l'unité active.

Rôles principal/secondaire et état actif/de secours

Lors de la configuration du basculement entre actif/veille, vous configurez une unité comme principale et l'autre comme secondaire. Lors de la configuration, les politiques de l'unité principale sont synchronisées avec celles de l'unité secondaire. À ce stade, les deux unités agissent comme un seul périphérique pour la configuration des périphériques et des politiques. Cependant, pour les événements, les tableaux de bord, les rapports et la surveillance de l'intégrité, ils continuent de s'afficher comme des périphériques distincts.

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité en veille, à savoir les adresses IP à utiliser et l'unité transmettant activement le trafic.

Cependant, il existe quelques différences entre les unités en fonction de l'unité principale (comme spécifié dans la configuration) et de l'unité secondaire :

- L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).
- Les adresses MAC de l'unité principale sont toujours associées aux adresses IP actives. L'exception à cette règle se produit lorsque l'unité secondaire devient active et ne peut pas obtenir les adresses MAC de l'unité principale sur la liaison de basculement. Dans ce cas, les adresses MAC des unités secondaires sont utilisées.

Détermination de l'unité active au démarrage

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue qui fonctionne déjà comme actif, elle devient l'unité de secours.

- Si une unité démarre et ne détecte pas d'homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active et l'unité secondaire devient l'unité de secours.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de secours, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 3 : Événements de basculement

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'unité active (alimentation ou matérielle)	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Aucun message Hello n'est reçu sur l'interface surveillée ou sur la liaison de basculement.
L'unité précédemment active récupère	Aucun basculement	Devient l'unité de secours	Aucune action	Aucun.
Défaillance de l'unité de secours (alimentation ou matériel)	Aucun basculement	Marquer l'unité de secours come défaillante	S.O.	Lorsque l'unité de secours est marquée comme défaillante, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Échec du la liaison de basculement pendant l'opération	Aucun basculement	Marquer la liaison de basculement comme défaillante	Marquer la liaison de basculement comme défaillante	Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active Marquer la liaison de basculement comme défaillante	Devenir active Marquer la liaison de basculement comme défaillante	Si la liaison de basculement est interrompue au démarrage, les deux unités deviennent actives.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Défaillance de l'interface sur l'unité active supérieure au seuil	Basculement	Marquer l'unité active comme défaillante	Devenir active	Aucun.

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'interface sur l'unité de secours supérieure au seuil	Aucun basculement	Aucune action	Marquer l'unité de secours come défaillante	Lorsque l'unité de secours est marquée comme en panne, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.

Optimisation de la synchronisation et de la configuration

Lorsqu'un redémarrage ou une jonction de nœud a lieu après la suspension ou la reprise du basculement, l'unité qui rejoint le nœud efface la configuration en cours. L'unité active envoie sa configuration complète à l'unité qui rejoint l'unité pour une synchronisation de configuration complète. Si la configuration de l'unité active est longue, il faut plusieurs minutes à l'unité qui se connecte pour synchroniser la configuration.

La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en phase d'adhésion correspond, l'unité en cours d'adhésion ignore la synchronisation complète de la configuration et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

Directives et limites de l'optimisation de la configuration et de la synchronisation

- La fonctionnalité d'optimisation de la synchronisation de la configuration est activée par défaut sur les défense contre les menaces version 7.2 et ultérieures.
- défense contre les menaces le mode de contexte multiple prend en charge la fonctionnalité d'optimisation de la configuration-synchronisation en partageant l'ordre des contextes lors de la synchronisation complète de la configuration, ce qui permet la comparaison de l'ordre des contextes lors de la jonction de nœuds suivante.
- Si vous configurez la phrase secrète et la clé IPsec de basculement, l'optimisation de la synchronisation de la configuration n'est pas effective, car la valeur de hachage calculée dans l'unité active et l'unité de secours est différente.
- Si vous configurez le périphérique avec une liste de contrôle d'accès dynamique ou SNMPv3, la fonctionnalité d'optimisation de la configuration et de la synchronisation n'est pas effective.
- L'unité active synchronise la configuration complète avec le basculement des liaisons LAN comme comportement par défaut. Pendant les oscillations de basculement entre les unités actives et les unités en veille, la fonction d'optimisation de la configuration et de la synchronisation n'est pas déclenchée et effectue une synchronisation complète de la configuration.

Surveillance de l'optimisation de la configuration et de la synchronisation

Lorsque la fonction d'optimisation de la synchronisation et de la configuration est activée, des messages syslog sont générés pour indiquer si les valeurs de hachage calculées sur l'unité active et en cours de jonction correspondent, ne correspondent pas ou si le délai de l'opération expire. Le message syslog affiche également le temps écoulé, depuis l'envoi de la demande de hachage jusqu'au moment d'obtenir et de comparer la réponse de hachage.

Exigences et prérequis pour la haute disponibilité

Prise en charge des modèles

Cisco Secure Firewall Threat Defense

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Lignes directrices pour High Availability (haute disponibilité)

Prise en charge des modèles

- Firepower 1010 :
  - Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l’utilisation de High Availability (haute disponibilité). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. High Availability (haute disponibilité) est conçu pour empêcher le trafic de passer par l’unité en veille, mais cette fonctionnalité ne s’étend pas aux ports de commutation. Dans une configuration réseau High Availability (haute disponibilité) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d’utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser High Availability (haute disponibilité) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
  - Vous ne pouvez utiliser qu'une interface de pare-feu comme lien de basculement.

Remarque Sur les périphériques Firepower 1010 sur lesquels la version 6.5 ou ultérieure est nouvellement installée et gérés par centre de gestion version 6.5 ou ultérieure, les interfaces par défaut seront de type de port de commutation. Puisque la fonctionnalité du port de commutation n’est pas prise en charge pour le basculement, désactivez le port de commutation sur ces interfaces, effectuez un déploiement, puis créez le basculement. Pour les systèmes Firepower 1010 qui sont mis à niveau à partir de versions antérieures à 6.5, les interfaces par défaut seront les mêmes que celles de la version précédente.

- Firepower 9300 : la haute disponibilité intra-châssis n’est pas prise en charge.

