Haute disponibilité (basculement)

Les rubriques suivantes décrivent comment configurer et gérer le basculement actif/de secours pour atteindre la haute disponibilité du système Firewall Threat Defense.

À propos de la haute disponibilité (basculement)

Une configuration à haute disponibilité ou de basculement joint deux périphériques de sorte que si le périphérique principal tombe en panne, le périphérique secondaire peut prendre le relais. Cela vous aide à garder votre réseau opérationnel en cas de défaillance d'un périphérique.

La configuration de la haute disponibilité nécessite deux périphériques Cisco Firewall Threat Defense identiques connectés l'un à l'autre par un lien de basculement dédié et, éventuellement, un lien d'état. Les deux unités communiquent en permanence sur le lien de basculement pour déterminer l'état de fonctionnement de chacune d'elles et pour synchroniser les modifications de configuration déployées. Le système utilise le lien d'état pour transmettre les informations d'état de connexion au périphérique de secours, de sorte que si un basculement se produit, les connexions des utilisateurs sont conservées.

Les unités forment une paire active/en veille, où l'unité principale 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.

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, l'unité active bascule vers l'unité en veille, qui devient alors active.

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un Firewall Threat Defense 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

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 1 : 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	Politique	Action de l'unité active	Action de l'unité de secours	Notes
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 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.

Liens de basculement et de basculement avec état

Le lien de basculement est une connexion dédiée entre les deux unités. Le lien de basculement avec état est également une connexion dédiée, mais vous pouvez soit utiliser le lien de basculement comme lien de basculement/avec état combiné, soit créer un lien d'état dédié distinct. Si vous utilisez uniquement le lien de basculement, les informations sur l'état passent également par ce lien; vous ne perdez pas la capacité de basculement avec état.

Par défaut, les communications sur les liens de basculement et de basculement avec état sont en texte brut (non chiffré). Vous pouvez chiffrer les communications pour une sécurité renforcée en configurant une clé de chiffrement IPsec.

Les rubriques suivantes expliquent ces interfaces plus en détail et comprennent des recommandations sur la façon de câbler les périphériques pour obtenir les meilleurs résultats.

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 et synchroniser les modifications de configuration.

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
- Mises à jour des bases de données du système, y compris la VDB et les règles, mais excluant les bases de données de géolocalisation et de Security Intelligence. Chaque système télécharge séparément les mises à jour de géolocalisation et de Security Intelligence. Si vous créez un calendrier de mise à jour, ceux-ci doivent rester synchronisés. Toutefois, si vous effectuez une mise à jour manuelle de géolocalisation ou de Security Intelligence sur le périphérique actif, vous devez également en faire une sur le périphérique en veille.

Remarque Les données d'événements, de rapports et du journal d'audit ne sont pas synchronisées. La visionneuse d'événements et les tableaux de bord affichent uniquement les données liées à l'unité concernée. En outre, l'historique de déploiement, l'historique des tâches et les autres événements du journal d'audit ne sont pas synchronisés.

Lien de basculement dynamique

Le système utilise la liaison d'état pour transmettre les informations d'état de connexion au périphérique de secours. Ces informations aident l'unité de secours à maintenir les connexions existantes en cas de basculement.

L'utilisation d'une liaison unique pour les liens de basculement et de basculement dynamique est la meilleure façon 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.

Interfaces pour les liens de basculement et d'état

Vous pouvez utiliser une interface de données inutilisée, mais activée (physique ou EtherChannel) comme liaison de basculement ; cependant, vous ne pouvez pas spécifier une interface actuellement configurée avec un nom. 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). Vous ne pouvez pas utiliser une interface de gestion, sous-interface, une interface VLAN ou un port de commutation pour le basculement.

L'appareil Cisco Firewall Threat Defense ne prend pas en charge le partage des interfaces entre les données utilisateur et le lien de basculement.

Consultez les consignes suivantes concernant la taille de la liaison de basculement et de l'état :

- 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.

Lorsque vous utilisez une interface EtherChannel comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec le même ID et les mêmes interfaces membres existe sur les deux appareils avant d'établir la haute disponibilité. S'il y a une incompatibilité EtherChannel, vous devez désactiver la HA, puis corriger la configuration sur l'unité secondaire avant de poursuivre. 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 des interfaces de basculement et de basculement dynamique

Vous pouvez utiliser toutes les interfaces physiques de données inutilisées comme liaison de basculement et liaison d'état dédiée facultative. Cependant, vous ne pouvez pas sélectionner une interface actuellement configurée avec un nom ou une interface qui comporte des sous-interfaces. Les interfaces de liaison de basculement et de basculement avec état ne sont pas configurées comme des interfaces réseau normales; elles existent uniquement pour la communication de basculement. Ils existent uniquement pour les communications de basculement, et vous ne pouvez pas les utiliser pour le trafic de transit ou l'accès de gestion.

Comme la configuration est synchronisée entre les périphériques, vous devez sélectionner le même numéro de port pour chaque extrémité de liaison. Par exemple, GigabitEthernet1/3 sur les deux appareils pour le lien de basculement.

Connectez le lien de basculement, et le lien d'état dédié si utilisé, 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 Cisco Firewall Threat Defense. Une liaison d'état dédiée a les mêmes exigences, mais doit se trouver sur un segment de réseau différent de celui de la liaison de basculement.

Remarque L'intérêt de l'utilisation d'un commutateur est que si l'une des interfaces de l'unité tombe en panne, il est facile de déterminer quelle interface est défaillante. Si vous utilisez une connexion directe par câble, en cas de défaillance d'une interface, la liaison est interrompue sur les deux homologues, ce qui rend difficile de déterminer quel périphérique est défectueux.

- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe. Le périphérique Cisco Firewall Threat Defense prend en charge Auto-MDI/MDIX sur ses ports Ethernet en cuivre ; vous pouvez donc utiliser un câble croisé ou un câble droit. Si vous utilisez un câble droit, l'interface détecte automatiquement le câble et échange l'une des paires de transmission/réception contre MDIX.

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 Cisco Firewall Threat Defense 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 Cisco Firewall Threat Defense, quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux périphériques deviennent actifs.Cisco Firewall Threat Defense 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

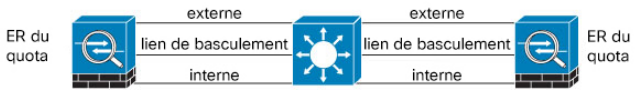
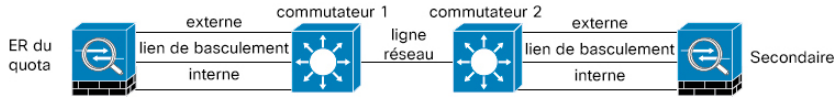


Illustration 2 : Connexion avec un double commutateur : non recommandée



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

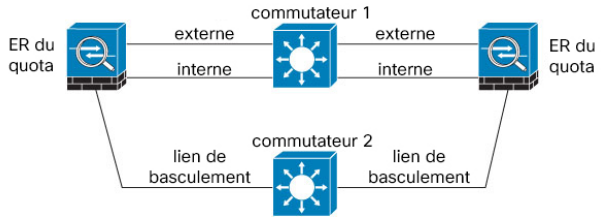
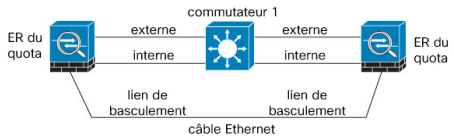


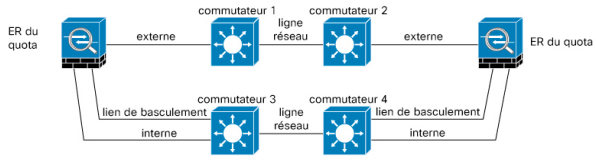
Illustration 4 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données Cisco Firewall Threat Defense 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



Incidence du basculement dynamique sur les connexions utilisateur

L'unité active partage les informations sur l'état de la connexion avec l'unité de secours. Cela signifie que l'unité de secours peut maintenir certains types de connexions sans nuire à l'utilisateur.

Cependant, il existe certains types de connexions qui ne prennent pas en charge le basculement avec état. Pour ces connexions, l'utilisateur devra rétablir la connexion en cas de basculement. Souvent, cela se produit automatiquement en fonction du comportement du protocole utilisé dans la connexion.

Les rubriques suivantes expliquent quelles fonctionnalités sont prises en charge ou non pour le basculement avec état.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis au Firewall Threat Defense 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 passif de la politique d'identité, mais pas celles recueillies lors de l'authentification active sur un portail captif.
- Décisions en matière de renseignements sur la sécurité.
- 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 le périphérique de secours.

Fonctionnalités non prises en charge

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises au Firewall Threat Defense de secours :

- Sessions dans des tunnels en texte brut comme GRE ou IP-in-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.
- Le routage de multidiffusion

Modifications de configuration et actions autorisées sur une unité de secours

Lorsque vous fonctionnez en mode de haute disponibilité, vous apportez des modifications de configuration à l'unité active uniquement. Lorsque vous déployez la configuration, les nouvelles modifications sont également transmises à l'unité de secours.

Cependant, certaines propriétés sont uniques à l'unité de secours. Vous pouvez modifier les éléments suivants sur une unité de secours :

- Adresse IP de l'interface de gestion et passerelle.
- (Interface de ligne de commande uniquement.) Le mot de passe du compte d'utilisateur admin et des autres comptes d'utilisateurs locaux. Vous pouvez effectuer cette modification dans l'interface de ligne de commande uniquement ; vous ne pouvez pas la faire dans Firepower Device Manager. Tout utilisateur local devra modifier son mot de passe sur les deux unités séparément.

En outre, les actions suivantes sont disponibles sur un périphérique de secours.

- Actions de haute disponibilité, telles que la suspension, la reprise, la réinitialisation et l'interruption de la haute disponibilité, ainsi que la commutation des modes entre actif et en veille.
- Les données de tableau de bord et d'événements sont propres à chaque périphérique et ne sont pas synchronisées. Cela inclut les affichages personnalisés dans Event Viewer (Visionneuse d'événements)
- Les informations du journal d'audit sont uniques par périphérique.
- Enregistrement de licence Smart. Cependant, vous devez activer ou désactiver les licences facultatives sur l'unité active, et l'action est synchronisée avec l'unité de secours, qui demande ou libère la licence appropriée.
- Sauvegarde, mais pas restauration. Vous devez interrompre la haute disponibilité sur l'unité pour restaurer une sauvegarde. Si la sauvegarde comprend la configuration à haute disponibilité, l'unité rejoindra le groupe à haute disponibilité.
- Installation de mise à niveau logicielle.
- Génération de journaux de dépannage.
- Mise à jour manuelle des bases de données de géolocalisation ou de Security Intelligence. Ces bases de données ne sont pas synchronisées entre les unités. Si vous créez un calendrier de mise à jour, les unités peuvent maintenir indépendamment la cohérence.
- Vous pouvez afficher les sessions utilisateur Firepower Device Manager actives et supprimer des sessions à partir de la page **Monitoring** > **Sessions** (sessions de surveillance).

Configuration requise pour la haute accessibilité

Les rubriques suivantes expliquent les exigences à respecter avant d'intégrer deux périphériques dans une configuration à haute accessibilité.

Configuration matérielle requise pour la haute disponibilité

Pour relier deux appareils dans une configuration à haute disponibilité, vous devez satisfaire aux exigences matérielles suivantes.

- Les appareils doivent être du même modèle exactement.

  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 comporte un SM-36 et un SM-44. Vous pouvez créer des paires haute disponibilité entre les modules SM-36 et entre les modules SM-44.

- Les appareils doivent avoir le même nombre et le même type d'interfaces.

  Pour le châssis Firepower 4100/9300, toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute disponibilité. Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

- Les mêmes modules doivent être installés sur les appareils. Par exemple, si l'un comporte un module d'interface réseau facultatif, vous devez installer le même module dans l'autre périphérique.

- La haute disponibilité intra-châssis pour Firepower 9300 n'est pas prise en charge. Vous ne pouvez pas configurer la haute disponibilité entre des périphériques logiques distincts sur le même châssis Firepower 9300.

Configuration logicielle requise pour la haute disponibilité

Pour relier deux appareils dans une configuration à haute disponibilité, vous devez satisfaire aux exigences logicielles suivantes.

- Les appareils doivent présenter exactement la même version de logiciel, ce qui signifie les mêmes numéros majeur (premier), mineur (deuxième) et de maintenance (troisième). Vous pouvez trouver la version dans le Firepower Device Manager sur la page **Devices (appareils)**, ou vous pouvez utiliser la commande **show version** dans l'interface de ligne de commande. Les appareils de versions différentes sont autorisés à s'associer, mais la configuration n'est pas importée dans l'unité en veille et le basculement ne fonctionne pas tant que vous ne mettez pas les unités à niveau vers la même version logicielle.

- Les deux appareils doivent être en mode gestionnaire local, c'est-à-dire configurés à l'aide de la fonction Firepower Device Manager. Si vous pouvez vous connecter au Firepower Device Manager sur les deux systèmes, ils sont en mode gestionnaire local. Vous pouvez également utiliser la commande **show managers** dans l'interface de ligne de commande pour vérifier.

