Basculement pour la haute disponibilité

Ce chapitre décrit comment configurer le basculement actif/en attente ou actif/actif pour une haute disponibilité de l'ASA.

À propos du basculement

La configuration du basculement nécessite deux ASA identiques connectés l'un à l'autre par une liaison de basculement dédiée et, éventuellement, un lien d'état. L'intégrité des unités actives et des interfaces est supervisée pour déterminer si elles répondent aux conditions de basculement spécifiques. Si ces conditions sont remplies, le basculement se produit.

Modes de basculement

L'ASA prend en charge deux modes de basculement : le basculement actif/actif et le basculement actif/veille. Chaque mode de basculement a sa propre méthode pour déterminer et effectuer le basculement.

- Dans le basculement actif/veille, un périphérique agit en tant qu'unité active et achemine le trafic. Le deuxième périphérique, désigné comme unité de veille, ne transmet pas activement le trafic. Lors d'un basculement, l'unité active est remplacée par l'unité de veille, qui devient alors active. Vous pouvez utiliser le basculement actif/veille pour les ASA en mode de contexte unique ou multiple.
- Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en 2 *groupes de basculement*. Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité.

Un groupe est attribué pour être actif sur l'ASA principal, et l'autre groupe est attribué pour être actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement.

Les deux modes de basculement prennent en charge le basculement avec ou sans état.

Configuration système requise pour Failover (basculement)

Cette section décrit les exigences matérielles, logicielles et de licence pour les périphériques ASA dans une configuration Failover (basculement).

Configuration matérielle requise

Les deux unités dans une configuration Failover (basculement) doivent :

- être du même modèle.

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

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

  Pour le Firepower 2100 en mode Plateforme et Châssis Firepower 4100/9300 , toutes les interfaces doivent être préconfigurées en FXOS de manière identique avant d'activer Failover (basculement). Si vous modifiez les interfaces après avoir activé Failover (basculement), modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active. Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

- Ayez les mêmes modules installés (le cas échéant);

- Ayez la même RAM installée.

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

Configuration logicielle requise

Les deux unités dans une configuration Failover (basculement) doivent :

- Être dans le même mode de contexte (simple ou multiple).

- Pour le mode unique : utilisez le même mode de pare-feu (routage ou transparent).

  Dans le mode de contexte multiple, le mode de pare-feu est défini au niveau du contexte et vous pouvez utiliser des modes mixtes.

- Avoir les mêmes version majeure (premier numéro) et mineure (deuxième numéro). Cependant, vous pouvez utiliser temporairement différentes versions du logiciel au cours d'un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 8.3(1) à la version 8.3(2) et faire en sorte que le basculement reste actif. Nous vous recommandons de mettre à niveau les deux unités à la même version pour assurer la compatibilité à long terme.
- Avoir les mêmes images Secure Client (services client sécurisés). Si les images de la paire de basculement ne concordent pas lorsqu'une mise à niveau sans appel est effectuée, la connexion du VPN SSL sans client s'interrompt à l'étape de redémarrage final du processus de mise à niveau, la base de données affiche une session orpheline et l'ensemble d'adresses IP indique que l'adresse IP attribuée au le client est « en cours d'utilisation ».
- Être dans le même mode FIPS.
- (Firepower 4100/9300) ont le même mode de déchargement de flux, activé ou désactivé.

Exigences de licence

Il n'est pas nécessaire que les deux unités d'une configuration de basculement aient des licences identiques; les licences se combinent pour créer une licence de grappe de basculement.

Liens de basculement et de basculement avec état

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

Mise en garde Toutes les informations envoyées sur les liens de basculement et d'état sont envoyées en texte clair, sauf si vous sécurisez la communication avec un tunnel IPsec ou une clé de basculement. Si l'ASA est utilisé pour mettre fin à des tunnels VPN, cette information comprend les noms d'utilisateur, les mots de passe et les clés prépartagées utilisés pour l'établissement des tunnels. La transmission de ces données sensibles en texte clair peut présenter un risque de sécurité important. Nous vous recommandons de sécuriser la communication de basculement avec un tunnel IPsec ou une clé de basculement si vous utilisez l'ASA pour mettre fin aux tunnels VPN.