- Les défense contre les menaces virtuelles sur les réseaux infonuagiques publics tels que Microsoft Azure et Amazon Web Services ne sont pas pris en charge par High Availability (haute disponibilité) standard, car une connectivité de couche 2 est requise.

Directives supplémentaires

- Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter la perte de trafic lorsque le port est dans un état bloquant, vous pouvez activer la fonctionnalité STP PortFast sur le commutateur :

  interface *interface_id* **spanning-tree portfast**

  Cette solution de contournement s'applique aux commutateurs connectés aux interfaces du mode routé et de groupe de ponts. La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- La configuration de la sécurité des ports sur les commutateurs connectés à la paire de basculement appareil de défense contre les menaces peut entraîner des problèmes de communication lors d'un basculement. Ce problème se produit lorsqu'une adresse MAC sécurisée configurée ou apprise sur un port sécurisé est déplacée vers un autre port sécurisé. Une violation est signalée par la fonctionnalité de sécurité du port du commutateur.

- Pour un tunnel High Availability (haute disponibilité) actif/en veille et un tunnel VPN IPsec, vous ne pouvez pas surveiller les unités active et en veille à l'aide de SNMP sur le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et abandonnera le trafic destiné au système NMS. Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.

- Les deux périphériques homologues passent dans un état inconnu, et la configuration à haute disponibilité échoue si vous exécutez clish sur l'un des périphériques homologues lors de la création d'une paire à haute disponibilité.

- Immédiatement après le basculement, l'adresse source des messages du journal système sera l'adresse de l'interface de basculement pendant quelques secondes.

- Pour une meilleure convergence (pendant un basculement), vous devez fermer les interfaces sur une paire à haute disponibilité qui ne sont associées à aucune configuration ou instance.

- Si vous configurez le chiffrement de basculement en mode d'évaluation, les systèmes utilisent DES pour le chiffrement. Si vous enregistrez ensuite les périphériques à l'aide d'un compte compatible avec l'exportation, ils utiliseront AES après un redémarrage. Ainsi, si un système redémarre pour une raison quelconque, y compris après l'installation d'une mise à niveau, les homologues ne pourront pas communiquer et les deux unités deviendront l'unité active. Nous vous recommandons de ne pas configurer le chiffrement avant d'avoir enregistré les périphériques. Si vous configurez cela en mode d'évaluation, nous vous recommandons de supprimer le chiffrement avant d'enregistrer les périphériques.

- Lorsque vous utilisez SNMPv3 avec basculement, si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se dupliquer sur la nouvelle unité.

- Le périphérique ne partage pas les données du moteur client SNMP avec son homologue.

- Si vous avez un très grand nombre de règles de contrôle d'accès et de NAT, la taille de la configuration peut empêcher une duplication efficace de la configuration, ce qui se traduit par le fait que l'unité de secours met trop de temps à atteindre l'état de veille. Cela peut également avoir une incidence sur votre capacité à vous connecter à l'unité de secours pendant la duplication via la console ou la session SSH. Pour améliorer les performances de duplication de la configuration, activez la validation transactionnelle pour les règles d'accès et la NAT à l'aide des commandes **asp rule-engine transactional-commit access-group** et **asp rule-engine transactional-commit nat**.
- Une unité d'une paire High Availability (haute disponibilité) qui passe en rôle de secours synchronise son horloge avec celle de l'unité active.

  Exemple :

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- Les unités de High Availability (haute disponibilité) ne synchronisent pas l'horloge de manière dynamique. Voici quelques exemples d'événements où la synchronisation a lieu :
  - Une nouvelle paire High Availability (haute disponibilité) est créée.
  - La paire High Availability (haute disponibilité) est défectueuse et recréée.
  - La communication sur la liaison de basculement a été interrompue et rétablie.
  - L' état de basculement a été modifié manuellement au niveau de l' interface de ligne de commande (CLI) à l'aide des commandes **no failover/failover** ou **configure high-availability suspend/resume** (défense contre les menaces).
- L'activation de High Availability (haute disponibilité) force la suppression de toutes les routes et leur rajout après le passage de la progression de High Availability (haute disponibilité) à l'état actif. Vous pourriez subir des pertes de connexion pendant cette phase.
- Si vous remplacez l'unité principale, vous devez définir l'unité de remplacement comme unité *secondaire* lorsque vous recréez la haute disponibilité, afin que les configurations soient reproduites de l'unité secondaire vers l'unité de remplacement. Si vous définissez l'unité de remplacement comme principale, vous écraserez accidentellement la configuration présente sur l'unité opérationnelle.
- Le déploiement de périphériques Firepower 1100 et 2100 à haute disponibilité avec des centaines d'interfaces configurées dessus peut entraîner une augmentation du délai de basculement (secondes).
- Dans la configuration High Availability (haute disponibilité), les connexions de courte durée, généralement qui utilisent le port 53, sont fermées rapidement et ne sont jamais transférées ou synchronisées de la position active à la zone en veille, il peut donc y avoir une différence dans le nombre de connexions sur les deux périphériques High Availability (haute disponibilité). C'est un comportement attendu pour les connexions de courte durée. Vous pouvez essayer de comparer les connexions qui sont de longue durée (par exemple, plus de 30 à 60 secondes).

Ajouter une paire à haute disponibilité

Lors de l'établissement d'une paire à haute disponibilité active/en veille, vous désignez l'un des périphériques comme principal et l'autre comme secondaire. Le centre de gestion déploie une configuration fusionnée sur les périphériques jumelés. En cas de conflit, le paramètre du périphérique principal est utilisé.

Remarque Le lien de basculement et le lien de basculement dynamique se trouvent dans un espace IP privé et ne sont utilisés que pour la communication entre les homologues dans une paire à haute disponibilité. Une fois la haute disponibilité établie, les liens d'interface et les paramètres de chiffrement sélectionnés ne peuvent pas être modifiés sans rompre la paire à haute disponibilité et la reconfigurer.