- Vous devez exécuter l'assistant de configuration initiale pour chaque périphérique.

- Chaque périphérique doit avoir sa propre adresse IP de gestion. La configuration de l'interface de gestion n'est pas synchronisée entre les appareils.

- Les périphériques doivent avoir la même configuration NTP.
- Vous ne pouvez configurer aucune interface pour obtenir son adresse en utilisant DHCP. Autrement dit, toutes les interfaces doivent avoir des adresses IP statiques.
- Pour les services en nuage, les deux appareils doivent être enregistrés dans la même région ou aucun appareil ne peut être inscrit. Vous ne pouvez pas avoir des enregistrements mixtes aux services en nuage.
- Vous devez déployer toutes les modifications en attente avant de configurer la haute disponibilité.

Exigences en matière de licence pour la haute disponibilité

Avant de configurer la haute disponibilité, les unités doivent être dans le même état : soit les deux sont enregistrées avec une licence De base, soit les deux sont enregistrées dans un mode d'évaluation. Si les périphériques sont enregistrés, ils peuvent être enregistrés dans différents comptes Cisco Smart Software Manager, mais les comptes doivent avoir le même état pour le paramètre de fonctionnalité de contrôle de l'exportation : activés ou désactivés. Cependant, il importe peu que vous ayez activé ou non différentes licences facultatives sur les unités. Si vous enregistrez les deux unités, vous devez sélectionner la même région Cisco Cloud Services pour les appareils.

Si les appareils sont enregistrés, ils doivent utiliser le même mode, soit Smart License ou Permanent License Reservation (PLR).

Pendant le fonctionnement, les unités de la paire à haute disponibilité doivent avoir les mêmes licences. Toutes les modifications de licence que vous apportez à l'unité active sont répétées sur l'unité en veille pendant le déploiement.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire. Vous devez vous assurer que les licences dans votre compte sont en nombre adéquat pour s'appliquer à chaque appareil. Il est possible d'être en conformité sur un appareil, mais non sur l'autre, si le nombre de licences est insuffisant.

Par exemple, si le périphérique actif possède la licence De base et que le Menace , et le périphérique en veille ne possède que la licence De base, l'unité en veille communique avec Cisco Smart Software Manager pour obtenir un Menace disponible à partir de votre compte. Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, votre compte devient non conforme (et l'appareil en veille est non conforme même si l'appareil actif est conforme) jusqu'à ce que vous achetiez le nombre correct de licences.

Attention :

- Si vous enregistrez les appareils dans des comptes qui ont des paramètres différents pour les fonctions contrôlées à l'exportation, ou essayez de créer une paire haute accessibilité avec une unité enregistrée et l'autre en mode d'évaluation, la jonction haute accessibilité peut échouer.
- Si vous configurez une clé de chiffrement IPsec avec des paramètres incohérents pour les fonctionnalités contrôlées à l'exportation, les deux appareils deviendront actifs après l'activation de la haute accessibilité. Cela aura une incidence sur le routage des segments de réseau pris en charge, et vous devrez interrompre manuellement la haute accessibilité sur l'unité secondaire pour récupérer.
- Ne modifiez pas les licences au milieu de la création du groupe à haute disponibilité. Les deux unités doivent avoir la même configuration au moment de la jonction de la haute disponibilité, sinon vous verrez l'erreur suivante : « Échec de la validation FDM – Incompatibilité de l'état d'inscription du service en nuage entre le nœud principal et le nœud secondaire ». Veuillez consulter l'interface de ligne de commande d'historique de synchronisation d'applications pour en savoir plus.

Lignes directrices pour la haute disponibilité

Prise en charge des modèles

- Firepower 9300 : vous pouvez configurer la haute disponibilité sur le Firepower 9300. Cependant, vous ne pouvez pas configurer la haute disponibilité entre des dispositifs logiques distincts sur le même châssisFirepower 9300.
- 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.
  - Lorsque le châssis est dans une paire à haute accessibilité, le voyant DEL de l'unité en veille est ambre.
- (Série Firepower 1000, Firepower 2100)—Le déploiement de périphériques en haute disponibilité avec des centaines d'interfaces configurées peut entraîner une augmentation du délai de basculement (en secondes).
- Firewall Threat Defense Virtual : la configuration à haute disponibilité n'est pas prise en charge pour Firewall Threat Defense Virtual pour le nuage Microsoft Azure ou le nuage Amazon Web Services (AWS).

Directives supplémentaires

- 169.254.0.0/16 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.
- La configuration de l'unité active est synchronisée avec l'unité de secours lorsque vous exécutez une tâche de déploiement sur l'unité active. Cependant, certaines modifications ne s'affichent pas dans les modifications en attente, même si elles ne sont pas synchronisées sur l'unité de secours jusqu'à ce que vous déployiez les modifications. Si vous modifiez l'un des éléments suivants, les modifications sont masquées et vous devez exécuter une tâche de déploiement avant qu'elles ne soient configurées sur l'unité de secours. Si vous devez appliquer la modification immédiatement, vous devrez apporter une autre modification qui ne s'affiche pas dans les modifications en attente. Les modifications masquées comprennent la modification des éléments suivants : les planifications des mises à jour des règles, de la base de données de géolocalisation, des renseignements de sécuritéou de la VDB ; les planifications des

sauvegardes ; NTP ; Serveur mandataire HTTP pour les connexions de gestion ; droits de licence ; options des services en nuage ; options de filtrage d'URL.

- Vous devez effectuer des sauvegardes sur les unités principale et secondaire. Pour restaurer une sauvegarde, vous devez d'abord interrompre la haute disponibilité. Ne restaurez pas la même sauvegarde sur les deux unités, car elles deviendraient alors actives. Au lieu de cela, restaurez la sauvegarde sur l'unité que vous souhaitez rendre active en premier, puis restaurez la sauvegarde équivalente sur l'autre unité.
- Le bouton **Test** (Tester) pour les différentes sources d'identité fonctionne uniquement sur l'unité active. Si vous devez tester la connectivité de la source d'identité pour le périphérique en veille, vous devez d'abord changer de mode pour faire de l'homologue en veille l'homologue actif.
- La création ou l'interruption de la configuration à haute disponibilité redémarre le processus d'inspection Snort sur les deux périphériques lorsque la modification de configuration est déployée. Cela peut entraîner une perturbation du trafic jusqu'à ce que le processus soit complètement redémarré.
- Lors de la configuration initiale de la haute disponibilité, si les versions des bases de données de renseignements de sécurité et de géolocalisation sur l'unité secondaire sont différentes de celles de l'unité principale, les tâches de mise à jour des bases de données sont planifiées sur l'unité secondaire. Ces tâches sont exécutées lors du prochain déploiement à partir de l'unité active. Même si la jonction à haute disponibilité échoue, ces tâches demeurent et seront exécutées lors du prochain déploiement.
- 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 en haute disponibilité 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.
- En haute disponibilité active/en veille avec un tunnel VPN IPsec, vous ne pouvez pas superviser à la fois l'unité active et l'unité de secours au moyen de SNMP via le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et laissera tomber le trafic destiné au système de gestion de réseau (NMS). Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.
- Les interfaces que vous utilisez pour les liens de basculement à haute disponibilité et de basculement dynamique ne doivent pas être activées. L'état de l'interface devrait indiquer que la liaison est activée, mais les interfaces elles-mêmes peuvent sembler désactivées. En outre, les informations d'interface ne sont pas mises à jour avec les adresses IP définies dans la configuration de haute disponibilité.

Configuration de la haute disponibilité

Utilisez une configuration à haute disponibilité pour assurer la connectivité réseau même en cas de défaillance d'un périphérique. Avec la haute disponibilité active/en veille, deux périphériques sont liés, de sorte que, si

le périphérique actif tombe en panne, le périphérique en veille prend le relais et les utilisateurs ne devraient voir qu'un bref problème de connectivité.

La procédure suivante explique le processus de bout en bout pour configurer une paire de haute disponibilité (HA) active/en veille.

Procédure

Étape 1 Préparer les deux unités pour la haute disponibilité, à la page 14.

Étape 2 Configurer l'unité principale pour la haute disponibilité, à la page 16.

Étape 3 Configurer l'unité secondaire pour la haute disponibilité, à la page 19.

Étape 4 Configurer les critères de basculement pour la surveillance de l'intégrité, à la page 20.

Les critères comprennent la surveillance des homologues et la surveillance des interfaces. Bien que tous les critères de basculement aient des paramètres par défaut, vous devez au moins les examiner pour vérifier que les paramètres par défaut fonctionnent pour votre réseau.

- Configurer les critères de basculement de la surveillance de l'intégrité des unités homologues, à la page 21.
- Configurer les critères de basculement pour la surveillance de l'intégrité des interfaces, à la page 22.

  Pour en savoir plus sur les tests d'interface, consultez Comment le système teste l'intégrité de l'interface, à la page 24.

Étape 5 (Facultatif, mais conseillé.) Configurer les adresses IP et MAC de secours, à la page 25.

Étape 6 (Facultatif) Vérifier la High Availability Configuration (Configuration de la haute disponibilité) , à la page 26.

Préparer les deux unités pour la haute disponibilité

Il y a beaucoup de choses que vous devez préparer correctement avant de pouvoir configurer la haute disponibilité.

Procédure

Étape 1 Assurez-vous que les appareils répondent aux exigences décrites dans Configuration matérielle requise pour la haute disponibilité, à la page 10.

Étape 2 Déterminez si vous allez utiliser un seul lien de basculement ou des liens distincts de basculement et de basculement avec état, puis définissez les ports que vous utiliserez.

Vous devez utiliser le même numéro de port sur chaque périphérique pour chaque lien. Par exemple, GigabitEthernet 1/3 sur les deux appareils pour le lien de basculement. Sachez lesquels vous utiliserez afin de ne pas les utiliser accidentellement à d'autres fins. Pour en savoir plus, consultez Liens de basculement et de basculement avec état, à la page 3.

Étape 3 Installez les périphériques, connectez-les au réseau et exécutez l'assistant de configuration initiale sur chaque périphérique.

a) Passez en revue les conceptions de réseau recommandées dans Éviter le basculement interrompu et les liaisons de données, à la page 6.
b) Connectez au moins les interfaces externes, comme expliqué dans Connecter les interfaces.

   Vous pouvez également connecter les autres interfaces, mais vous devez vous assurer d'utiliser le même port sur chaque périphérique pour vous connecter à un sous-réseau donné. Comme les appareils partagent la même configuration, vous devez les connecter à vos réseaux en parallèle.

   Remarque
   L'assistant de configuration ne vous permet pas de modifier les adresses IP sur l'interface de gestion et l'interface interne. Ainsi, si vous connectez l'une de ces interfaces sur le périphérique principal avec le réseau, ne connectez pas non plus les interfaces sur le périphérique secondaire, sinon vous aurez un conflit d'adresses IP. Vous pouvez connecter directement votre poste de travail à l'une de ces interfaces et obtenir une adresse au moyen du protocole DHCP, afin de pouvoir vous connecter à Firepower Device Manager et configurer l'appareil.

c) Terminez l'assistant de configuration initiale sur chaque périphérique. Assurez-vous de spécifier des adresses IP statiques pour l'interface externe. En outre, configurez les mêmes serveurs NTP. Pour en savoir plus, consultez Compléter la configuration initiale avec l'assistant d'installation.

   Choisissez les mêmes licences et options de Cisco Success Network (Réseau de succès Cisco) pour les unités. Par exemple, le mode d'évaluation pour chacun ou l'enregistrement des appareils.

d) Sur le périphérique secondaire, sélectionnez **Device (périphérique)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)** et configurez une adresse IP unique, modifiez la passerelle si nécessaire, puis désactivez ou modifiez les paramètres du serveur DHCP selon vos besoins.
e) Sur le périphérique secondaire, sélectionnez l'interface de périphérique **Device** > **Interface** et modifiez l'interface interne. Supprimez l'adresse IP ou modifiez-la. Supprimez également le serveur DHCP défini pour l'interface, car vous ne pouvez pas avoir deux serveurs DHCP sur le même réseau.
f) Déployez la configuration sur le périphérique secondaire.
g) Si nécessaire, en fonction de votre topologie de réseau, connectez-vous au périphérique principal et modifiez l'adresse de gestion, la passerelle et les paramètres du serveur DHCP, ainsi que l'adresse IP de l'interface interne et les paramètres du serveur DHCP. Déployez la configuration si vous apportez des modifications.
h) Si vous n'avez pas connecté l'interface interne ou l'interface de gestion si vous utilisez un réseau de gestion distinct, vous pouvez maintenant les connecter aux commutateurs.

Étape 4 Vérifiez que les appareils présentent exactement la même version de logiciel, ce qui signifie les mêmes numéros majeur (premier), mineur (deuxième) et de maintenance (troisième). Vous pouvez trouver la version dans le Firepower Device Manager sur la page Devices (appareils), ou vous pouvez utiliser la commande **show version** dans l'interface de ligne de commande.