Lien de basculement

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

Données de la liaison de basculement

Les informations suivantes sont transmises par la liaison de basculement :

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

- Réplication et synchronisation de la configuration

Interface de la liaison de basculement

Vous pouvez utiliser une interface de données inutilisée (physique, sous-interface 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). Pour la plupart des modèles, vous ne pouvez pas utiliser une interface de gestion pour le basculement, à moins que cela ne soit explicitement décrit ci-dessous.

Le ASA ne prend pas en charge les interfaces de partage entre les données de l'utilisateur et le lien de basculement. Vous ne pouvez pas non plus utiliser des sous-interfaces distinctes sur le même parent pour la liaison de basculement et pour les données.

Consultez les consignes suivantes concernant la liaison de basculement :

- 5506-X à 5555-X : vous ne pouvez pas utiliser l'interface de gestion comme liaison de basculement; vous devez utiliser une interface de données. La seule exception est pour le modèle 5506H-X, où vous pouvez utiliser l'interface de gestion comme liaison de basculement.
- 5506H-X : vous *pouvez* utiliser l'interface de gestion Management 1/1 comme liaison de basculement. Si vous le configurez pour le basculement, vous devez recharger le périphérique pour que la modification prenne effet. Dans ce cas, vous ne pouvez pas également utiliser le module ASA Firepower, car il nécessite l'interface de gestion à des fins de gestion.
- Firepower 4100/9300 : vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement.
- Consultez les lignes directrices suivantes pour dimensionner la liaison.

Tableau 1 : Taille de la liaison de basculement

Modèle	Taille de l'interface pour la liaison combinée de basculement et d'état
Firepower 1010	1 Gbit/sec
Firepower 1100	1 Gbit/sec
Firepower de la série 2100	1 Gbit/sec
Secure Firewall 3100	Secure Firewall 3105, 1 Gbit/s Secure Firewall 3110, 1 Gbit/s Secure Firewall 3120, 1 Gbit/s Secure Firewall 3130, 10 Gbit/s Secure Firewall 3140, 10 Gbit/s
Firepower 4100	10 Gbit/s
Firepower 9300	10 Gbit/s

La fréquence d'alternance est égale au temps de maintien de l'unité (la commande **failover polltime unit**).

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

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

Connexion de la liaison de basculement

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

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

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

LeASA Firewall Threat Defense prend en charge Auto-MDI/MDIX sur ses ports Ethernet en cuivre, vous pouvez donc utiliser un câble croisé ou droit. Si vous utilisez un câble droit, l'interface détecte automatiquement le câble et échange l'une des paires de transmission/réception contre MDIX.

Lien de basculement dynamique

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

Partagé avec la liaison de basculement

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

Interface dédiée

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

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

Éviter le basculement interrompu et les liaisons de données

Nous recommandons que les liens de basculement et les interfaces de données empruntent différentes voies pour réduire le risque d'échec de toutes les interfaces en même temps. Si la liaison de basculement est hors service, l'ASA 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 ASA, quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux ASA deviennent actifs. Par conséquent, les deux méthodes de connexion illustrées dans les figures suivantes ne sont PAS conseillées.

Illustration 1 : Connexion avec un commutateur unique : non recommandée

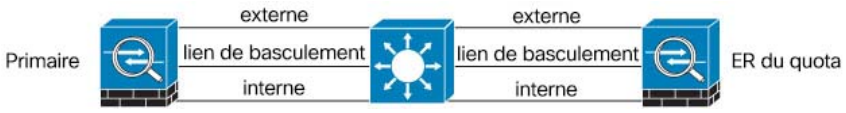


Illustration 2 : Connexion avec un double commutateur : non recommandée

Scénario 2 (recommandé)

Nous conseillons que les liaisons 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

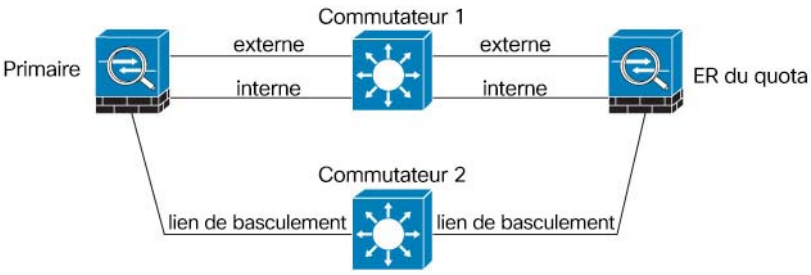
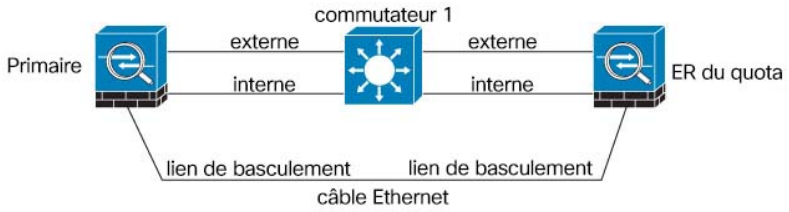