Mise en garde La création ou la rupture d'une paire à haute disponibilité redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Avant de commencer

Confirmez que les deux périphériques :

- Sont du même modèle.
- Ont le même nombre et les mêmes types d'interfaces.
- Se trouvent dans le même domaine et groupe.
- Ont un état d'intégrité normal et exécutent le même logiciel.
- Sont en mode routé ou transparent.

Remarque Seul le mode routé est pris en charge pour l'accès du gestionnaire à une interface de données.

- Ont la même configuration NTP. Consultez Synchronisation du temps.
- Sont entièrement déployés sans modifications non validées.
- Ne comportent pas DHCP ou PPPoE configurés sur les interfaces.
- Pour l'accès de gestionnaire sur une interface de données :
  - Utilisez la même interface de données sur les deux périphériques pour l'accès du gestionnaire.
  - L'interface de données d'accès au gestionnaire redondante n'est pas prise en charge.

- Vous ne pouvez pas utiliser DHCP; seule une adresse IP statique est prise en charge. Les fonctionnalités qui reposent sur DHCP ne peuvent pas être utilisées, y compris DDNS et le provisionnement à faible intervention.
- Avoir différentes adresses IP statiques dans le même sous-réseau.
- Utilisez IPv4 ou IPv6; vous ne pouvez pas définir les deux.
- Utilisez la même configuration de gestionnaire (commande**configure manager add** pour vous assurer que la connectivité est la même.
- Vous ne pouvez pas utiliser l'interface de données comme lien de basculement ou de lien d'état.

Remarque La formation de la haute disponibilité est possible entre les deux périphériques défense contre les menaces lorsque le certificat disponible sur le périphérique principal n'est pas présent sur le périphérique secondaire. Lorsque la haute disponibilité est formée, le certificat est synchronisé sur le périphérique secondaire.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventory** (Inventaire).

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique que vous souhaitez établir comme appareil principal.

Étape 4 Dans le volet **Management** (gestion), cliquez sur **High Availability** (haute disponibilité).

Étape 5 Saisissez un **nom** d'affichage pour la paire à haute disponibilité.

Étape 6 Sous **Type de périphérique**, choisissez **Firepower Threat Defense**.

Étape 7 Choisissez le périphérique **homologue principal** pour la paire à haute disponibilité.

Étape 8 Choisissez le périphérique **homologue secondaire** pour la paire à haute disponibilité.

Remarque Dans le déploiement à distance, les périphériques apparaissant dans la liste **des homologues secondaires** dépendent du périphérique actif sélectionné dans la liste des **homologues principaux** :

- Si l'homologue principal sélectionné utilise une interface de données pour la gestion, seuls les périphériques gérés de l'interface de données sont répertoriés dans la liste d'homologues secondaire.
- Si l'interface de gestion des données de l'homologue principal est dotée d'une adresse IPv4, l'homologue secondaire répertorie uniquement les périphériques gérés de l'interface de données qui ont une adresse IPv4 configurée. La même règle s'applique aux périphériques gérés par IPv6.
- Les noms d'interface de gestion des données des périphériques principaux et secondaires doivent être identiques. Les périphériques portant des noms d'interface différents ne seront pas répertoriés dans la liste des homologues secondaires.

Étape 9 Cliquez sur **Continue** (Continuer).

Étape 10 Sous **LAN Failover Link** (Lien de basculement LAN), choisissez une **interface** avec une bande passante suffisante à réserver pour les communications de basculement.

Remarque Seules les interfaces qui n'ont pas de nom logique, qui n'appartient à aucune zone de sécurité et qui ne sont pas utilisées pour le traitement du trafic de gestion seront répertoriées dans la liste déroulante **Interface** de la boîte de dialogue **Add High Availability pair** (ajouter une paire à haute disponibilité).

Étape 11 Saisissez un **nom logique** d'identification .

Étape 12 Saisissez une adresse **IP principale** pour le lien de basculement sur l'unité active.

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254 ou /31) avec seulement deux adresses IP.

Remarque 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne et ne peuvent pas être utilisés pour le basculement ou les liens d'état.

Étape 13 Vous pouvez également choisir **Use IPv6 Address**(utiliser l'adresse IPv6).

Étape 14 Saisissez une adresse **IP secondaire** pour le lien de basculement sur l'unité de secours. Les adresses doivent provenir du même sous-réseau que l'adresse IP de l'interface.

Étape 15 Si des adresses IPv4 sont utilisées, saisissez un **masque de sous-réseau** qui s'applique aux adresses IP principale et secondaire.

Étape 16 Vous pouvez également choisir la même **interface** sous **Stateful Failover Link** (Lien de basculement avec état), ou choisir une interface différente et saisir les informations de configuration à haute disponibilité.

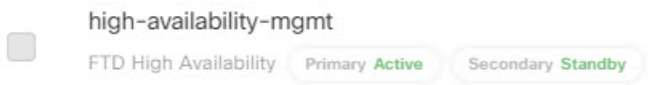
Ce sous-réseau peut être de 31 bits (255.255.255.254 ou /31) avec seulement deux adresses IP.

Remarque 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne et ne peuvent pas être utilisés pour le basculement ou les liens d'état.

Étape 17 Choisissez **Enabled** (activé) et choisissez la méthode de **génération de clé** pour le chiffrement IPsec entre les liens de basculement.

Étape 18 Cliquez sur **OK**. Ce processus prend quelques minutes car le processus synchronise les données système.

Après une configuration réussie, vous pouvez voir l'étiquette **FTD à haute disponibilité** sur le nœud défense contre les menaces dans la page **Inventory** (inventaire) CDO. Sélectionnez le nœud pour voir les périphériques actifs et en veille que vous avez configurés pour la haute disponibilité



.

Prochaine étape

Sauvegardez les périphériques. Vous pouvez utiliser la sauvegarde pour remplacer rapidement les périphériques en cas de défaillance et pour restaurer le service à haute disponibilité sans être dissocié de centre de gestion.

Configurer les paramètres facultatifs de haute disponibilité

Vous pouvez consulter la configuration à haute disponibilité initiale sur le centre de gestion. Vous ne pouvez pas modifier ces paramètres sans rompre la paire à haute disponibilité, puis la rétablir.