S'ils n'exécutent pas les mêmes versions de logiciel, procurez-vous la version de logiciel préférée sur Cisco.com et installez-la sur chaque appareil. Pour de plus amples renseignements, consultez la section Mise à niveau Firewall Threat Defense.

Étape 5 Connectez et configurez les liens de basculement et de basculement avec état.

a) Selon votre conception de réseau préférée (choisie depuis Éviter le basculement interrompu et les liaisons de données, à la page 6), connectez les interfaces de basculement de chaque périphérique de manière appropriée, soit avec un commutateur, soit directement les unes avec les autres.
b) Si vous utilisez un lien d'état distinct, connectez également les interfaces de basculement avec état pour chaque périphérique de manière appropriée.

c) Connectez-vous à chaque appareil à son tour et accédez à l'interface de périphérique (**Device** > **Interface**). Modifiez chaque interface et vérifiez qu'il n'y a pas de noms d'interface ou d'adresses IP configurés.

Si les interfaces sont configurées avec des noms, vous devrez peut-être les supprimer des zones de sécurité et supprimer d'autres configurations avant de pouvoir supprimer le nom. Si la suppression du nom échoue, examinez les messages d'erreur pour déterminer les autres modifications à apporter.

Étape 6 Sur le périphérique principal, connectez les interfaces de données restantes et configurez le périphérique.

a) Sélectionnez **Device** > **Interface** (interface de périphérique), modifiez chaque interface utilisée pour le trafic traversant et configurez les adresses IP statiques principales.

b) Ajoutez les interfaces aux zones de sécurité et configurez les politiques de base nécessaires pour gérer le trafic sur les réseaux connectés. Pour des exemples de configurations, consultez la liste des rubriques dans Meilleures pratiques : scénarios d'utilisation pour Firewall Threat Defense.

c) Déployez la configuration.

Étape 7 Vérifiez que vous répondez à toutes les exigences décrites dans Configuration logicielle requise pour la haute disponibilité, à la page 10.

Étape 8 Vérifiez que les licences sont cohérentes (enregistrement des appareils ou mode d'évaluation). Pour en savoir plus, consultez Exigences en matière de licence pour la haute disponibilité, à la page 11.

Étape 9 Sur le périphérique secondaire, connectez les interfaces de données restantes aux mêmes réseaux que les interfaces équivalentes sur le périphérique principal. Ne configurez pas les interfaces.

Étape 10 Sur chaque appareil, sélectionnez **Périphérique** > **Paramètres du système** > **Services en nuage** et vérifiez que vous avez les mêmes paramètres.

Vous êtes maintenant prêt à configurer la haute disponibilité sur l'appareil principal.

Configurer l'unité principale pour la haute disponibilité

Pour configurer une paire à haute disponibilité actif/en veille, vous devez d'abord configurer le périphérique principal. L'appareil principal est l'unité qui doit être active dans des circonstances normales. L'appareil secondaire reste en mode veille jusqu'à ce que l'unité principale ne soit plus disponible.

Sélectionnez le périphérique que vous souhaitez être principal, puis connectez-vous au Firepower Device Manager sur ce périphérique et suivez cette procédure.

Remarque Une fois la paire de haute disponibilité établie, vous devez rompre la paire afin de modifier la configuration décrite dans cette procédure.

Avant de commencer

Assurez-vous que les interfaces que vous configurerez pour le lien de basculement et le lien de basculement dynamique ne portent aucun nom. Si elles sont actuellement nommées, vous devez supprimer les interfaces de toutes les politiques qui les utilisent, y compris les objets de zone de sécurité, puis modifier les interfaces pour supprimer le nom. Les interfaces doivent également être en mode routé, et non en mode passif. Ces interfaces doivent être dédiées à une utilisation dans la configuration à haute disponibilité : vous ne pouvez pas les utiliser à d'autres fins.

Si des modifications sont en attente, vous devez les déployer avant de pouvoir configurer la haute disponibilité.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Dans la partie droite du résumé du périphérique, cliquez sur **Configure** (Configurer) à côté du groupe **High Availability** (Haute disponibilité).

Si vous configurez la haute disponibilité pour la première fois sur le périphérique, le groupe ressemblerait à ce qui suit.

Étape 3 Sur la page High Availability (Haute disponibilité), cliquez sur la case **Primary Device** (Périphérique principal).

Si le périphérique secondaire est déjà configuré et que vous avez copié la configuration dans le presse-papiers, vous pouvez cliquer sur le bouton **Paste from Clipboard** (Coller à partir du presse-papiers) et coller la configuration. Cela mettra à jour les champs avec les valeurs appropriées, que vous pourrez ensuite vérifier.

Étape 4 Configurez les propriétés du **Failover Link** (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 et synchroniser les modifications de configuration. Pour en savoir plus, consultez Lien de basculement, à la page 4.

- **Physical Interface** (Interface physique) : sélectionnez l'interface que vous avez connectée au périphérique secondaire pour l'utiliser comme lien de basculement. Il doit s'agir d'une interface sans nom.

  Lorsque vous utilisez une interface EtherChannel comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec le même ID et les mêmes interfaces membres existe sur les deux appareils avant d'établir la haute disponibilité. S'il y a une incompatibilité EtherChannel, vous devez désactiver la HA, puis corriger la configuration sur l'unité secondaire avant de poursuivre. 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.

- **Type** : choisissez si vous utiliserez une adresse IPv4 ou IPv6 pour l'interface. Vous ne pouvez configurer qu'un seul type d'adresse.

- **Primary IP** (IP principale) : saisissez l'adresse IP de l'interface sur ce périphérique. Par exemple, 192.168.10.1. Pour les adresses IPv6, vous devez inclure la longueur du préfixe en notation standard, par exemple, 2001:a0a:b00::a0a:b70/64.

- **Secondary IP** (IP secondaire) : saisissez l'adresse IP à configurer à l'autre extrémité du lien, sur l'interface du périphérique secondaire. L'adresse doit se trouver sur le même sous-réseau que l'adresse principale et elle doit être différente de l'adresse principale. Par exemple, 192.168.10.2 ou 2001:a0a:b00::a0a:b71/64.

- **Netmask (IPv4 only)** (Masque réseau) (IPv4 uniquement) : saisissez le masque de sous-réseau pour l'adresse IP principale/secondaire.

Étape 5 Configurez les propriétés du Stateful Failover Link (Lien de basculement dynamique).

Le système utilise la liaison d'état pour transmettre les informations d'état de connexion au périphérique de secours. Ces informations aident l'unité de secours à maintenir les connexions existantes en cas de basculement. Vous pouvez soit utiliser la même liaison que la liaison de basculement, soit configurer une liaison distincte.

- **Use the Same Interface as the Failover Link** (Utiliser la même interface que le lien de basculement) : sélectionnez cette option si vous souhaitez utiliser un lien unique pour les communications de basculement et de basculement dynamique. Si vous sélectionnez cette option, passez à l'étape suivante.
- **Physical Interface** (Interface physique) : si vous souhaitez utiliser un lien de basculement dynamique distinct, sélectionnez l'interface que vous avez connectée au périphérique secondaire pour l'utiliser comme lien de basculement dynamique. Il doit s'agir d'une interface sans nom. Configurez les propriétés suivantes :
  - **Type** : choisissez si vous utiliserez une adresse IPv4 ou IPv6 pour l'interface. Vous ne pouvez configurer qu'un seul type d'adresse.
  - **Primary IP** (IP principale) : saisissez l'adresse IP de l'interface sur ce périphérique. L'adresse doit se trouver sur un sous-réseau différent de celui utilisé pour la liaison de basculement. Par exemple, 192.168.11.1. Pour les adresses IPv6, vous devez inclure la longueur du préfixe en notation standard, par exemple, 2001:a0a:b00:a::a0a:b70/64.
  - **Secondary IP** (IP secondaire) : saisissez l'adresse IP à configurer à l'autre extrémité du lien, sur l'interface du périphérique secondaire. L'adresse doit se trouver sur le même sous-réseau que l'adresse principale et elle doit être différente de l'adresse principale. Par exemple, 192.168.11.2 ou 2001:a0a:b00:a::a0a:b71/64.
  - **Netmask (IPv4 only)** (Masque réseau) (IPv4 uniquement) : saisissez le masque de sous-réseau pour l'adresse IP principale/secondaire.

Étape 6 (Facultatif) Saisissez une chaîne de **IPsec Encryption Key** (Clé de chiffrement IPsec) si vous souhaitez chiffrer les communications entre les deux unités de la paire.

Vous devez configurer exactement la même clé sur le nœud secondaire ; notez donc la chaîne que vous saisissez.

Si vous ne saisissez pas de clé, toutes les communications sur les liens de basculement et de basculement dynamique se font en texte brut. Si vous n'utilisez pas de connexions directes par câble entre les interfaces, il peut s'agir d'un problème de sécurité.

Remarque
Si vous configurez le chiffrement du basculement HA en mode d'évaluation, le système utilise DES comme algorithme de 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.

Étape 7 Cliquez sur **Activate HA** (Activer HA).

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si vous ne voyez pas de message indiquant que votre configuration a été enregistrée et que le déploiement est en cours, faites défiler la page vers le haut pour voir les messages d'erreur.

La configuration est également copiée dans le presse-papiers. Vous pouvez utiliser la copie pour configurer rapidement l'unité secondaire. Pour plus de sécurité, la clé de chiffrement n'est pas incluse dans la copie du presse-papiers.

Une fois la configuration terminée, vous recevez un message expliquant les prochaines étapes à suivre. Cliquez sur **Got It (J'ai compris)** après avoir pris connaissance des informations.

À ce stade, vous devriez vous trouver sur la page High Availability (Haute disponibilité), et l'état de votre périphérique devrait être Negotiating (Négociation). L'état doit passer à Active (Actif) même avant que vous ne configuriez l'unité homologue, laquelle doit apparaître comme Failed (En échec) jusqu'à sa configuration.

Vous pouvez maintenant configurer l'unité secondaire. Consultez Configurer l'unité secondaire pour la haute disponibilité, à la page 19.

Remarque
Les interfaces sélectionnées ne sont pas configurées directement. Toutefois, si vous saisissez **show interface** dans l'interface de ligne de commande, vous constaterez que les interfaces utilisent les adresses IP spécifiées. Les interfaces sont nommées « failover-link » et, si vous configurez une liaison d'état distincte, « stateful-failover-link ».

Configurer l'unité secondaire pour la haute disponibilité

Après avoir configuré le périphérique principal pour la haute disponibilité active/en veille, vous devez configurer le périphérique secondaire. Connectez-vous à Firepower Device Manager sur ce périphérique et suivez cette procédure.

Remarque Si vous ne l'avez pas encore fait, copiez la configuration de haute disponibilité du périphérique principal dans le presse-papiers. Il est beaucoup plus facile de configurer le périphérique secondaire à l'aide du copier/coller que de saisir manuellement les données.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Dans la partie droite du résumé du périphérique, cliquez sur **Configure** (Configurer) à côté du groupe **High Availability** (Haute disponibilité).

Si vous configurez la haute disponibilité pour la première fois sur le périphérique, le groupe ressemblerait à ce qui suit.

Étape 3 Sur la page High Availability (Haute disponibilité), cliquez sur la case **Secondary Device** (Périphérique secondaire).

Étape 4 Effectuez l'une des opérations suivantes :

- **Méthode facile** : cliquez sur le bouton **Paste from Clipboard** (Coller à partir du presse-papiers), collez la configuration et cliquez sur **OK**. Cela mettra à jour les champs avec les valeurs appropriées, que vous pourrez ensuite vérifier.
- **Méthode manuelle** : configurez les liens de basculement et de basculement avec état directement. Saisissez exactement les mêmes paramètres sur le périphérique secondaire que vous avez saisis sur le périphérique principal.

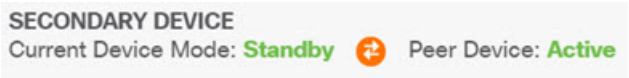
Étape 5 Si vous avez configuré une **clé de chiffrement IPSec** sur le périphérique principal, saisissez exactement la même clé pour le périphérique secondaire.

Étape 6 Cliquez sur **Activate HA** (Activer HA).

Le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si vous ne voyez pas de message indiquant que votre configuration a été enregistrée et que le déploiement est en cours, faites défiler la page vers le haut pour voir les messages d'erreur.

Une fois la configuration terminée, vous recevez un message indiquant que vous avez configuré la haute disponibilité. Cliquez sur **Got It** (J'ai compris) pour supprimer le message.

À ce stade, vous devriez être sur la page High Availability (haute disponibilité), et l'état de votre périphérique doit indiquer qu'il s'agit du périphérique secondaire. Si la jonction avec le périphérique principal a réussi, le périphérique se synchronisera avec le périphérique principal et, finalement, le mode devrait être Standby (veille) et l'homologue devrait être Active (actif).