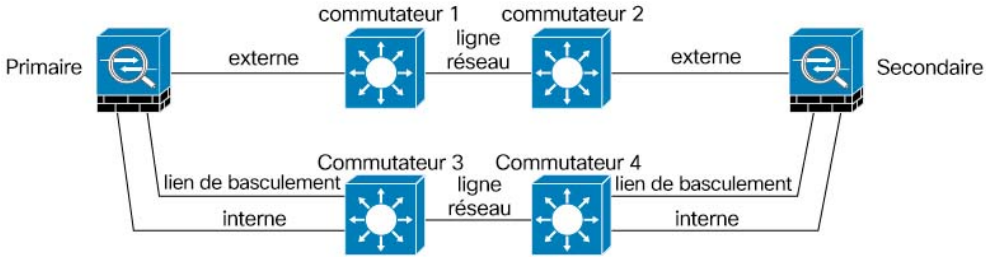
Illustration 4 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données ASA 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



Les adresses MAC et les adresses IP en Failover (basculement)

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

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

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

Adresses IP et adresses MAC actives/en attente

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

1. L'unité active utilise toujours les adresses IP et MAC de l'unité principale.
2. Lorsque l'unité active bascule, l'unité en veille adopte les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.

3. Lorsque l'unité défaillante est remise en ligne, elle est maintenant en état de veille et prend le relais des adresses IP et MAC de secours.

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

Si vous désactivez le basculement et définissez les configurations de basculement à un état désactivé, vous devrez reprendre manuellement le basculement ou redémarrer le périphérique. Il est conseillé d'utiliser la commande **failover reset** et de reprendre le basculement au lieu de redémarrer le périphérique. Si vous rechargez l'unité de secours avec la configuration de basculement désactivée, l'unité de secours démarre en tant qu'unité active et utilise les adresses IP et MAC de l'unité principale. Cela conduit à des adresses IP en double et entraîne des perturbations du trafic réseau. Utilisez la commande **failover reset** pour activer le basculement et restaurer le flux de trafic.

Remarque Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.

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

Adresses IP et adresses MAC actives/actives

Pour le basculement actif, consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité principale génère automatiquement des adresses MAC actives et de secours pour toutes les interfaces dans les contextes des groupes de basculement 1 et 2. Vous pouvez également configurer manuellement les adresses MAC au besoin, par exemple en cas de conflit d'adresses MAC.
2. Chaque unité utilise les adresses IP et MAC actives pour son groupe de basculement actif et les adresses de secours pour son groupe de basculement en veille. Par exemple, l'unité principale est active pour le groupe de basculement 1, elle utilise donc les adresses actives pour les contextes du groupe de basculement 1. Elle est en veille pour les contextes du groupe de basculement 2, où elle utilise les adresses de secours.
3. Lors du basculement d'une unité, l'autre unité prend les adresses IP et les adresses MAC actives du groupe de basculement et commence à transmettre le trafic.
4. Lorsque l'unité défaillante est remise en ligne et que vous avez activé l'option de préemption, elle reprend le groupe de basculement.

Adresses MAC virtuelles

L'ASA comporte plusieurs méthodes pour configurer les adresses MAC virtuelles. Nous vous recommandons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible. Les méthodes manuelles comprennent la commande interface mode **mac-address**, la commande **failover mac address** et, pour le basculement actif/actif, la commande failover group mode **mac address**, en plus des méthodes de génération automatique décrites ci-dessous.

En mode de contexte multiple, vous pouvez configurer l'ASA pour générer automatiquement des adresses MAC virtuelles actives et de secours pour les interfaces partagées, et ces affectations sont synchronisées avec l'unité secondaire (voir la commande **mac-address auto**). Pour les interfaces non partagées, vous pouvez définir manuellement les adresses MAC pour le mode actif/veille (le mode actif/actif génère automatiquement les adresses MAC pour toutes les interfaces).