Vous pouvez modifier les critères de déclenchement du basculement pour améliorer les résultats de ce dernier. La surveillance des interfaces vous permet de déterminer quelles interfaces sont les mieux adaptées pour le basculement.

Configurer les adresses IP de secours et la surveillance de l'interface

Pour chaque interface, définissez une adresse IP de secours. Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

Par défaut, la surveillance est activée sur toutes les interfaces physiques et, pour le périphérique Firepower 1010, toutes les interfaces VLAN, sur lesquelles les noms logiques sont configurés. Vous pourriez souhaiter empêcher les interfaces connectées à des réseaux moins critiques d'affecter votre politique de basculement. Les ports de commutation Firepower 1010 ne sont pas admissibles à la surveillance d'interface.

Procédure

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

Étape 2 En regard de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Edit** (✎).

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

Étape 3 Cliquez sur l'onglet **High Availability** (haute disponibilité).

Étape 4 Dans la zone **Monitored Interfaces** (interfaces surveillées), cliquez sur le bouton **Edit** (✎) à côté de l'interface que vous souhaitez modifier.

Étape 5 Cochez la case **Monitor this interface for failures** (surveillance de cette interface pour détecter les défaillances).

Étape 6 Dans l'onglet **IPv4**, entrez **l'adresse IP de secours**.

Cette adresse doit être une adresse libre sur le même réseau que l'adresse IP active.

Étape 7 Si vous avez configuré l'adresse IPv6 manuellement, dans l'onglet **IPv6**, cliquez sur **Edit** (✎) à côté de l'adresse IP active, saisissez l'**adresse IP de secours**, puis cliquez sur **OK**.

Cette adresse doit être une adresse libre sur le même réseau que l'adresse IP active. Pour les adresses EUI 64 générées automatiquement et les adresses **Enforce EUI 64** (Appliquer EUI 64), l'adresse de secours est générée automatiquement.

Étape 8 Cliquez sur **OK**.

Modifier les critères de basculement haute disponibilité

Vous pouvez personnaliser les critères de basculement en fonction de votre déploiement réseau.

Procédure

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

Étape 2 En regard de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Edit** ( ).

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

Étape 3 Choisissez **High Availability** (haute disponibilité).

Étape 4 À côté de **Failover Trigger Criteria** (critères de déclenchement du basculement), cliquez sur **Edit** ( ).

Étape 5 Sous **Interface Failure Threshold** (seuil de défaillance de l'interface), choisissez le nombre ou le pourcentage d'interfaces qui doivent basculer avant le basculement du périphérique.

Étape 6 Sous **Hello packet Intervals** (Intervalles des paquets Hello), choisissez la fréquence d'envoi des paquets Hello sur le lien de basculement.

Remarque Si vous utilisez le VPN d'accès à distance sur la Firepower 2100, utilisez les intervalles par défaut des paquets Hello. Sinon, vous pourriez constater une utilisation élevée du processeur qui peut entraîner un basculement.

Étape 7 Cliquez sur **OK**.

Configurer des adresses MAC virtuelles

Vous pouvez configurer des adresses MAC actives et de secours pour le basculement en utilisant les méthodes suivantes dans Cisco Secure Firewall Management Center :

- sous l'onglet **Advanced** (Avancé) de la page de modification de l'**interface**, lors de la configuration de l'interface; voir Configurer l'adresse MAC.
- Dans la boîte de dialogue **Add Interface MAC Address** (ajouter une adresse MAC d'interface), accessible à partir de la page **High Availability** (haute disponibilité); Consultez cette procédure.

Remarque Pour configurer l'adresse MAC dans les unités principale et secondaire (de sorte que l'adresse MAC soit transférée à toutes les sous-interfaces des deux unités à haute disponibilité), l'approche recommandée est d'utiliser l'onglet **Interfaces** pour reproduire les adresses MAC sur les sous-interfaces sur des unités à haute disponibilité actives et de secours.

Si vous configurez des adresses MAC active et de secours dans les deux emplacements, les adresses définies lors de la configuration de l'interface prévalent pour le basculement.

Vous pouvez minimiser la perte de trafic pendant le basculement en désignant des adresses MAC active et de secours pour l'interface physique. Cette fonctionnalité offre une redondance par rapport au mappage des adresses IP pour le basculement.

Procédure

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

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

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

Étape 3 Cliquez sur **Haute disponibilité**.

Étape 4 Cliquez sur l'icône **Ajouter** ( ) à côté des adresses MAC d'interface.

Étape 5 Choisissez une **interface physique**.

Étape 6 Saisissez **l'adresse Mac de l'interface active**.

Étape 7 Saisissez **l'adresse Mac de l'interface en veille**.

Étape 8 Cliquez sur **OK**.

Remarque Pour en savoir plus, consultez les étapes 10 à 14 de la tâche 2, dans Configure la haute disponibilité FTD sur les périphériques Firepower.

.

Gérer High Availability (haute disponibilité)

Cette section décrit comment gérer les unités High Availability (haute disponibilité) après avoir activé High Availability (haute disponibilité), y compris comment modifier la configuration High Availability (haute disponibilité) et comment forcer le basculement d'une unité à une autre.

Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces

Après avoir établi la paire de haute disponibilité défense contre les menaces , vous pouvez permuter manuellement entre les unités active et de secours, forçant ainsi le basculement pour des raisons telles qu'une défaillance persistante ou des événements d'intégrité sur l'unité active actuelle. Les deux unités doivent être entièrement déployées avant de terminer cette procédure.

Avant de commencer

Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces, à la page 27. Cela garantit que l'état de la paire de périphériques à haute disponibilité défense contre les menaces est synchronisé avec celui de centre de gestion.

Procédure

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

Étape 2 À côté de la paire à haute disponibilité pour laquelle vous souhaitez changer d'homologue actif, cliquez sur l'icône **Switch Active Peer** (Permuter l'homologue actif).

Étape 3 Vous pouvez réaliser les actions suivantes :

- Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.
- Cliquez sur **No** (non) pour annuler et revenir à la page Device Management (gestion des périphériques).

Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces

Chaque fois que des périphériques actifs ou en veille de la paire à haute disponibilité défense contre les menaces sont redémarrés, centre de gestion peut ne pas afficher l'état de disponibilité précis pour l'un ou l'autre des périphériques. En effet, lorsque le périphérique redémarre, l'état de haute disponibilité est immédiatement mis à jour sur le périphérique et l'événement correspondant est envoyé à centre de gestion. Cependant, l'état peut ne pas être mis à jour sur le centre de gestion, car la communication entre le périphérique et le centre de gestion n'est pas encore établie.

Les défaillances de communication ou la faible communication entre centre de gestion et les périphériques peuvent entraîner une désynchronisation des données. Lorsque vous changez de périphérique actif et de périphérique en veille dans une paire à haute disponibilité, le changement peut ne pas être reflété dans centre de gestion, même après un certain temps.

Dans ces scénarios, vous pouvez actualiser l'état du nœud à haute disponibilité pour obtenir des informations précises sur les périphériques actif et en veille dans une paire à haute disponibilité.

Procédure

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

Étape 2 À côté de la paire à haute disponibilité pour laquelle vous souhaitez actualiser l'état du nœud, cliquez sur **Refresh HA Node Status** (actualisation de l'état du nœud à haute disponibilité).

Étape 3 Cliquez sur **Yes** (oui) pour actualiser l'état du nœud.

Suspendre et reprendre la haute disponibilité

Vous pouvez suspendre une unité dans une paire à haute disponibilité, ce qui est utile dans les cas suivants :

- Les deux unités sont dans une situation active-active, et la correction de la communication sur la liaison de basculement ne résout pas le problème.
- Vous souhaitez effectuer le dépannage d'une unité active ou en veille et que vous ne souhaitez pas que les unités basculent pendant ce temps.

Lorsque vous suspendez la haute disponibilité, le périphérique actuellement actif reste actif et gère toutes les connexions d'utilisateur. Cependant, les critères de basculement ne sont plus surveillés et le système ne basculera jamais sur le périphérique maintenant en pseudo-veille.

le différence clé entre la suspension de la haute disponibilité et l'arrêt de la haute disponibilité est que sur un périphérique à haute disponibilité interrompu, la configuration de haute disponibilité est conservée. Lorsque vous annulez la haute disponibilité, la configuration est effacée. Ainsi, vous avez la possibilité de rétablir la haute disponibilité sur un système interrompu, ce qui active la configuration existante et fait fonctionner les deux périphériques à nouveau comme paire de basculement.

Pour suspendre la haute disponibilité, utilisez la commande **configure high-availability suspend**.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

Si vous suspendez la haute disponibilité sur l'unité active, la configuration est suspendue sur l'unité active et l'unité de secours (en veille). La configuration de l'interface de l'unité de secours est également effacée. Si vous la suspendez sur l'unité en veille, elle est suspendue sur l'unité en veille uniquement, mais l'unité active ne tentera pas de basculer vers une unité suspendue.

Pour reprendre le basculement, utilisez la commande **configure high-availability resume**.

```
> configure high-availability resume
Successfully resumed high-availablity.
```

Vous pouvez reprendre une unité uniquement si elle est à l'état Suspended (Suspendu). L'unité négociera l'état actif/en veille avec l'unité homologue.

Remarque La suspension de la haute disponibilité est un état temporaire. Si vous rechargez une unité, elle reprend automatiquement la configuration de haute disponibilité et négocie l'état actif/en veille avec l'homologue.

Remplacement d'une unité dans la paire Défense contre les menaces à haute disponibilité

Pour remplacer une unité défaillante dans la paire défense contre les menaces à haute disponibilité à l'aide d'un fichier de sauvegarde, consultez *Restauration des Centre de gestion et des périphériques gérés* dans le Guide d'administration Cisco Secure Firewall Management Center.

Si vous n'avez pas de sauvegarde du périphérique en panne, vous devez interrompre la haute disponibilité. Enregistrez ensuite le périphérique de remplacement dans Cisco Secure Firewall Management Center et rétablissez la haute disponibilité. Le processus varie selon qu'il s'agisse du périphérique principal ou secondaire :

- Remplacer une unité principale Défense contre les menaces à haute disponibilité par aucune unité de sauvegarde, à la page 29
- Remplacer une unité Défense contre les menaces secondaire à haute disponibilité sans sauvegarde, à la page 29

Remplacer une unité principale Défense contre les menaces à haute disponibilité par aucune unité de sauvegarde

Suivez les étapes ci-dessous pour remplacer une unité principale défaillante dans la défense contre les menaces paire à haute disponibilité. Si vous ne suivez pas ces étapes, vous risquez de détruire la configuration de haute disponibilité existante.

Mise en garde La création ou la rupture de la paire à haute disponibilité défense contre les menaces redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Mise en garde Ne déplacez jamais un disque d'un capteur ou de centre de gestion vers un autre périphérique sans récréer l'image du disque. Il s'agit d'une configuration non prise en charge et peut entraîner une défaillance de la fonctionnalité.

Procédure

Étape 1 Choisissez **Force Break** (forcer la rupture) pour séparer la paire à haute disponibilité; voir Rompre une paire à haute disponibilité, à la page 30.

Remarque L'opération de rupture supprime toute la configuration liée à la haute disponibilité de défense contre les menaces et centre de gestion, et vous devez la recréer manuellement ultérieurement. Pour configurer avec succès la même paire à haute disponibilité, veillez à enregistrer les adresses IP, les adresses MAC et la configuration de surveillance de toutes les interfaces/sous-interfaces avant d'exécuter l'opération d'interruption de la haute disponibilité.

Étape 2 Désinscrire le périphérique défense contre les menaces principal défaillant de centre de gestion.

Étape 3 Enregistrez le défense contre les menaces de remplacement dans le centre de gestionConditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Configurer la haute disponibilité en utilisant l'unité secondaire/active existante comme appareil principal et le périphérique de remplacement comme appareil secondaire ou de secours lors de l'enregistrement. voir Ajouter une paire à haute disponibilité, à la page 21.