Remarque
Les interfaces sélectionnées ne sont pas configurées directement. Toutefois, si vous saisissez **show interface** dans l'interface de ligne de commande, vous constaterez que les interfaces utilisent les adresses IP spécifiées. Les interfaces sont nommées « failover-link » et, si vous configurez une liaison d'état distincte, « stateful-failover-link ».

Configurer les critères de basculement pour la surveillance de l'intégrité

Les unités dans une configuration à haute disponibilité se surveillent elles-mêmes pour l'intégrité globale et l'intégrité des interfaces.

Les critères de basculement définissent les mesures de surveillance d'intégrité qui déterminent si un homologue est défaillant. Si l'homologue actif est l'unité qui ne respecte pas les critères, il déclenche un basculement vers l'unité de secours. Si l'homologue de secours est l'unité qui ne respecte pas les critères, elle est marquée comme ayant échoué et n'est pas disponible pour le basculement.

Vous pouvez configurer les critères de basculement sur le périphérique actif uniquement.

Le tableau suivant présente les événements déclencheurs de basculement et la synchronisation de détection des défaillances.

Tableau 2 : Délais de basculement en fonction des critères de basculement

Événement déclencheur de basculement	Minimum	Par défaut	Maximum
L'unité active perd de l'alimentation ou arrête le fonctionnement normal.	800 milliseconde	15 secondes	45 secondes
Le lien physique de l'interface de l'unité active est en panne.	500 millisecondes	5 secondes	15 secondes
L'interface de l'unité active est en service, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

Les rubriques suivantes expliquent comment personnaliser les critères de surveillance de l'intégrité du basculement et comment le système teste les interfaces.

Configurer les critères de basculement de la surveillance de l'intégrité des unités homologues

Chaque unité dans une configuration à haute disponibilité 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. La mesure que prend le périphérique dépend de la réponse de l'autre unité.

- Si le périphérique reçoit une réponse sur le lien de basculement, il ne bascule pas.
- Si le périphérique 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 ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Vous pouvez configurer l'interrogation et le délai de rétention des messages Hello.

Procédure

Étape 1 Sur le périphérique actif, cliquez sur **Device** (Périphérique).

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Les critères de basculement sont répertoriés dans la colonne de droite de la page High Availability (Haute disponibilité).

Étape 3 Définissez la **Peer Timing Configuration** (Configuration de synchronisation de l'unité homologue).

Ces paramètres déterminent la vitesse à laquelle le périphérique actif peut basculer vers le périphérique en veille. Avec un temps de sondage plus court, le périphérique peut détecter une défaillance et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné. Les paramètres par défaut sont appropriés pour la plupart des situations.

Si une unité ne reçoit pas de paquet hello sur l'interface de basculement pendant une période de sondage, des tests supplémentaires sont effectués sur les interfaces restantes. S'il n'y a toujours aucune réponse de l'unité homologue pendant le délai de maintien, l'unité est considérée comme défaillante et, si l'unité défaillante est l'unité active, l'unité en veille prend le relais comme unité active.

- **Poll Time (Délai de sondage)** : durée entre les messages hello. Saisissez de 1 à 15 secondes ou de 200 à 999 millisecondes. La valeur par défaut est de 1 seconde.
- **Hold Time** (Délai de rétention) : durée pendant laquelle une unité doit recevoir un message hello sur le lien de basculement, après quoi l'unité homologue est déclarée en panne. Le délai de rétention doit être au moins 3 fois supérieur au délai de sondage. Saisissez de 1 à 45 secondes ou de 800 à 999 millisecondes. La valeur par défaut est de 15 secondes.

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

Configurer les critères de basculement pour la surveillance de l'intégrité des interfaces

Vous pouvez surveiller jusqu'à 211 interfaces, selon le modèle de votre périphérique. Vous devez surveiller les interfaces importantes. Par exemple, les interfaces qui assurent le débit entre les réseaux importants. Surveillez une interface uniquement si vous configurez des adresses IP de secours pour celle-ci et si l'interface doit toujours être opérationnelle.

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 2 périodes de sondage, elle exécute des tests d'interface. Si tous les tests d'interface échouent pour une interface, mais que cette même interface sur l'autre unité continue de transmettre correctement le trafic, l'interface est considérée comme défaillante. Si le seuil pour les interfaces défaillantes est atteint, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Unknown » (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 repasse en mode veille si le seuil de défaillance d'interface n'est plus atteint.

Vous pouvez surveiller l'état de l'interface à haute disponibilité à partir de l'interface de ligne de commande ou de la console d'interface de ligne de commande en utilisant la commande **show monitor-interface**. Pour en savoir plus, consultez Surveillance de l'état pour les interfaces surveillées par la haute disponibilité, à la page 40.

Remarque Lorsqu'une interface tombe en panne, elle est toujours considérée comme un problème d'unité pour le basculement. Si l'unité détecte qu'une interface est en panne, le basculement se produit immédiatement (si vous conservez le seuil par défaut de 1 interface), sans attendre le délai de rétention de l'interface. Le délai de rétention de l'interface n'est utile que lorsque l'unité considère que son état est OK, bien qu'elle ne reçoive pas de paquets Hello de l'homologue.

Avant de commencer

Par défaut, toutes les interfaces physiques nommées sont sélectionnées pour la surveillance à haute disponibilité. Ainsi, vous devez désactiver la surveillance sur les interfaces physiques moins critiques. Pour les sous-interfaces ou les groupes de ponts, vous devez activer manuellement la surveillance.

Pour désactiver complètement la surveillance des interfaces et empêcher le basculement en raison d'une défaillance d'interface, assurez-vous simplement qu'aucune interface n'est activée pour la surveillance à haute disponibilité.

Procédure

Étape 1 Sur le périphérique actif, cliquez sur **Device** (Périphérique).

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Les critères de basculement sont répertoriés dans la colonne de droite de la page High Availability (Haute disponibilité).

Étape 3 Définissez le **Interface Failure Threshold** (Seuil de défaillance de l'interface).

Si le nombre d'interfaces défaillantes atteint le seuil, l'unité se marque comme défaillante. Si l'unité est l'unité active, elle bascule vers l'unité de secours. Si l'unité est l'unité de secours, en se notant comme défaillante, l'unité active ne considérera pas l'unité comme disponible pour le basculement.

Lors de la définition de ces critères, tenez compte du nombre d'interfaces que vous surveillez. Par exemple, si vous activez la surveillance sur seulement 2 interfaces, le seuil de 10 interfaces ne sera jamais atteint. Vous configurez la surveillance pour une interface en sélectionnant l'option **Enable for HA Monitoring** (Activer la surveillance à haute disponibilité) sous l'onglet **Advanced Options** (Options avancées) lors de la modification des propriétés de l'interface.

Par défaut, l'unité se marque d'elle-même comme défaillante si une interface surveillée tombe en panne.

Vous pouvez définir le seuil de défaillance de l'interface en sélectionnant l'une des options **Failover Criteria** (Critère de basculement) suivantes :

- **Number of failed interfaces exceeds** (Nombre d'interfaces défaillantes supérieur à) : saisissez le nombre brut d'interfaces. La valeur par défaut est 1. Le maximum dépend en fait du modèle de périphérique et peut varier, mais vous ne pouvez pas saisir plus de 211. Si vous utilisez ce critère, vous obtiendrez une erreur de déploiement si vous saisissez un nombre supérieur à celui que le périphérique prend en charge. Essayez un nombre plus petit ou utilisez plutôt un pourcentage.
- **Percentage of failed interfaces exceed**s (Le pourcentage d'interfaces défaillantes dépasse) : saisissez un nombre de 1 à 100. Par exemple, si vous saisissez 50 % et que vous surveillez 10 interfaces, le périphérique se marque lui-même comme comme défaillant si 5 interfaces échouent.

Étape 4 Définissez **Interface Timing Configuration** (Configuration de la temporisation de l'interface)

Ces paramètres déterminent la vitesse à laquelle l'appareil actif peut déterminer si une interface est défaillante. Étant donné que le délai de sondage est plus rapide, l'appareil peut détecter plus rapidement les défaillances d'interface. Cependant, une détection plus rapide peut signifier que les interfaces occupées sont marquées comme étant défaillantes alors qu'elles fonctionnent correctement, ce qui peut entraîner des basculements inutilement fréquents. Les paramètres par défaut sont appropriés pour la plupart des situations.

Si une liaison d'interface est en panne, le test d'interface n'est pas effectué et l'unité de secours peut devenir active en une seule période d'interrogation d'interface si le nombre d'interfaces défaillantes atteint ou dépasse le seuil de basculement d'interface configuré.

- **Poll Time** (Délai de sondage) : la fréquence à laquelle les paquets Hello sont envoyés sur les interfaces de données. Saisissez de 1 à 15 secondes ou de 500 à 999 millisecondes. La valeur par défaut est de 5 secondes.

- **Hold Time** (Temps de rétention : la durée entre le moment où un paquet Hello est manqué et le moment où l'interface est marquée comme défaillante. Saisissez entre 5 et 75 secondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 5 fois le délai de sondage.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Activez la surveillance à haute disponibilité pour chaque interface que vous souhaitez surveiller.

a) Choisissez **Device (Périphérique)** > **Interfaces**.

Si une interface est surveillée, la colonne Monitor for HA (Surveillance HA) indique Enabled (Activé).

b) Cliquez sur l'icône de modification ( ) d'une interface dont vous souhaitez modifier l'état de surveillance.

Vous ne pouvez pas modifier les interfaces de basculement ou de basculement dynamique. La surveillance des interfaces ne s'applique pas à elles.

c) Cliquez sur l'onglet **Advanced Options** (Options avancées).

d) Cochez ou décochez la case **Enable for HA Monitoring** (Activer la surveillance à haute disponibilité) selon vos préférences.

e) Cliquez sur **OK**.

Étape 7 (Facultatif, mais conseillé.) Configurez les adresses IP de secours et les adresses MAC pour les interfaces surveillées. Consultez Configurer les adresses IP et MAC de secours, à la page 25.

Comment le système teste l'intégrité de l'interface

Le système teste en continu les interfaces que vous supervisez afin de vérifier leur état de haute disponibilité. L'adresse utilisée pour le test d'une interface dépend des types d'adresses que vous configurez :

- 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).

Le système effectue les tests suivants sur chaque unité :

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test Link Up/Down (liaison active/désactivée) indique que l'interface est en panne, l'unité la considère comme défaillante. Si l'état est Up (activé), l'unité exécute le Network Activity test (test d'activité réseau).
2. Test d'activité réseau : test d'activité réseau reçu. Le but de ce test est de générer le trafic réseau à l'aide des messages LANTEST pour déterminer quelle unité (le cas échéant) a échoué. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets pendant le test (jusqu'à 5 secondes), l'interface est considérée comme opérationnelle. 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. Si aucune des unités ne reçoit de trafic, l'unité démarre le test ARP.
3. Test ARP : lecture du cache ARP de l'unité pour les 2 dernières entrées. Une à la fois, l'unité envoie des requêtes ARP à ces périphériques, pour tenter de relancer le trafic réseau. Après chaque demande, l'unité compte tout le trafic reçu pendant 5 secondes maximum. Si le trafic est reçu, l'interface est considérée comme opérationnelle. Si aucun trafic n'est reçu, une demande ARP est envoyée au périphérique suivant. Si à la fin de la liste aucun trafic n'a été reçu, l'unité démarre le test ping.

4. Test de ping de diffusion : test de ping qui consiste à envoyer une demande de ping de diffusion. L'unité compte ensuite tous les paquets reçus pendant un maximum de 5 secondes. Si des paquets sont reçus à tout moment pendant cet intervalle, l'interface est considérée comme opérationnelle et le test s'arrête. Si aucun trafic n'est reçu, les tests recommencent avec le test ARP.

Configurer les adresses IP et MAC de secours

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. 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.

1. Lorsque l'unité principale bascule, l'unité secondaire adopte les adresses IP et MAC de l'unité principale et commence à transmettre le trafic.
2. L'unité qui est maintenant en état de veille prend le relais des adresses IP et MAC de secours.

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.

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. Cependant, 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.

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. Vous pouvez configurer manuellement des adresses MAC virtuelles.

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. Firewall Threat Defense 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.

Procédure

Étape 1 Choisissez **Device (Périphérique)** > **Interfaces**.

Vous devez au moins configurer des adresses IP et MAC de secours pour les interfaces que vous surveillez pour la haute disponibilité. Si une interface est surveillée, la colonne Monitor for HA (Surveillance HA) indique Enabled (Activé).

Étape 2 Cliquez sur l'icône de modification ( ) de l'interface dont vous souhaitez configurer les adresses de secours.

Vous ne pouvez pas modifier les interfaces de basculement ou de basculement dynamique. Vous définissez les adresses IP de ces interfaces lorsque vous configurez la haute disponibilité.

Étape 3 Configurez les adresses IP de secours dans les onglets **IPv4 Address** (Adresse IPv4) et **IPv6 Address** (Adresse IPv6).

L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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. Configurez des adresses de secours pour chaque version IP utilisée.