Pour le basculement actif, les adresses MAC virtuelles sont toujours utilisées, avec des valeurs par défaut ou des valeurs que vous pouvez définir par interface.

Mise à jour du tableau d'adresses MAC dans le basculement

Pendant le basculement, le périphérique désigné comme le nouveau périphérique actif génère des paquets de multidiffusion pour chaque entrée d'adresse MAC dans le tableau MAC et les envoie à toutes les interfaces du groupe de ponts. Cette action incite les commutateurs en amont du groupe de ponts à mettre à jour leurs tables de routage avec l'interface du nouveau périphérique actif pour assurer un transfert précis du trafic.

Le temps nécessaire pour générer des paquets de multidiffusion et mettre à jour les tables de routage des commutateurs en amont dépend du nombre d'entrées dans le tableau d'adresses MAC et du nombre d'interfaces du groupe de ponts. Utilisez la commande **show failover statistics state-switch-delay** pour afficher les statistiques relatives aux retards rencontrés lors des événements de basculement.

Basculement avec et sans état

L'ASA prend en charge deux types de basculement, sans état et avec état, pour les modes actif/veille et actif/actif.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état n'est pas conseillé pour le SSL VPN sans client.

Basculement sans état

Lorsqu'un basculement se produit, toutes les connexions actives sont abandonnées. Les clients doivent rétablir les connexions lorsque la nouvelle unité active prend le relais.

Remarque Certains éléments de configuration pour le SSL VPN sans client (comme les signets et la personnalisation) utilisent le sous-système de basculement VPN, qui fait partie du basculement dynamique. Vous devez utiliser le basculement dynamique pour synchroniser ces éléments entre les membres de la paire de basculement. Le basculement sans état (standard) n'est pas conseillé pour le SSL VPN sans client.

Basculement avec état

Lorsque le basculement dynamique est activé , l'unité active transmet en permanence des informations sur l'état de la connexion à l'unité en veille, ou en cas de basculement actif/actif, entre les groupes de basculement actif et de secours. Après un basculement, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications de l'utilisateur final prises en charge ne sont pas tenues de se reconnecter pour conserver la même session de communication.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis à l'ASA de secours :

- table de traduction NAT
- Les connexions et les états TCP et UDP. 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.
- Le tableau de connexion HTTP (sauf si vous activez la duplication HTTP).
- Les états de la connexion HTTP (si la duplication HTTP est activée) : Par défaut, l'ASA ne reproduit pas les informations de session HTTP lorsque le basculement avec état est activé. Nous vous suggérons d'activer la duplication HTTP.
- États de la connexion SCTP Cependant, le basculement avec état de l'inspection SCTP est préférable. Pendant le basculement, si des paquets SACK sont perdus, la nouvelle unité active abandonnera tous les autres paquets dans le désordre dans la file d'attente jusqu'à ce que le paquet manquant soit reçu.
- 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.
- ICMP connection state (état de connexion ICMP) : la duplication de connexion ICMP n'est activée que si l'interface respective est affectée à un groupe de routage dissymétrique.
- 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.
- Sessions Cisco IPSoftPhone : Si un basculement se produit pendant une session Cisco IPSoftPhone active, l'appel reste actif, car les informations sur l'état de la session d'appel sont répliquées sur l'unité de secours. Lorsque l'appel est terminé, le client IPSoftPhone perd la connexion avec Cisco Call Manager. Cette perte de connexion se produit parce qu'il n'y a pas d'informations de session pour le message de raccrochage CTIQBE sur l'unité de secours. Lorsque le client IP SoftPhone ne reçoit pas de réponse du gestionnaire d'appels dans un certain délai, il considère que le gestionnaire d'appels est injoignable et se désenregistre.
- 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 ASA de secours :

- Le tableau d'authentification des utilisateurs (uauth)
- Les connexions de contournement d'état TCP
- Le routage de multidiffusion
- Fonctionnalités sélectionnées du VPN SSL sans client :
  - Tunnels intelligents
  - Transfert de port
  - Modules d'extension
  - Applets Java
  - Sessions IPv6 sans client ou Secure Client (services client sécurisés)
  - Authentification Citrix (les utilisateurs de Citrix doivent se réauthentifier après le basculement)