Remplacer une unité Défense contre les menaces secondaire à haute disponibilité sans sauvegarde

Suivez les étapes ci-dessous pour remplacer l'unité secondaire défaillante de la paire défense contre les menaces à haute disponibilité.

Mise en garde La création ou la rupture de la paire à haute disponibilité défense contre les menaces redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Procédure

Étape 1 Choisissez **Force Break** (forcer la rupture) pour séparer la paire à haute disponibilité; voir Rompre une paire à haute disponibilité, à la page 30.

Remarque L'opération de rupture supprime toute la configuration liée à la haute disponibilité de défense contre les menaces et centre de gestion, et vous devez la recréer manuellement ultérieurement. Pour configurer avec succès la même paire à haute disponibilité, veillez à enregistrer les adresses IP, les adresses MAC et la configuration de surveillance de toutes les interfaces/sous-interfaces avant d'exécuter l'opération d'interruption de la haute disponibilité.

Étape 2 Annulez l'enregistrement du périphérique défense contre les menaces secondaire du centre de gestion.

Étape 3 Enregistrez le défense contre les menaces de remplacement dans le centre de gestionConditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Configurez la haute disponibilité en utilisant l'unité principale/active existante comme appareil principal et le périphérique de remplacement comme appareil secondaire/de secours lors de l'enregistrement. voir Ajouter une paire à haute disponibilité, à la page 21.

Rompre une paire à haute disponibilité

Lorsque vous rompez une paire à haute disponibilité, la configuration à haute disponibilité est supprimée des deux unités.

l'unité active reste active et transmet le trafic. La configuration de l'interface de l'unité de secours est effacée.

Les politiques qui n'ont pas été déployées sur l'unité active avant l'opération d'interruption demeurent non déployées après la fin de l'opération d'interruption. Déployez les politiques sur le périphérique autonome une fois l'opération d'interruption terminée.

Remarque Si vous ne pouvez pas atteindre la paire à haute disponibilité à l'aide de centre de gestion, connectez-vous à l'interface de ligne de commande sur chaque périphérique et saisissez **configure high-availability disable** pour interrompre manuellement la haute disponibilité. Consultez aussi Remove (Désenregistrer (Supprimer)) une paire à haute disponibilité , à la page 31.

Mise en garde La rupture de la paire défense contre les menaces à haute disponibilité redémarre immédiatement le processus Snort sur les unités principale et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Avant de commencer

- Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces, à la page 27. Cela garantit que l'état de la paire à haute disponibilité est synchronisé avec l'état de centre de gestion.

Procédure

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

Étape 2 Cliquez sur **Rompre** la paire à haute disponibilité à côté de la paire à haute disponibilité que vous souhaitez rompre.

Étape 3 Si l'homologue en attente ne répond pas, cochez **Forcer la rupture**.

Étape 4 Cliquez sur **Yes** (Oui).

L'opération Rupture supprime la configuration à haute disponibilité des unités active et de secours.

Une politique FlexConfig déployée sur l'unité active peut indiquer un échec de déploiement après l'opération d'interruption de la haute disponibilité. Vous devez modifier et redéployer la politique FlexConfig sur l'unité active.

Prochaine étape

Si vous utilisez une politique FlexConfig sur l'unité active, modifiez et déployez la politique FlexConfig pour éliminer les erreurs de déploiement.

Remove (Désenregistrer (Supprimer)) une paire à haute disponibilité

Vous pouvez annuler l'enregistrement de la paire à partir de centre de gestion, ce qui conserve la paire à haute disponibilité inchangée. Vous pouvez annuler l'enregistrement de la paire si vous souhaitez l'enregistrer à un nouveau centre de gestion ou si centre de gestion ne peut plus atteindre la paire.

Pour annuler l'enregistrement d'une paire à haute disponibilité :

- Rompre toutes les communications entre centre de gestion et la paire.
- Supprime la paire de la page **Device Management** (gestion des périphériques).
- Retourne la paire à la gestion de l'heure locale si la politique de paramètres de plateforme de la paire est configurée pour recevoir l'heure de centre de gestion au moyen de NTP.
- Laisse la configuration inchangée afin que la paire 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.

Le fait d'enregistrer de nouveau la paire sur le même ou un autre centre de gestion entraîne la suppression de la configuration, de sorte que la paire cessera de traiter le trafic à ce stade; la configuration à haute disponibilité reste inchangée, vous pouvez donc ajouter la paire 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 au niveau de l'interface de ligne de commande à l'unité principale.

Procédure

Étape 1 Connectez-vous à CDO et cliquez sur **Inventory** (inventaire).

Étape 2 Cliquez sur l'onglet **FTD** et localisez la paire à haute disponibilité que vous souhaitez annuler. Sélectionnez-la pour que la ligne du périphérique soit mise en surbrillance.

Étape 3 Dans le volet **Device Actions** (Actions du périphérique) situé à droite, cliquez sur **Delete** (Supprimer).

Étape 4 Lorsque vous y êtes invité, sélectionnez **OK** pour confirmer la suppression du périphérique sélectionné.

Surveillance de High Availability (haute disponibilité)

Cette section vous permet de surveiller l'état de High Availability (haute disponibilité).

Afficher l'historique du basculement

Vous pouvez afficher l'historique de basculement des deux périphériques à haute disponibilité dans un seul écran. L'historique s'affiche par ordre chronologique et comprend la raison de tout basculement.

Procédure

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

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

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

Étape 3 Choisissez **Summary**(résumé).

Étape 4 Sous Général, cliquez sur **Afficher** ( ).

Statistiques de basculement avec état

Vous pouvez afficher les statistiques de la liaison de basculement dynamique des périphériques principaux et secondaires dans la paire à haute disponibilité.

Procédure

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

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

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

Étape 3 Choisissez **High Availability** (haute disponibilité).

Étape 4 Sous liaison de basculement dynamique, cliquez sur **Afficher** ( ).

Étape 5 Choisissez un périphérique pour afficher les statistiques.

Dépannage de la rupture de la haute disponibilité dans le déploiement d'une succursale distante

Cette section décrit comment résoudre certains des problèmes courants que vous pouvez rencontrer lors de la rupture d'une paire à haute disponibilité dans un déploiement à distance.