Étape 4 Cliquez sur l'onglet **Advanced Options** (Options avancées) et configurez les adresses MAC.

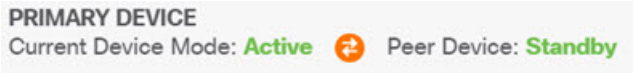
Par défaut, le système utilise l'adresse MAC gravée dans la carte d'interface réseau (NIC) pour l'interface. Ainsi, toutes les sous-interfaces d'une interface utilisent la même adresse MAC. Vous pouvez donc créer des adresses uniques par sous-interface. Des adresses MAC actives/en attente configurées manuellement sont également recommandées si vous configurez la haute accessibilité. La définition des adresses MAC permet de maintenir la cohérence du réseau en cas de basculement.

- **MAC Address** (Adresse MAC) : l'adresse Media Access Control au format H.H.H, où H correspond à une valeur hexadécimale de 16 bits. Par exemple, vous devez entrer l'adresse MAC 00-0C-F1-42-4C-DE comme 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.
- **Standby MAC Address** (adresse MAC en veille) : À utiliser avec la haute disponibilité. Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.

Étape 5 Cliquez sur **OK**.

Vérifier la High Availability Configuration (Configuration de la haute disponibilité)

Après avoir terminé la configuration de la haute disponibilité, vérifiez que l'état du périphérique indique que les deux périphériques sont opérationnels et en mode actif/en veille.



Vous pouvez vérifier que la configuration de haute disponibilité fonctionne en suivant cette procédure.

Procédure

Étape 1 Testez que votre unité active transmet le trafic comme prévu en utilisant FTP (par exemple) pour envoyer un fichier entre des hôtes sur différentes interfaces.

Testez au minimum les connexions d'un poste de travail vers les systèmes connectés à chacune des interfaces configurées.

Étape 2 Basculez de mode de sorte que l'unité active devienne l'unité de secours en effectuant l'une des opérations suivantes :

- Dans le Firepower Device Manager, sélectionnez **Switch Mode** (Changer de mode) à partir du menu d'engrenage sur la page **Device (Périphérique)** > **High Availability (Haute disponibilité)**.
- Dans l'interface de ligne de commande de l'unité active, saisissez **no failover active**.

Étape 3 Répétez les tests de connexion pour vérifier que vous pouvez établir les mêmes connexions par l'intermédiaire de l'autre unité de la paire de haute disponibilité.

Si le test échoue, vérifiez que vous avez connecté les interfaces de l'unité aux mêmes réseaux que les interfaces équivalentes sur l'autre unité.

Vous pouvez voir l'état de HA à partir de la page High Availability (Haute disponibilité). Vous pouvez également utiliser l'interface de ligne de commande ou la console d'interface de ligne de commande de l'unité et saisir la commande **show failover** pour vérifier l'état du basculement. Utilisez également la commande **show interface** pour vérifier la configuration d'interface pour les interfaces utilisées dans les tests de connexion qui ont échoué.

Si ces actions ne détectent pas le problème, il existe d'autres étapes que vous pouvez suivre. Consultez Dépannage de la haute disponibilité (basculement), à la page 42.

Étape 4 Lorsque vous avez terminé, vous pouvez basculer de mode pour rétablir l'état actif de l'unité d'origine qui était active.

Gérer la haute disponibilité

Vous pouvez gérer une paire à haute disponibilité en cliquant sur le lien **High Availability** (Haute disponibilité) sur la page **Device Summary** (Résumé des périphériques).

La page Haute disponibilité comprend les éléments suivants :

- **État du rôle et du mode** : la zone d'état gauche indique si le périphérique est le Primary (Primaire) ou le Secondary (Secondaire) du groupe. Le mode indique si ce périphérique est actif ou en veille, ou si la haute disponibilité a été suspendue ou si le périphérique attend de rejoindre le périphérique homologue. Il affiche également l'état du périphérique homologue, qui peut être actif, en veille, suspendu ou en panne. Par exemple, lorsque vous êtes connecté au périphérique principal et qu'il s'agit également du périphérique actif, et que le périphérique secondaire est intègre et prêt à basculer si nécessaire, l'état ressemblerait à ce qui suit. Vous pouvez cliquer sur l'icône entre les homologues pour obtenir des informations sur l'état de la synchronisation de la configuration entre les périphériques.

- **Dernière raison de l'échec** : si la configuration de la haute disponibilité (HA) échoue pour une raison quelconque, comme le périphérique actif devient indisponible et bascule vers le périphérique de secours, la dernière raison de l'échec est indiquée sous les informations d'état du rôle et du mode. Ce message est dérivé de l'historique de basculement.
- Lien **Failover History** (Historique de basculement) : cliquez sur ce lien pour voir l'historique détaillé de l'état des périphériques de la paire. Le système ouvre la console d'interface de ligne de commande et exécute la commande **show failover history details**.
- Lien **Deployment History** (Historique de déploiement) : cliquez sur ce lien pour accéder au journal d'audit avec les événements filtrés pour afficher uniquement les tâches de déploiement.

- **Gear button** (Bouton d'engrenage) : cliquez sur ce bouton pour effectuer des actions sur les appareils.
  - **Suspend HA** (Suspendre la haute disponibilité)/**Resume HA** (Reprendre la haute disponibilité) : la suspension de la haute disponibilité empêche les périphériques de fonctionner en tant que paire à haute disponibilité sans supprimer la configuration de haute disponibilité. Vous pouvez ultérieurement reprendre, c'est-à-dire réactiver, la haute disponibilité sur les périphériques. Pour de plus amples renseignements, consultez la section Suspendre et reprendre la haute disponibilité, à la page 28.
  - **Break HA (Rupture de la haute disponibilité)** : la rupture de la haute disponibilité supprime la configuration de haute disponibilité des deux périphériques et les ramène aux périphériques autonomes. Pour de plus amples renseignements, consultez la section Rupture de la haute disponibilité, à la page 30.
  - **Switch Mode** (Mode de commutation) : le mode de commutation vous permet de forcer un périphérique actif à passer en veille ou un périphérique en veille à devenir actif, selon le périphérique à partir duquel vous effectuez l'action. Pour de plus amples renseignements, consultez la section Commutation des homologues actifs et de secours (forcer le basculement), à la page 31.
- **High Availability Configuration** (Configuration de la haute disponibilité) : ce panneau affiche la configuration de la paire de basculement. Cliquez sur le bouton **Copy to Clipboard** (Copier dans le presse-papier) pour charger les informations dans le presse-papier, à partir duquel vous pouvez les coller dans la configuration du périphérique secondaire. Vous pouvez également le copier dans un autre fichier pour vos enregistrements. Ces informations n'affichent pas si vous avez défini une clé de chiffrement IPsec.

Remarque La configuration d'interface pour la haute disponibilité n'est pas reflétée dans la page Interfaces (**Device (appareil)** > **Interfaces**). Vous ne pouvez pas modifier les interfaces que vous utilisez dans une configuration à haute disponibilité.

- **Failover Criteria** (Critères de basculement) : ce panneau comprend les paramètres qui déterminent les critères d'intégrité utilisés pour évaluer si l'unité active est défaillante et si l'unité de secours doit devenir l'unité active. Ajustez ces critères afin d'obtenir les performances de basculement requises dans votre réseau. Pour de plus amples renseignements, consultez la section Configurer les critères de basculement pour la surveillance de l'intégrité, à la page 20.

Les rubriques suivantes expliquent diverses tâches de gestion liées à une configuration à haute disponibilité.

Suspendre et reprendre la haute disponibilité

Vous pouvez suspendre une unité dans une paire à haute disponibilité. C'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.
- Vous souhaitez empêcher le basculement lors de l'installation d'une mise à niveau logicielle sur le périphérique de secours.

Lorsque vous suspendez la haute disponibilité, vous empêchez la paire de périphériques de se comporter comme une unité de basculement. 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 périphérique en veille conservera sa configuration, mais il restera inactif.

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 à haute disponibilité est conservée. Lorsque vous annulez la haute disponibilité, la configuration est effacée. Ainsi, vous avez la possibilité de réactiver 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.

La suspension de la haute disponibilité sur l'unité active suspend la haute disponibilité sur l'unité active et l'unité en veille. 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.

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 Si nécessaire, vous pouvez suspendre la haute disponibilité depuis l'interface de ligne de commande en saisissant la commande **configure high-availability suspend**. Pour réactiver la haute disponibilité, saisissez **configure high-availability resume**.

Avant de commencer

Si vous suspendez la haute disponibilité par l'intermédiaire du Firepower Device Manager, elle reste suspendue jusqu'à ce que vous la repreniez, même si vous rechargez l'unité. Cependant, si vous la suspendez au moyen de la console d'interface en ligne de commande, il s'agit d'un état temporaire et, lors du rechargement, l'unité reprend automatiquement la configuration de haute disponibilité et négocie l'état actif/en veille avec l'homologue.

Si vous suspendez la haute disponibilité sur l'unité en veille, vérifiez si l'unité active exécute actuellement une tâche de déploiement. Si vous changez de mode alors qu'une tâche de déploiement est en cours, la tâche échouera et vous perdrez vos modifications de configuration.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 Choisissez la commande appropriée dans l'icône en forme d'engrenage ( ).

- **Suspend HA** (Suspendre la haute disponibilité) : vous êtes invité à confirmer l'action. Lisez le message et cliquez sur **OK**. L'état de la haute disponibilité devrait indiquer que le périphérique est en mode Suspended (Suspendu).

- **Resume HA** (Reprendre la haute disponibilité) : vous êtes invité à confirmer l'action. Lisez le message et cliquez sur **OK**. L'état de haute disponibilité devrait redevenir normal, soit actif, soit en veille, après que l'unité a négocié avec l'homologue.

Rupture de la haute disponibilité

Si vous ne souhaitez plus que les deux périphériques fonctionnent en tant que paire à haute disponibilité, vous pouvez interrompre la configuration à haute disponibilité. Lorsque vous annulez la haute disponibilité, chaque périphérique devient un périphérique autonome. Leurs configurations sont modifiées comme suit :

- Le périphérique actif conserve la configuration complète telle qu'elle était avant l'interruption, avec la configuration à haute disponibilité supprimée.
- Le périphérique de secours voit toute la configuration d'interface supprimée en plus de la configuration à haute disponibilité. Toutes les interfaces physiques sont désactivées, bien que les sous-interfaces ne soient pas désactivées. L'interface de gestion reste active, vous pouvez donc vous connecter au périphérique et le reconfigurer.

Remarque Vous pouvez également utiliser la ressource API BreakHAStatus (à partir de l'explorateur d'API) et utiliser l'attribut **interfaceOption** pour demander au système de reconfigurer les interfaces du périphérique en veille à l'aide des adresses IP en veille. Vous devez utiliser l'API si vous souhaitez ce résultat ; sinon, Firepower Device Manager désactive toujours les interfaces. Notez que le système reconfigure les adresses IP, mais ne reconfigure pas toutes les options d'interface, de sorte que le trafic peut ne pas se comporter comme prévu tant que vous n'avez pas déployé les modifications après l'interruption.

La façon dont l'interruption affecte réellement les unités dépend de l'état de chaque unité lorsque vous effectuez l'interruption.

- Si les unités sont dans un état actif/en veille intègre, cassez la haute disponibilité de l'unité active. Cela supprimera la configuration à haute disponibilité des deux périphériques de la paire à haute disponibilité. Si vous souhaitez interrompre la haute disponibilité sur l'unité de secours uniquement, vous devez vous y connecter et d'abord suspendre la haute disponibilité, puis vous pourrez interrompre la haute disponibilité.
- Si l'unité de secours est en état suspendu ou en panne, l'interruption de la haute disponibilité de l'unité active supprime la configuration à haute disponibilité de l'unité active uniquement. Vous devez vous connecter à l'unité de secours et également interrompre la haute disponibilité sur cette unité.
- Si les homologues négocient toujours la haute disponibilité ou synchronisent leur configuration, vous ne pouvez pas interrompre la haute disponibilité. Attendez que la négociation ou la synchronisation soit terminée ou expire. Si vous pensez que les systèmes sont bloqués dans cet état, vous pouvez suspendre la haute disponibilité, puis l'interrompre.

Remarque Lorsque vous utilisez Firepower Device Manager, vous ne pouvez pas interrompre la haute disponibilité de l'interface de ligne de commande à l'aide de la commande **configure high-availability disable**.

Avant de commencer

Pour des résultats idéaux, mettez les périphériques dans un état actif/en veille et effectuez cette action à partir du périphérique actif.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 Dans l'icône en forme d'engrenage ( ), choisissez **Break HA** (Rompre la haute disponibilité).

Étape 4 Lisez le message de confirmation, décidez de sélectionner l'option de désactivation des interfaces, puis cliquez sur **OK**.

Vous devez sélectionner l'option de désactivation des interfaces si vous rompez la haute disponibilité à partir de l'unité de secours.

Le système déploie immédiatement vos modifications sur ce périphérique et le périphérique homologue (si possible). Cela peut prendre quelques minutes pour que le déploiement sur chaque périphérique et pour que chaque périphérique devienne indépendant.