Exigences en matière de groupes de ponts pour le basculement

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

Exigences en matière de groupes de ponts pour les appareils, ASAv

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 les pertes de trafic lorsque le port est dans un état bloquant, vous pouvez configurer l'une des solutions de contournement suivantes en fonction du mode du port du commutateur :

- Mode d'accès : activez la fonctionnalité STP PortFast sur le commutateur :

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

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

- Mode de liaison : bloquez les BPDU sur l'ASA sur les interfaces membres d'un groupe de ponts avec un critère d'accès EtherType.

  ```
  access-list id ethertype deny bpdu
  access-group id in interface name1
  access-group id in interface name2
  ```

  Le blocage des BPDU désactive le STP sur le commutateur. Assurez-vous de ne pas avoir de boucles concernant l'ASA dans la disposition de votre réseau.

Si aucune des options ci-dessus n'est possible, vous pouvez utiliser l'une des solutions de contournement moins souhaitables suivantes qui a une incidence sur la fonctionnalité de basculement ou la stabilité STP :

- Désactivez la supervision d'interface.
- Augmentez le temps de rétention à une valeur élevée qui permettra au STP de converger avant le basculement des ASA.
- Réduisez les minuteries STP pour permettre au STP de converger plus rapidement que le temps de rétention de l'interface.

Surveillance de l'intégrité du basculement

Le ASA surveille l'intégrité générale et l'intégrité de l'interface de chaque unité. Cette section comprend des informations sur la façon dont leASA effectue les tests pour déterminer l'état de chaque unité.

Surveillance de l'intégrité de l'unité

Le ASA 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. Pour les périphériques Firepower 9300 et 4100, vous pouvez activer la surveillance de la détection de transfert bidirectionnel (BFD), qui est plus fiable que les messages Hello. L'action du ASA dépend de la réponse de l'autre unité. Consultez les exemples d'actions suivantes :

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

Surveillance d'interfaces

Vous pouvez surveiller jusqu'à 1 025 interfaces (en mode contextes multiples, réparties entre tous les contextes). Vous devez surveiller les interfaces importantes. Par exemple, en mode de contexte multiple, vous pouvez configurer un contexte pour surveiller une interface partagée : comme l'interface est partagée, tous les contextes bénéficient de la surveillance.

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes (valeur par défaut), elle exécute des tests d'interface. (Pour modifier la période, consultez la commande **failover polltime interface** ou, pour le basculement actif/actif, la commande **polltime interface**, (Configuration > Gestion du périphérique > Haute disponibilité et évolutivité > Basculement > Critères > Durées d'interrogation du basculement).) Si l'un des tests d'interface échoue pour une interface, mais que cette même interface sur l'autre unité continue de transmettre le trafic avec succès, l'interface est considérée comme ayant échoué et leASA arrête d'exécuter les tests.

Si le seuil que vous avez défini pour le nombre d'interfaces défaillantes est atteint (voir la commande **failover interface-policy**, ou pour le basculement actif/actif, la commande **interface-policy**) et que l'unité active a plus d'interfaces défaillantes que l'unité en attente, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Inconnu » et ne sont pas prises en compte dans la limite de basculement définie par la politique d'interface de basculement.

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

Si une interface a des adresses IPv4 et IPv6 configurées, le ASA utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité. Si une interface n'a que des adresses IPv6 configurées, le ASA 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 ASA utilise l'adresse de tous les nœuds IPv6 (FE02::1).

Remarque Si une unité défaillante ne récupère pas et que vous pensez qu'elle ne devrait pas tomber en panne, vous pouvez réinitialiser l'état en saisissant la commande « **failover reset** ». Si la condition de basculement persiste, l'unité échouera à nouveau.

Tests d'interface

LeASA Firewall Threat Defense utilise les tests d'interface suivants. La durée de chaque test est d'environ 1,5 seconde par défaut, ou de 1/16 du temps d'attente de l'interface de basculement (voir la commande **failover polltime interface** ou, pour le basculement actif/actif, la commande **interface-policy**).

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

État d'interface

Les interfaces surveillées peuvent avoir l'état suivant :

- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- 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.

détection

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

- Plus de 50 % des instances Snort sur l'unité active sont en panne.
- L'espace disque de l'unité active est plein à plus de 90 %.
- La commande **no failover active** est exécutée sur l'unité active ou la commande **failover active** est exécutée sur l'unité de secours.