- Les deux unités sont à l'état actif-actif.
- Le périphérique principal ou secondaire a perdu la connectivité avec CDO et la liaison de basculement est devenue non opérationnelle.
- Le périphérique secondaire est en état de défaillance ou désactivé et a perdu la connectivité avec CDO.

Comment rompre une paire à haute disponibilité à l'état actif-actif

Les deux unités d'un déploiement distant sont dans un état actif-actif, car l'interface de basculement n'est plus opérationnelle et elles ont cessé de recevoir de réponse sur leurs interfaces de données. Dans ce cas, les deux unités utilisent l'adresse IP active sur leur interface de gestion des données, ce qui entraîne un réseau instable entre les unités et CDO.

Vous pouvez déterminer si les unités sont les deux en mode actif en vous connectant à l'interface de ligne de commande du périphérique et en utilisant la commande « show Failover state » sur les deux unités. L'état du périphérique des deux unités indique « actif », et la même adresse IP active est attribuée aux deux unités.

Remarque Vous pouvez essayer de rectifier l'interface de basculement pour restaurer la communication entre les deux homologues, puis effectuer l'opération **Forcer la rupture**.

Si vous ne pouvez pas résoudre les problèmes de connectivité de l'interface de basculement, procédez comme suit :

Procédure

Étape 1 Parmi les deux unités, identifiez un périphérique que vous souhaitez supprimer du réseau.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique identifié, soit à partir du port de console ou à l'aide de SSH.

Étape 3 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 4 Saisissez la commande **pmtool disablebyid sftunnel**.

Remarque Utilisez les commandes **pmtool** uniquement sous la direction du centre d'assistance technique de Cisco.

Étape 5 Déconnectez toutes les interfaces du périphérique que vous souhaitez supprimer du réseau.

Étape 6 Saisissez la commande **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip_address* **interface***interface_id*.

Dans *ip_address,* spécifiez l'adresse IP du périphérique en veille.

Exemple:

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully..!!
```

Étape 7 Saisissez **configure high-availability suspend** pour suspendre la haute disponibilité.

```
configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

Étape 8 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 9 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 10 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 11 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 12 Choisissez **Device** (Périphérique) > **Device Management (gestion des périphériques)**.

Étape 13 À côté de la paire à haute disponibilité où vous souhaitez séparer la paire à haute disponibilité, cliquez sur **Forcer la rupture**.

Un message s'affiche pour indiquer que la paire à haute disponibilité a été séparée avec succès.

Étape 14 Connectez toutes les interfaces au périphérique.

Étape 15 Au niveau de l'interface de ligne de commande FTD, saisissez **pmtool enablebyId sftunnel**.

Le périphérique de défense contre les menaces établit sa connexion avec CDO après un délai.

Remarque Cela peut prendre jusqu'à 5 minutes au périphérique pour établir la communication avec CDO.

Étape 16 Saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

```
sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Wed Feb 9 09:21:57 2020 UTC
Last disconnect time : Wed Feb 9 09:19:09 2020 UTC
```

Étape 17 Choisissez **Déployer** > **Déploiement** pour déployer les modifications.

Avant de déployer les modifications, CDO détecte les différences de configuration et arrête le déploiement. CDO détecte le changement d'adresse IP apporté au périphérique en dehors de l'orchestrateur de défense.

Étape 18 Synchroniser les modifications de l'interface avec CDO. Consultez Synchroniser les modifications apportées à l'interface avec le Centre de gestion.

Étape 19 Vous pouvez maintenant déployer les modifications en attente sur le périphérique. Consultez Déployer les changements de configuration..

Le périphérique devient maintenant un périphérique autonome avec une nouvelle adresse IP du périphérique en veille.

Prochaine étape

(Facultatif) Déployez les modifications en attente sur l'autre périphérique ayant l'adresse IP du périphérique actif.

Rompre une paire à haute disponibilité lorsqu'une unité active ou de secours a perdu la connexion

Problème : l'un des homologues a perdu la connectivité avec Centre de gestionet le lien de basculement est devenu non opérationnel.

Tableau 4 : Scénario :

État du périphérique principal	État du périphérique secondaire	Connectivité du périphérique principal avec CDO?	Connectivité du périphérique secondaire avec CDO?	La liaison de basculement est-elle opérationnelle? (Connectivité entre les périphériques principal et secondaire)
Actif	En veille	Oui	Non	Non
En veille	Actif	Non	Oui	Non

Solution :

Tout d'abord, vous pouvez essayer de rectifier l'interface de basculement pour rétablir la communication entre les deux homologues, puis effectuer l'opération d'interruption ou de forçage de l'interruption pour séparer les unités.

Si vous ne pouvez pas résoudre les problèmes de connectivité de l'interface de basculement, vous devez effectuer des étapes supplémentaires à l'aide de l'interface de ligne de commande du périphérique après avoir effectué une opération de rupture de la haute disponibilité.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 4 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 5 Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

Étape 6 À côté de la paire à haute disponibilité que vous souhaitez rompre, cliquez sur le bouton **Break HA** (Rompre la haute disponibilité).

Étape 7 Vous pouvez également cocher la case pour forcer l'arrêt car l'un des homologues ne répond pas.

Étape 8 Cliquez sur **Yes** (Oui).

Étape 9 Supprimez le périphérique de secours de CDO.

a) Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).
b) À côté du périphérique que vous souhaitez supprimer, cliquez sur **Delete** (Supprimer).

Étape 10 Connectez-vous à l'interface de ligne de commande du périphérique de secours, soit à partir du port de console ou à l'aide de SSH.

Étape 11 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 12 Saisissez la commande **configure manager delete**(configurer la suppression du gestionnaire) pour supprimer le gestionnaire.

Cette commande désactive le CDO actuel du gestionnaire.

Étape 13 Saisissez **configure high-availability disable** pour supprimer la configuration de basculement et désactiver l'interface de gestion des données sur le périphérique.

Étape 14 Saisissez **configure network management-data-interface**.