Commutation des homologues actifs et de secours (forcer le basculement)

Vous pouvez permuter les modes actif / en veille pour une paire à haute disponibilité opérationnelle, c'est-à-dire qu'un homologue est actif, l'autre est en veille. Par exemple, si vous installez une mise à niveau logicielle, vous pouvez mettre l'unité active en veille afin que la mise à niveau n'ait pas d'incidence sur le trafic des utilisateurs.

Vous pouvez changer de mode à partir de l'unité active ou en veille, mais l'unité homologue doit fonctionner du point de vue de l'autre unité. Vous ne pouvez pas changer de mode si une unité est suspendue (vous devez d'abord reprendre la haute disponibilité) ou en échec.

Remarque Au besoin, vous pouvez basculer entre les modes actif et en veille à partir de la console d'interface en ligne de commande. À partir de l'unité en veille, dans la console d'interface en ligne de commande, saisissez la commande **failover active**. À partir de l'unité active, entrez la commande **no failover active**.

Avant de commencer

Avant de changer de mode, vérifiez que l'unité active n'est pas en cours de tâche de déploiement. Attendez que le déploiement soit terminé avant de changer de mode.

Si l'unité active a des modifications non déployées en attente, déployez-les avant de changer de mode. Sinon, vous perdrez vos modifications si vous exécutez une tâche de déploiement à partir de la nouvelle unité active.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Cliquez sur le lien **High Availability** (Haute disponibilité) sur le côté droit du résumé du périphérique.

Étape 3 À partir de l'icône en forme d'engrenage (⚙), choisissez **Switch Mode** (Mode de commutation).

Étape 4 Lisez le message de confirmation et cliquez sur **OK**.

Le système force le basculement de sorte que l'unité active passe en veille et que l'unité en veille devient la nouvelle unité active.

Préservation des modifications de configuration non déployées après un basculement

Lorsque vous apportez des modifications à la configuration des unités d'une paire à haute disponibilité, vous modifiez la configuration sur l'unité active. Vous déployez ensuite vos modifications, et les unités active et en veille sont mises à jour avec la nouvelle configuration. Peu importe que l'unité active soit le périphérique principal ou secondaire.

Cependant, les modifications non déployées ne sont pas synchronisées entre les unités. Toutes les modifications non déployées sont disponibles uniquement sur l'unité où vous avez apporté ces modifications.

Ainsi, si un basculement se produit lorsque vous avez des modifications non déployées, ces modifications ne sont pas disponibles sur la nouvelle unité active. Les modifications restent cependant en place sur l'unité qui est maintenant en veille.

Pour récupérer vos modifications non déployées, vous devez changer de mode pour forcer un basculement et faire revenir l'autre unité à l'état actif. Lorsque vous vous connectez à l'unité nouvellement active, vos modifications non déployées sont disponibles et vous pouvez les déployer. Utilisez la commande **Switch Modes** (changer de mode) dans le menu d'engrenage des paramètres de **High Availability** (haute disponibilité) (⚙).

Veuillez garder à l'esprit les éléments suivants :

- Si vous déployez des modifications à partir de l'unité active alors qu'il y a des modifications non déployées sur l'unité en veille, les modifications non déployées sur l'unité en veille seront effacées. Vous ne pourrez pas les récupérer.
- Lorsqu'une unité de secours rejoint une paire à haute accessibilité, toutes les modifications non déployées sur l'unité de secours sont effacées. La configuration est synchronisée chaque fois qu'une unité rejoint ou rejoint la paire.
- Si l'unité qui contient les modifications non déployées a échoué de manière catastrophique et que vous avez dû la remplacer ou la recréer, vos modifications non déployées sont définitivement perdues.

Modification des licences et de l'enregistrement en mode de haute disponibilité

Les unités de la paire à haute disponibilité doivent avoir les mêmes licences et le même statut d'enregistrement. Pour apporter des modifications :

- Vous activez ou désactivez les licences facultatives sur l'unité active. Puis vous déployez la configuration et l'unité de secours demande (ou libère) les licences nécessaires. Lorsque vous activez des licences, vous devez vous assurer que votre compte Cisco Smart Software Manager dispose de suffisamment de licences, sinon vous pourriez vous retrouver avec une unité conforme alors que l'autre unité est non conforme.
- Vous enregistrez ou annulez l'enregistrement des unités séparément. Pour fonctionner correctement, les unités doivent être en mode d'évaluation ou enregistrées. Si les périphériques sont enregistrés, ils peuvent être enregistrés dans différents comptes Cisco Smart Software Manager, mais les comptes doivent avoir le même état pour le paramètre de fonctionnalité de contrôle de l'exportation : activés ou désactivés. Vous ne pouvez pas déployer les modifications de configuration si les unités ont un état d'enregistrement incohérent.

Modification de la clé de chiffrement IPsec à haute disponibilité ou de la configuration à haute disponibilité

Vous pouvez modifier n'importe quel critère de basculement en vous connectant à l'unité active, en effectuant vos modifications et en les déployant.

Toutefois, si vous devez modifier la clé de chiffrement IPsec utilisée sur vos liaisons de basculement, ou modifier les interfaces ou les adresses IP pour les liaisons de basculement ou de basculement dynamique, vous devez d'abord interrompre la configuration à haute disponibilité. Vous pouvez ensuite reconfigurer les unités principale et secondaire avec la nouvelle clé de chiffrement ou les paramètres de basculement ou de liaison de basculement dynamique.

Marquer une unité défaillante comme saine

Une unité dans une configuration à haute disponibilité peut être marquée comme défaillante en raison d'une surveillance régulière de l'intégrité. Si l'unité est saine, elle devrait revenir à l'état normal lorsqu'elle répond de nouveau aux exigences de surveillance de l'intégrité. Si vous voyez un périphérique sain échouer fréquemment, vous pouvez augmenter les délais d'expiration de pair, cesser de superviser certaines interfaces moins importantes, ou modifier les délais d'expiration de supervision des interfaces.

Vous pouvez forcer une unité défaillante à être vue comme saine en saisissant la commande **failover reset** à partir de l'interface de ligne de commande. Nous vous recommandons d'entrer la commande à partir de l'unité active, ce qui réinitialisera l'état de l'unité de secours. Vous pouvez afficher l'état de basculement de l'unité à l'aide des commandes **show failover** ou **show failover state**.

La restauration d'une unité défaillante à un état sans défaillance ne la rend pas automatiquement active. Les unités restaurées restent à l'état de secours jusqu'à ce qu'elles soient activées par le basculement (contraint ou normal).

La réinitialisation de l'état du périphérique ne résout pas les problèmes qui ont mené au marquage du périphérique comme défaillant. Si vous ne corrigez pas les problèmes, ou si vous relâchez vos délais d'expiration de supervision, le périphérique peut être marqué comme défaillant de nouveau.

à niveau de la haute disponibilité Firewall Threat Defense

Utilisez cette procédure pour mettre à niveau des périphériques à haute disponibilité. Mettez-les à niveau un à la fois. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. C'est-à-dire que vous mettez à niveau le serveur de secours actuel, changez de rôle, puis mettez à niveau le nouveau serveur de secours. Si vous devez mettre à jour FXOS, faites-le sur les deux châssis avant de mettre à niveau Firewall Threat Defense sur l'un ou l'autre. Encore une fois, mettez toujours à niveau le serveur de secours.

Mise en garde N'apportez pas et n'utilisez pas de modifications de configuration sur une unité pendant que l'autre est en cours de mise à niveau, ou vers une paire de versions mixte. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité, à la page 36.

Avant de commencer

Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Astuces La planification de la mise à niveau commence par la lecture du Cisco Secure Firewall Threat Defense Notes de mise à jour. Elle inclut ensuite la création de sauvegardes, l'obtention des paquets de mise à niveau et l'exécution des mises à niveau associées (comme FXOS pour Firepower 4100/9300). Elle comprend également la vérification des modifications de configuration nécessaires, de la préparation, de la vérification de l'espace disque et de la vérification des tâches en cours d'exécution et planifiées. Pour en savoir plus, consultez le http://www.cisco.com/go/ftd-quick pour votre version.

Procédure

Étape 1 Connectez-vous à l'unité en veille.

Étape 2 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 3 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Parcourir** ou sur ,**Remplacer le fichier** pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Exécuter la mise à niveau Immédiatement** pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est

particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 4 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour plus de renseignements, consultez Exécution d'une vérification de l'état de préparation aux mises à niveau

Étape 5 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continuer** pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 6 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (Résumé du périphérique) affiche la version du logiciel actuellement exécutée et l'état de la haute disponibilité. Ne continuez pas tant que vous n'avez pas vérifié la réussite *et que* la haute disponibilité n'a pas été rétablie. Si la haute disponibilité reste suspendue après une mise à niveau réussie, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité, à la page 36.

Étape 7 Mettez à niveau la deuxième unité.

a) Changer de rôle, rendant cet appareil actif : sélectionnez **Device** > **High Availability**(haute disponibilité du périphérique), puis sélectionnez **Switch Mode** (changer de mode) dans le menu déroulant ( ). Attendez que l'état de l'unité passe à actif et confirmez que le trafic circule normalement. Déconnectez-vous.

b) Mise à niveau : répétez les étapes précédentes pour vous connecter au nouveau serveur de secours, téléverser le paquet, mettre à niveau le périphérique, surveiller la progression et vérifier la réussite.

Étape 8 Examiner les rôles des périphériques.

Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 9 Connectez-vous à l'unité active.

Étape 10 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.

b) Apportez toutes les modifications de configuration requises après la mise à niveau.

c) Déployez.

Dépannage des mises à niveau de Threat Defense haute disponibilité

Dépannage général de la mise à niveau

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours; voir Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).

Mise en garde Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez *pas* manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si vous continuez à rencontrer des problèmes et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être revenir à une version majeure ou de maintenance antérieure; voir Rétablissement Firewall Threat Defense en cours.... Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez la commande **Annuler automatiquement en cas d'échec de la mise à niveau...** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez Annulation ou nouvelle tentative des Firewall Threat Defense mises à niveau. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Dépannage de la mise à niveau haute disponibilité

Ces problèmes sont spécifiques aux mises à niveau à haute disponibilité.

La mise à niveau ne commencera pas sans le déploiement des modifications non validées.

Si vous obtenez un message d'erreur indiquant que vous devez déployer toutes les modifications non validées, même s'il n'y en a pas, connectez-vous à l'unité active (n'oubliez pas que vous devriez mettre à niveau l'unité de secours), créez des modifications mineures et déployez. Ensuite, annulez la modification, redéployez et réessayez la mise à niveau sur le serveur de secours.

Si cela ne fonctionne pas et que les unités exécutent des versions logicielles différentes par rapport aux recommandations, changez de rôle pour rendre l'unité en veille active, puis suspendez la haute disponibilité. Vous pouvez ensuite effectuer le déploiement à partir de l'unité active/suspendue, reprendre la haute disponibilité, puis changer encore les rôles pour mettre l'unité active en veille à nouveau. La mise à niveau devrait alors fonctionner.

Le déploiement à partir de l'unité active échoue pendant la mise à niveau de secours ou provoque une erreur de synchronisation de l'application.

Cela peut se produire si vous déployez à partir de l'unité active tandis que l'unité de secours est en cours de mise à niveau, ce qui n'est pas pris en charge. Procédez à la mise à niveau malgré l'erreur. Après avoir mis à niveau les deux unités, apportez les modifications de configuration requises et déployez à partir de l'unité active. L'erreur devrait être résolue.

Pour éviter ces problèmes, n'apportez pas et ne déployez pas de modifications de configuration sur une unité pendant que l'autre unité est en cours de mise à niveau, ou vers une paire de versions mixte.

Les modifications de configuration apportées depuis la mise à niveau seront perdues.

Si vous devez absolument apporter et déployer des modifications sur une paire de versions, vous devez apporter les modifications aux deux unités, sinon elles seront perdues après la mise à niveau de l'unité active de bas niveau.

La haute disponibilité est suspendue après la mise à niveau.

Après le redémarrage après la mise à niveau, la haute disponibilité est brièvement suspendue pendant que le système effectue certaines tâches automatisées finales, telles que la mise à jour des bibliothèques et le redémarrage de Snort. Vous êtes susceptible de le remarquer si vous vous connectez à la CLI *très*

peu de temps après la mise à niveau. Si la haute disponibilité ne reprend pas d'elle-même après la fin de la mise à niveau et que Firepower Device Manager est disponible, faites-le manuellement :

1. Connectez-vous au périphérique actif et au périphérique en veille et consultez les listes des tâches. Attendez que toutes les tâches aient fini de s'exécuter sur les deux périphériques. Si vous remettez la haute disponibilité trop tôt, vous pourriez avoir un problème futur dans lequel le basculement provoque une panne.
2. Sélectionnez **Périphérique** > **Haute disponibilité**, puis **Reprendre** la haute disponibilité dans le menu engrenage ( ).