- L’unité active comporte plus d’interfaces défaillantes que l’unité en veille.
- La défaillance d’interface sur le périphérique actif dépasse le seuil configuré.

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

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

Tableau 2 :

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

Remarque Si vous basculez manuellement à l’aide de l’interface de ligne de commande ou de l’ASDM, ou si vous rechargez l’ASA, le basculement démarre immédiatement et n’est pas soumis aux minuteurs ci-dessous.

Tableau 3 : ASA

la condition de basculement	Minimum	Par défaut	Maximum
L'unité active n'est plus alimentée, le matériel tombe en panne, le logiciel est rechargé ou se bloque. Lorsque l’un de ces événements se produit, les interfaces surveillées ou le lien de basculement ne reçoivent aucun message Hello.	800 milliseconde	15 secondes	45 secondes
Lien de l’interface de la carte principale de l’ unité active en panne.	500 millisecondes	5 secondes	15 secondes
Lien d’interface de module 4GE de l’unité active inactif.	2 secondes	5 secondes	15 secondes
L’interface de l’unité active est active, mais un problème de connexion entraîne des tests d’interface.	5 secondes	25 secondes	75 secondes

Synchronisation de la configuration

Le basculement comprend différents types de synchronisation de configuration.

Réplication de la configuration en cours d'exécution

La réplication de la configuration en cours d'exécution se produit lorsque l'un des périphériques de la paire de basculement ou les deux démarrent.

Dans le basculement actif/veille, les configurations sont toujours synchronisées de l'unité active avec l'unité en veille.

Dans le basculement actif/actif, quelle que soit l'unité de démarrage, elle obtient la configuration en cours d'exécution de l'unité qui démarre en premier, quelle que soit la désignation principale ou secondaire de l'unité de démarrage. Une fois que les deux unités sont opérationnelles, les commandes saisies dans l'espace d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Lorsque l'unité de secours/seconde termine son démarrage initial, elle efface sa configuration en cours d'exécution (à l'exception des commandes **failover** nécessaires pour communiquer avec l'unité active) et l'unité active envoie sa configuration complète à l'unité de secours/seconde. Lorsque la réplication démarre, la console ASA sur l'unité active affiche le message « Début de la réplication de la configuration : envoi à l'unité jumelle » et lorsqu'elle est terminée, l'ASA affiche le message « Fin de la réplication de la configuration vers l'unité jumelle ». Selon la taille de la configuration, la réplication peut prendre de quelques secondes à plusieurs minutes.

Sur l'unité recevant la configuration, la configuration existe uniquement dans la mémoire en cours d'exécution. Vous devez enregistrer la configuration dans la mémoire flash en fonction de Enregistrer les modifications de configuration. Par exemple, dans le basculement actif/actif, saisissez la commande **write memory all** dans l'espace d'exécution du système sur l'unité qui a le groupe de basculement 1 à l'état actif. La commande est répliquée sur l'unité homologue, qui continue d'écrire sa configuration dans la mémoire flash.

Remarque Pendant la réplication, les commandes saisies sur l'unité qui envoie la configuration peuvent ne pas être répliquées correctement sur l'unité homologue, et les commandes saisies sur l'unité qui reçoit la configuration peuvent être remplacées par la configuration en cours de réception. Évitez de saisir des commandes sur l'une ou l'autre des unités de la paire de basculement pendant le processus de réplication de la configuration.

Réplication du fichier

La synchronisation de la configuration ne réplique pas les fichiers et composants de configuration suivants. Vous devez donc copier ces fichiers manuellement pour qu'ils correspondent :

- Images Secure Client (services client sécurisés)
- Images CSD
- Profils Secure Client (services client sécurisés)

  L'ASA utilise un fichier mis en mémoire cache pour le profil Secure Client (services client sécurisés) stocké dans cache:/stc/profiles, et non le fichier stocké dans le système de fichiers flash. Pour répliquer le profil Secure Client (services client sécurisés) sur l'unité en veille, effectuez l'une des opérations suivantes :

- Saisissez la commande **write standby** sur l'unité active.
- Réappliquez le profil sur l'unité active.
- Rechargez l'unité en veille.