Exemple :

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
```

```
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

Les nouveaux paramètres réseau sont affectés au périphérique de données.

Prochaine étape

Vous pouvez intégrer le périphérique en tant qu'appareil autonome à CDO si nécessaire.

Procédure de rupture d'une paire à haute disponibilité lorsque le périphérique secondaire est en état de défaillance ou désactivé

Problème : le périphérique secondaire est en état de défaillance ou désactivé et a perdu la connectivité avec CDO. En outre, la liaison de basculement peut être opérationnelle ou non.

Tableau 5 : Scénario :

État du périphérique principal	État du périphérique secondaire	Connectivité du périphérique principal avec CDO?	Connectivité du périphérique secondaire avec CDO?	La liaison de basculement est-elle opérationnelle? (Connectivité entre les périphériques principal et secondaire)
Actif	Échec	Oui	Non	Oui ou non
Actif	Désactivé	Oui	Non	Oui ou non

Solution :

Effectuez une rupture forcée à haute disponibilité pour séparer les unités, puis utilisez l'interface de ligne de commande du périphérique pour supprimer la configuration de l'unité en veille et faire du périphérique un périphérique autonome.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 4 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 5 Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

Étape 6 À côté de la paire à haute disponibilité que vous souhaitez rompre, cliquez sur le bouton **Break HA** (Rompre la haute disponibilité).

Étape 7 Cochez la case pour forcer l'arrêt car l'un des homologues ne répond pas.

Étape 8 Cliquez sur **Yes** (Oui).

Étape 9 Supprimez le périphérique de secours de CDO.

a) Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

b) À côté du périphérique que vous souhaitez supprimer, cliquez sur **Delete** (Supprimer).

Étape 10 Connectez-vous à l'interface de ligne de commande du périphérique de secours, soit à partir du port de console ou à l'aide de SSH.

Étape 11 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 12 Saisissez **configure high-availability disable** pour supprimer la configuration de basculement et désactiver l'interface de gestion des données sur le périphérique.

Étape 13 Saisissez **configure network management-data-interface**.

Exemple :

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

Les nouveaux paramètres réseau sont affectés au périphérique de données.

Prochaine étape

Vous pouvez intégrer le périphérique en tant qu'appareil autonome à CDO si nécessaire.

Historique de la haute disponibilité

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
La désinscription d'une paire à haute disponibilité vous permet désormais de vous réinscrire sans rompre la paire	7.3	N'importe lequel	Lorsque vous supprimez (désenregistrez) une paire à haute disponibilité, vous n'avez plus besoin de rompre manuellement la paire au niveau de l'interface de ligne de commande pour réenregistrer les périphériques autonomes. Vous pouvez maintenant ajouter l'unité principale à un nouveau centre de gestion et l'unité de secours sera détectée automatiquement. Le réenregistrement de la paire effacera toujours la configuration et vos politiques devront être réappliquées.
Prise en charge de la restauration des politiques pour la haute disponibilité	7.2	N'importe lequel	La commande **configure policy rollback** est prise en charge pour la haute disponibilité.
Fonction d'optimisation Config-Sync pour un appairage haute disponibilité	7.2	N'importe lequel	La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en cours de jonction correspond, l'unité à joindre ignore la configuration de synchronisation complète et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.
Améliorations du flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité	7.1	N'importe lequel	Nous avons apporté les améliorations suivantes au flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité : • L'assistant de mise à niveau affiche désormais correctement les unités en grappe et à haute disponibilité en tant que groupes plutôt que comme périphériques individuels. Le système peut repérer, signaler et exiger à titre provisoire des correctifs pour les problèmes de groupe que vous pourriez rencontrer. Par exemple, vous ne pouvez pas mettre à niveau une grappe sur des périphériques Firepower 4100/9300 si vous avez effectué des modifications non synchronisées sur le gestionnaire de châssis Firepower. • Nous avons amélioré la vitesse et l'efficacité de la copie des paquets de mise à niveau vers les grappes et les paires à haute disponibilité. Auparavant, FMC copiait le paquet sur chaque membre du groupe dans l'ordre. Désormais, les membres du groupe peuvent se procurer le paquet dans le cadre de leur processus de synchronisation normal. • Vous pouvez désormais préciser l'ordre de mise à niveau des unités de données dans une grappe. L'unité de contrôle est toujours mise à niveau en dernier.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Effacer les routages dans un groupe ou une grappe à haute disponibilité.	7.1	N'importe lequel	Dans les versions précédentes, la commande **clear route** efface la table de routage de l'unité uniquement. Désormais, lors d'une utilisation dans un groupe ou une grappe à haute disponibilité, la commande est disponible sur l'unité active ou de contrôle uniquement et efface la table de routage sur toutes les unités du groupe ou de la grappe.

Renforcement renforcé de la disponibilité élevée de FTD	6.2.3	N'importe lequel	La version 6.2.3 introduit les fonctionnalités suivantes pour les périphériques FTD en haute disponibilité :
			• Chaque fois que des périphériques actifs ou en veille du FTD dans une paire à haute disponibilité redémarrent, le FMC peut ne pas afficher l'état de disponibilité élevé précis pour l'un ou l'autre des périphériques gérés. Cependant, l'état peut ne pas être mis à niveau sur le FMC, car la communication entre le périphérique et le FMC n'est pas encore établie. L'option **Refresh Node Status** (actualiser l'état du nœud) sur la page **Devices** – **Device Management (gestion des périphériques)** vous permet d'actualiser l'état de l'unité à haute disponibilité pour obtenir des renseignements précis sur les périphériques actif et en veille dans une paire à haute disponibilité.
			• La page **Devices** (périphériques) – **Device Management** (gestion des périphériques) de l'interface utilisateur de FMC comporte une nouvelle icône **Switch Active Peer** (Changer d'homologue actif).
			• La version 6.2.3 comprend un nouvel objet d'API REST, les **services de paires de périphériques à haute disponibilité**, qui contient quatre fonctions :
			  • **DELETE ftddevicehapairs**
			  • **PUT ftddevicehapairs**
			  • **POST ftddevicehapairs**
			  • **GET ftddevicehapairs**

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.