Le basculement ne se produit pas avec une paire de versions mixtes.

Bien que l'avantage de la haute disponibilité soit que vous puissiez mettre à niveau votre déploiement sans interruption de trafic ni inspection, le basculement est désactivé pendant l'ensemble du processus de mise à niveau. C'est-à-dire que non seulement le basculement est nécessairement désactivé lorsqu'un périphérique est hors ligne (car il n'y a rien vers lequel le basculement est effectué), mais le basculement est également désactivé avec les paires de versions mixtes. C'est le seul moment où les paires de versions mixtes sont autorisées (temporairement) pendant la mise à niveau. Planifiez les mises à niveau pendant les périodes de maintenance, au moment où elles auront le moins d'incidence en cas de problème, et assurez-vous d'avoir suffisamment de temps pour mettre à niveau les deux périphériques dans cette fenêtre.

Échec de la mise à niveau sur un seul périphérique, ou un périphérique a été annulé. La paire utilise maintenant des versions mixtes.

Les paires de versions ne sont pas prises en charge pour les opérations générales. Mettez à niveau le périphérique de version antérieure ou inversez le périphérique de version ultérieure. Pour les correctifs, car la restauration n'est pas prise en charge, si vous ne pouvez pas mettre à niveau le périphérique de version antérieure, vous devez interrompre la haute disponibilité, recréer l'image d'un ou des deux périphériques, puis rétablir la haute disponibilité.

Remplacement d'une unité dans une paire à haute disponibilité

Au besoin, vous pouvez remplacer une unité dans un groupe à haute disponibilité sans perturber le trafic réseau.

Procédure

Étape 1 Si l'unité que vous remplacez est fonctionnelle, assurez-vous de basculer vers l'unité homologue, puis utilisez la commande **shutdown** à partir de l'interface de ligne de commande du périphérique pour le mettre hors service correctement. Si l'unité n'est pas fonctionnelle, confirmez que l'homologue fonctionne en mode actif.

Si vous disposez de privilèges d'administrateur, vous pouvez également entrer la commande **shutdown** par le biais de la console d'interface de ligne de commande Firepower Device Manager.

Étape 2 Retirez l'unité du réseau.

Étape 3 Installez l'unité de remplacement et reconnectez les interfaces.

Étape 4 Terminez l'assistant de configuration du périphérique sur l'unité de remplacement.

Étape 5 Sur l'unité homologue, accédez à la page High Availability (Haute disponibilité) et copiez la configuration dans le presse-papiers. Notez s'il s'agit de l'unité principale ou secondaire.

Si des modifications sont en attente, déployez-les et attendez la fin du déploiement.

Étape 6 Sur l'unité de remplacement, cliquez sur **Configure** (Configurer) dans le groupe **High Availability** (Haute disponibilité), puis sélectionnez le type d'unité opposé parmi l'homologue. Autrement dit, si l'homologue est principal, sélectionnez **Secondary** (Secondaire), si l'homologue est secondaire, sélectionnez **Primary** (Primaire).

Étape 7 Collez la configuration de haute disponibilité de l'homologue, puis saisissez la clé IPsec si vous en utilisez une. Cliquez sur **Activate HA** (Activer HA).

Une fois le déploiement terminé, l'unité communiquera avec l'homologue et rejoindra le groupe de haute disponibilité. La configuration de l'homologue actif sera importée et l'unité de remplacement sera l'unité principale ou secondaire du groupe, en fonction de votre sélection. Vous pouvez maintenant vérifier que la haute disponibilité fonctionne correctement et, si vous le souhaitez, changer de mode pour que la nouvelle unité soit l'unité active.

Surveillance de la haute disponibilité

Les rubriques suivantes expliquent comment surveiller la haute disponibilité.

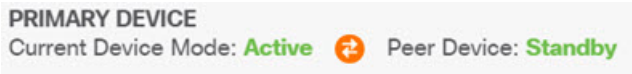
Notez que Event Viewer (Visionneuse d'événements) et les tableaux de bord affichent uniquement les données liées à l'appareil auquel vous êtes connecté. Ils n'affichent pas les données fusionnées des deux appareils.

Surveillance de l'état et de l'historique du basculement général

Vous pouvez surveiller l'état général et l'historique de haute disponibilité à l'aide des éléments suivants :

- Dans Device Summary (Résumé du périphérique) (cliquez sur **Device** (Périphérique)), le groupe High Availability (Haute disponibilité) affiche l'état de l'unité.

- Sur la page High Availability (Haute disponibilité) (cliquez sur **Device (Périphérique)** > **High Availability (Haute disponibilité)**), vous pouvez voir l'état des deux unités. Si des défaillances se sont produites, la dernière raison de défaillance (provenant de l'historique de basculement) s'affiche. Cliquez sur l'icône de synchronisation entre eux pour obtenir un état supplémentaire.



- Dans la page High Availability (Haute disponibilité), cliquez sur le lien **Failover History** (Historique de basculement) à côté de l'état. Le système ouvre la console CLI et exécute la commande **show failover history details**. Vous pouvez également entrer cette commande directement dans la CLI ou la console CLI.

Commandes de l'interface de ligne de commande

À partir de la CLI ou de la console CLI, vous pouvez utiliser les commandes suivantes :

- **show failover**

  Affiche des informations sur l'état de basculement de l'unité.

- **show failover history** [**details**]

  Affiche les changements d'état de basculement passés et la raison du changement d'état. Ajoutez le mot-clé **details** pour afficher l'historique de basculement à partir de l'unité homologue. Ces renseignements aident au dépannage.

- **show failover state**

  Affiche l'état de basculement des deux unités. Les informations affichées comprennent l'état principal ou secondaire de l'unité, l'état actif ou en veille de l'unité et le dernier motif signalé pour le basculement.

- **show failover statistics**

  Affiche le nombre de paquets de transmission (tx) et de réception (rx) de l'interface de basculement. Par exemple, si la sortie indique que l'unité envoie des paquets, mais n'en reçoit aucun, vous avez un problème de liaison. Il peut s'agir d'un mauvais câble, de mauvaises adresses IP configurées sur les homologues ou encore du fait que les unités connectent les interfaces de basculement à des sous-réseaux différents.

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

  Affiche la configuration des liens de basculement et de basculement avec état. Par exemple :

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  Affiche les renseignements sur les interfaces surveillées pour la haute disponibilité. Pour de plus amples renseignements, consultez la section Surveillance de l'état pour les interfaces surveillées par la haute disponibilité, à la page 40.

- **show running-config failover**

  Affiche les commandes de basculement dans la configuration actuelle. Ce sont les commandes qui configurent la haute disponibilité.

Surveillance de l'état pour les interfaces surveillées par la haute disponibilité

Si vous avez activé la surveillance HA pour toute interface, vous pouvez vérifier l'état des interfaces surveillées dans la CLI ou la console CLI à l'aide de la commande **show monitor-interface**.

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

Les interfaces surveillées peuvent avoir l'état suivant :

- (En attente) associé à tout autre état, comme Inconnu (En attente) — l'interface n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- 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.
- Aucune liaison : le lien physique de l'interface est inactif.
- Échec : aucun trafic n'est reçu sur l'interface, mais le trafic est diffusé sur l'interface homologue.

Surveillance des messages Syslog liés à la haute disponibilité

Le système envoie un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Les plages d'identifiants de message associés au basculement sont les suivantes : 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx et 727xxx. Par exemple, 105032 et 105043 indiquent un problème avec la liaison de basculement. Pour obtenir une explication des messages syslog, consultez le guide *Messages syslog de Cisco Firepower Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

Remarque Lors du basculement, le système s'éteint logiquement, puis affiche les interfaces, générant les messages syslog 411001 et 411002. Il s'agit d'une activité normale.

Pour pouvoir voir les messages du journal système, vous devez configurer la journalisation des diagnostics dans **Device (Périphérique)** > **Logging Settings (Paramètres de journalisation)**. Configurez un serveur syslog externe afin de pouvoir surveiller les messages de manière fiable.

Exécution à distance des commandes CLI sur l'unité homologue

À partir de l'interface de ligne de commande, vous pouvez entrer des commandes afficher sur le périphérique homologue à l'aide de la commande exec de basculement sans avoir à vous connecter à l'homologue.

failover exec {**active** | **standby** | **mate**} *commande*

Vous devez indiquer quelle unité doit exécuter la commande, qu'elle soit active ou en veille, ou entrer **mate** si vous souhaitez vous assurer que l'autre unité répond au lieu de l'unité à laquelle vous êtes connecté.

Par exemple, si vous souhaitez voir la configuration de l'interface et les statistiques de l'unité homologue, vous pouvez saisir :

```
> failover exec mate show interface
```

Vous ne pouvez pas entrer de commandes **configure**. Cette fonctionnalité est à utiliser avec les commandes **show**.

Remarque Si vous êtes connecté à l'unité active, vous pouvez recharger l'unité de secours à l'aide de la commande **failover reload-standby**.

Vous ne pouvez pas entrer ces commandes par le biais de la console d'interface de ligne de commande Firepower Device Manager.

Dépannage de la haute disponibilité (basculement)

Si les unités d'un groupe à haute disponibilité ne fonctionnent pas comme prévu, tenez compte des étapes suivantes pour résoudre les problèmes de configuration.

Si l'unité active affiche l'unité homologue comme échec, voir Dépannage de l'état de défaillance d'une unité, à la page 44.

Procédure

Étape 1 À partir de chaque périphérique (principal et secondaire) :

- Envoyez un message Ping à l'adresse IP de l'autre périphérique pour la liaison de basculement.
- Envoyez un message Ping à l'adresse IP de l'autre périphérique pour la liaison de basculement dynamique si vous utilisez une liaison distincte.

Si la commande Ping échoue, vérifiez que les interfaces de chaque périphérique sont connectées au même segment de réseau. Si vous utilisez une connexion directe par câble, vérifiez le câble.

Étape 2 Effectuez les vérifications générales suivantes :

- Vérifiez les adresses IP de gestion en double sur les périphériques principal et secondaire.
- Vérifiez les adresses IP de basculement en double et de basculement dynamique sur les unités.
- Vérifiez que le port d'interface équivalent sur chaque périphérique est connecté au même segment de réseau.

Étape 3 Vérifiez la liste des tâches ou le journal d'audit sur le périphérique de secours. Vous devriez voir une tâche « Importation de la configuration à partir du nœud actif » réussie après chaque déploiement réussi sur le périphérique actif. Si la tâche échoue, vérifiez la liaison de basculement et réessayez le déploiement.

Remarque

Si la liste des tâches indique qu'une tâche de déploiement a échoué, il se peut qu'il y ait eu un basculement pendant la tâche de déploiement. Si le périphérique de secours était l'unité active lorsque vous avez lancé la tâche de déploiement, mais qu'un basculement s'est produit pendant la tâche, le déploiement échouera. Pour résoudre le problème, changez de mode pour faire de l'unité de secours l'unité active, puis redéployez les modifications de configuration.

Étape 4 Utilisez la commande **show failover history** pour obtenir des informations détaillées sur les changements d'état d'un périphérique.

Certains éléments à rechercher :

- Échecs de synchronisation des applications :

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

  La phase de synchronisation d'application est l'endroit où la configuration du périphérique actif est transportée vers le périphérique de secours. Un échec de synchronisation de l'application met le périphérique à l'état désactivé, et le périphérique n'est plus disponible pour être activé.

  Si le périphérique est désactivé en raison d'un problème de synchronisation d'application, vous utilisez peut-être des interfaces différentes sur les périphériques pour les points terminaux des liaisons de basculement et de basculement dynamique. Vous devez utiliser le même numéro de port pour chaque extrémité de la liaison.

  Si la commande show failover (afficher le basculement) affiche le périphérique secondaire à l'état Pseudo en veille, cela peut indiquer que vous avez configuré des adresses IP différentes pour la liaison de basculement sur le périphérique secondaire de celles que vous avez configurées sur le périphérique principal. Assurez-vous d'utiliser les mêmes adresses IP principales et secondaires sur les deux périphériques pour la liaison de basculement.

  L'état de pseudo-veille peut également indiquer que vous avez configuré différentes clés IPsec sur les périphériques principal et secondaire.

  Pour d'autres problèmes de synchronisation d'applications, consultez Dépannage des échecs de synchronisation des applications à haute disponibilité, à la page 45.

- Des basculements anormalement fréquents (passant de « actif » à « de secours ») peuvent indiquer des problèmes de liaison de basculement. Dans le pire des cas, les deux unités peuvent devenir actives, ce qui perturbe le trafic. Envoyez un message Ping à chaque extrémité du lien pour vérifier la connectivité. Vous pouvez également utiliser **show arp** pour vérifier que l'adresse IP de basculement et le mappage ARP sont appropriés.

  Si la liaison de basculement est saine et configurée correctement, envisagez d'augmenter l'interrogation de l'homologue et le délai de rétention, l'interrogation et le temps de rétention de l'interface, de réduire le nombre d'interfaces surveillées pour la haute disponibilité ou d'augmenter le seuil d'interface.

- Défaillances dues aux vérifications de l'interface. La raison de la vérification de l'interface comprend une liste des interfaces qui ont été considérées comme ayant échoué. Vérifiez ces interfaces pour vous assurer qu'elles sont correctement configurées et qu'il n'y a aucun problème matériel. Vérifiez qu'il n'y a aucun problème de configuration du commutateur à l'autre extrémité des liaisons. S'il n'y a aucun problème, envisagez de désactiver la surveillance de haute disponibilité sur ces interfaces. Vous pouvez aussi augmenter le seuil de défaillance de l'interface ou le délai associé.

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                          This Host:3

                             admin: inside

                             ctx-1: ctx1-1

                             ctx-2: ctx2-1

                          Other Host:0
```

Étape 5 Si l'unité de secours ne peut pas être détectée et que vous ne trouvez pas de raison précise, comme une mauvaise connexion de réseau local (LAN) ou de câble sur la liaison de basculement, essayez les étapes suivantes.

a) Connectez-vous à l'interface de ligne de commande sur l'unité de secours et entrez la commande **failover reset**. Cette commande devrait faire passer une unité de l'état de défaillance à un état normal. Vérifiez maintenant l'état de HA sur le périphérique actif. Si l'homologue de secours est maintenant détecté, l'opération est terminée.

b) Connectez-vous à l'interface de ligne de commande sur l'unité active et entrez la commande **failover reset**. Cela devrait réinitialiser l'état de HA sur les unités active et de secours. Idéalement, cela rétablira le lien entre les périphériques. Vérifiez l'état de HA ; s'il n'est pas encore correct, poursuivez.

c) Soit à partir de l'interface de ligne de commande sur le périphérique actif, soit à partir de Firepower Device Manager, suspendez d'abord la haute disponibilité, puis réactivez-la. Les commandes CLI sont **configure high-availability suspend** et **configure high-availability resume**.

d) Si ces étapes échouent, **reboot** le périphérique de secours.

Dépannage de l'état de défaillance d'une unité

Si une unité est marquée comme échec dans l'état de haute accessibilité de l'unité homologue (sur la page **Device (Périphérique)** ou **Device (Périphérique)** > **(High Availability (Haute accessibilité)**), voici les raisons générales possibles en fonction de l'unité A étant l'unité active et de l'unité B étant l'homologue défaillant.

- Si l'unité B n'a pas encore été configurée pour la haute accessibilité (elle est toujours en mode Standalone (Autonome)), l'unité A l'affiche comme Failed (Échec).
- Si vous suspendez la haute accessibilité sur l'unité B, l'unité A l'affichera comme Failed (Échec).
- Si vous redémarrez l'unité B, l'unité A l'affichera comme Failed (Échec) jusqu'à ce que l'unité B termine le redémarrage et reprenne la communication sur la liaison de basculement.
- Si la synchronisation de l'application (App Sync) échoue sur l'unité B, l'unité A l'affichera comme Failed (Échec). Consultez Dépannage des échecs de synchronisation des applications à haute disponibilité, à la page 45.
- Si l'unité B échoue dans la surveillance de l'intégrité de l'unité ou de l'interface, l'unité A le marque comme ayant échoué. Vérifiez l'unité B pour détecter les problèmes système. Essayez de redémarrer le périphérique. Si l'unité présente globalement une intégrité satisfaisante, envisagez d'assouplir les

paramètres de surveillance de l'intégrité de l'unité ou de l'interface. La sortie de **show failover history** devrait fournir des informations sur les échecs de contrôle d'intégrité de l'interface.

- Si les deux unités deviennent actives, chaque unité affichera l'homologue comme ayant échoué. Cela indique généralement un problème de liaison de basculement.

  Cela peut également indiquer un problème de licence. Les périphériques doivent avoir une licence cohérente, soit en mode d'évaluation, soit enregistrée. S'ils sont enregistrés, les comptes de licences Smart utilisés peuvent être différents, mais les deux comptes doivent avoir la même sélection pour les fonctionnalités contrôlées à l'exportation, qu'elles soient activées ou désactivées. Si vous configurez une clé de chiffrement IPsec avec des paramètres incohérents pour les fonctionnalités contrôlées à l'exportation, les deux appareils deviendront actifs après l'activation de la haute accessibilité. Cela aura une incidence sur le routage des segments de réseau pris en charge, et vous devrez interrompre manuellement la haute accessibilité sur l'unité secondaire pour récupérer.

Dépannage des échecs de synchronisation des applications à haute disponibilité

Si l'unité homologue ne parvient pas à rejoindre le groupe à haute disponibilité, ou si elle échoue pendant que vous déployez des modifications à partir de l'unité active, connectez-vous à l'unité défaillante, accédez à la page **High Availability** (Haute disponibilité), puis cliquez sur le lien **Failover History** (Historique de basculement). Si la sortie **show failover history** indique un échec de synchronisation d'application, il y a eu un problème pendant la phase de validation de la haute disponibilité, où le système vérifie que les unités peuvent fonctionner correctement en tant que groupe de haute disponibilité.

Ce type de défaillance peut ressembler à ce qui suit :

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
App Sync                  Disabled                  CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

Idéalement, vous souhaitez voir le message « Toute la validation a été transmise » lorsque l'état de provenance est Synchronisation d'application, et le nœud atteindra l'état prêt en veille. Tout échec de validation fera passer l'homologue à l'état désactivé (échec). Vous devez résoudre les problèmes pour que les homologues fonctionnent à nouveau en tant que groupe à haute disponibilité. Notez que si vous corrigez une erreur de synchronisation d'applications en modifiant l'unité active, vous devez les déployer, puis relancer la haute disponibilité pour que le nœud homologue se joigne.

Les messages suivants indiquent les échecs, avec une explication de la façon dont vous pouvez résoudre les problèmes. Ces erreurs peuvent se produire lors de la jonction de nœuds et lors de chaque déploiement ultérieur. Lors de la jonction de nœuds, le système effectue une vérification par rapport à la dernière configuration déployée sur l'unité active.

- Incompatibilité du mode d'enregistrement de licence entre le nœud principal et le nœud secondaire.

  L'erreur de licence indique qu'un homologue est enregistré alors que l'autre homologue est en mode d'évaluation. Les homologues doivent être tous deux enregistrés ou en mode d'évaluation pour qu'ils rejoignent un groupe à haute disponibilité. Comme vous ne pouvez pas faire revenir un périphérique enregistré en mode d'évaluation, vous devez enregistrer l'autre homologue à partir de la page **Device (Périphérique)** > **Smart License (Licence Smart)**.

  Si le périphérique que vous enregistrez est l'unité active, après l'enregistrement du périphérique, effectuez un déploiement. Le déploiement force les unités à actualiser et à synchroniser les configurations, ce qui devrait permettre à l'unité secondaire de rejoindre correctement le groupe de haute disponibilité.

- Incompatibilité de conformité d'exportation de licences entre le nœud principal et le nœud secondaire.

  L'erreur de conformité de licence indique que les périphériques sont enregistrés sur différents comptes Cisco Smart Software Manager, et qu'un compte est activé pour la fonctionnalité contrôlée à l'exportation, alors que l'autre ne l'est pas. Les périphériques doivent être enregistrés avec des comptes qui ont le même paramètre, activé ou désactivé, pour la fonctionnalité contrôlée à l'exportation. Modifiez l'enregistrement du périphérique sur la page **Device (Périphérique)** > **Smart License (Licence Smart)**.

- Disparité de version logicielle entre le nœud principal et le nœud secondaire.

  L'erreur d'incompatibilité de version logicielle indique que les homologues exécutent des versions différentes du logiciel Firewall Threat Defense. Le système n'autorise une incompatibilité que temporairement, pendant que vous installez des mises à niveau logicielles, un périphérique à la fois. Cependant, vous ne pouvez pas déployer les modifications de configuration entre la mise à niveau des homologues. Pour résoudre ce problème, mettez à niveau l'homologue, puis reprenez le déploiement.

- Incompatibilité des interfaces physiques entre le nœud principal et le nœud secondaire.

  L'unité de secours dans un groupe à haute disponibilité doit avoir toutes les interfaces physiques qui existent sur l'unité active, et ces interfaces doivent avoir les mêmes noms de matériel et les mêmes types (comme GigabitEthernet1/1). Cette erreur indique qu'il manque dans l'unité de secours certaines interfaces présentes dans l'unité active. Vous êtes autorisé à avoir plus d'interfaces sur l'unité de secours que sur l'unité active ; vous pouvez donc soit permuter l'unité active, soit choisir une autre unité homologue. Cependant, une incompatibilité d'interfaces ne devrait être que temporaire, par exemple si vous remplacez un module d'interface sur une unité et que vous devez la faire fonctionner sans ce module pendant une courte période. Pour le fonctionnement normal, les deux unités doivent avoir le même nombre et les mêmes types d'interfaces.

- Incompatibilité d'interface de liaison de basculement entre le nœud principal et le nœud secondaire.

  Lorsque vous liez l'interface physique de basculement au réseau sur chaque unité, vous devez choisir la même interface physique. Par exemple, GigabitEthernet1/8 sur chaque unité. Cette erreur indique que vous avez utilisé des interfaces différentes. Pour résoudre l'erreur, corrigez le câblage sur l'unité homologue.

- Incompatibilité d'interface de liaison de basculement dynamique entre le nœud principal et le nœud secondaire.

  Si vous utilisez une liaison de basculement dynamique distincte, lorsque vous liez l'interface physique de basculement dynamique au réseau sur chaque unité, vous devez choisir la même interface physique.

Par exemple, GigabitEthernet1/7 sur chaque unité. Cette erreur indique que vous avez utilisé des interfaces différentes. Pour résoudre l'erreur, corrigez le câblage sur l'unité homologue.

- Incompatibilité des interfaces membres d'EtherChannel du lien de basculement/de basculement dynamique entre le nœud principal et le nœud secondaire

  Si vous sélectionnez une interface EtherChannel pour les interfaces de basculement ou de basculement dynamique, les EtherChannels doivent avoir le même ID et les mêmes interfaces membres sur chaque périphérique. Ce message d'erreur indique s'il s'agit du basculement ou de la liaison de basculement dynamique qui présente l'incompatibilité. Pour résoudre l'erreur, corrigez la configuration des interfaces EtherChannel de manière à ce qu'elles utilisent le même ID et incluent les mêmes interfaces sur chaque périphérique.

- Disparité du numéro de modèle du périphérique entre le nœud principal et le nœud secondaire.

  Pour que les homologues rejoignent un groupe à haute disponibilité, ils doivent être des périphériques exactement du même modèle. Cette erreur indique que les homologues ne sont pas du même modèle de périphérique. Vous devez choisir un autre homologue pour configurer la haute disponibilité.

- Les nœuds actifs et de secours ne peuvent pas se trouver sur le même châssis.

  Vous ne pouvez pas configurer la haute disponibilité à l'aide de périphériques hébergés sur le même châssis matériel. Lors de la configuration de la haute disponibilité sur des modèles qui prennent en charge plusieurs périphériques sur le même châssis, vous devez sélectionner des périphériques qui résident sur du matériel distinct.

- Une erreur inconnue s'est produite, veuillez réessayer.

  Une erreur s'est produite lors de la synchronisation de l'application, mais le système n'a pas pu identifier le problème. Essayez de déployer la configuration à nouveau.

- Le paquet de règles est corrompu. Veuillez mettre à jour le paquet de règles et réessayer.

  Il y a un problème avec la base de données des règles de prévention des intrusions. Sur l'homologue défaillant, accédez à **Device (Périphérique)** > **Updates (Mises à jour)**, puis cliquez sur **Update Now (Mettre à jour maintenant)** dans le groupe **Rule (Règle)**. Attendez que la mise à jour soit terminée et déployez les modifications. Vous pouvez ensuite réessayer le déploiement à partir de l'unité active.

- Incompatibilité de l'état d'inscription du service en nuage entre le nœud principal et le nœud secondaire.

  L'un des nœuds est inscrit au nuage Cisco, mais l'autre n'est pas inscrit. Les deux nœuds doivent être inscrits ou aucun ne peut être inscrit pour former un groupe à haute disponibilité. Accédez à **Device (Périphérique)** > **System Settings (Paramètres du système)** > **Cloud Services (Services en nuage)** sur chacun des périphériques et assurez-vous que les deux périphériques sont inscrits dans la même région Cloud Services.

- Les nœuds Actif et de secours ne peuvent pas avoir de régions de nuage différentes.

  Les appareils sont enregistrés dans différentes régions de services en nuage Cisco. Déterminez quelle région est correcte, annulez l'enregistrement de l'autre périphérique des licences Smart et sélectionnez la région correcte lors du réenregistrement. Si les deux périphériques ont la mauvaise région, annulez l'enregistrement des deux périphériques et réenregistrez-les dans la bonne région.

- Le paquet de déploiement est corrompu. Veuillez réessayer.

  Il s'agit d'une erreur de système interne. Réessayez le déploiement, ce qui devrait résoudre le problème.

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.