- Autorités de certification (CA) locales
- Images ASA
- Images ASDM

Réplication de la commande

Après le démarrage, les commandes que vous saisissez sur l'unité active sont immédiatement répliquées sur l'unité de secours. Vous n'avez pas besoin d'enregistrer la configuration active dans la mémoire flash pour répliquer les commandes.

Dans le basculement actif/actif, des commandes saisies dans l'espace d'exécution du système sont répliquées à partir de l'unité sur laquelle le groupe de basculement 1 est à l'état actif.

Si lesde commandes ne sont pas saisies sur l'unité appropriée pour que la réplication des commandes puisse avoir lieu, les configurations ne seront plus synchronisées. Ces modifications pourraient être perdues lors de la prochaine synchronisation de la configuration initiale.

Les commandes suivantes sont répliquées sur l'ASA de secours :

- Toutes les commandes de configuration, à l'exception de **mode**, **firewall** et **failover lan unit**
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

Les commandes suivantes ne sont *pas* répliquées sur l'ASA de secours :

- Toutes les formes de la commande **copy**, à l'exception de **copy running-config startup-config**
- Toutes les formes de la commande **write**, à l'exception de **write memory**
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** et **pager**

Optimisation de la synchronisation et de la configuration

Lorsqu'un périphérique redémarre ou se reconnecte après une suspension ou une reprise du basculement, le périphérique qui rejoint le nœud efface la configuration en cours d'exécution. Le périphérique actif envoie alors l'intégralité de sa configuration au périphérique en phase de jonction afin de synchroniser complètement les configurations. Si le périphérique actif a une configuration importante, ce processus peut prendre plusieurs minutes.

La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration du périphérique en phase de jonction et du périphérique actif en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les périphériques actifs et en phase de jonction correspond, le périphérique en cours d'adhésion ignore la synchronisation complète de la configuration et rejoint la configuration du basculement. Cette fonctionnalité garantit un appairage plus rapide et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

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

- La fonctionnalité d'optimisation de la synchronisation de la configuration est activée par défaut.
- Le mode de contexte multiple de l'ASA prend en charge l'optimisation de la synchronisation de la configuration en partageant l'ordre des contextes lors de la synchronisation complète de la configuration, ce qui permet la comparaison de l'ordre des contextes lors de la jonction de nœuds suivante.
- Si vous configurez la phrase secrète et la clé IPsec de basculement, l'optimisation de la synchronisation de la configuration n'est pas effective, car la valeur de hachage calculée dans le périphérique actif et le périphérique en veille est différente.
- Si vous configurez le périphérique avec une ACL dynamique ou SNMPv3, l'optimisation de la synchronisation de la configuration n'est pas effective.
- Le périphérique actif synchronise la configuration complète avec le basculement des liaisons LAN comme comportement par défaut. Pendant les oscillations de basculement entre les périphériques actifs et en veille, l'optimisation de la synchronisation de la configuration n'est pas déclenchée et les périphériques effectuent une synchronisation complète de la configuration.
- L'optimisation de la synchronisation de la configuration est déclenchée lorsque la configuration du basculement récupère d'une interruption ou d'une perte de communication réseau entre les périphériques actifs et en veille.

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

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

Utilisez les commandes suivantes pour superviser l'optimisation de la synchronisation de la configuration.

- **show failover config-sync checksum**

  Affiche des informations sur l'état du périphérique et la somme de contrôle.

- **show failover config-sync configuration**

  Affiche des informations sur la configuration du périphérique et la somme de contrôle.

- **show failover config-sync status**

  Affiche l'état de la fonctionnalité d'optimisation de la synchronisation de la configuration.

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un ASA 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. Cependant, vous devez définir l'unité de secours comme unité principale avant de remplacer l'unité défectueuse, afin de conserver la configuration de l'unité secondaire.

Remarque Pour le mode de contexte multiple, l'ASA peut basculer l'unité entière (y compris tous les contextes), mais ne peut pas basculer des contextes individuels séparément.

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. Même sur les systèmes exécutés dans le mode à contextes multiples, vous ne pouvez pas basculer des contextes ou des groupes de contextes.

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 4 : Événements de basculement

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

À propos du basculement actif/actif

Cette section décrit le basculement actif/actif.

Présentation du basculement actif/actif

Dans une configuration de basculement actif/actif, les deux ASA peuvent transmettre le trafic réseau. Le basculement actif/actif n'est disponible que pour les ASA en mode de contexte multiple. Dans le basculement actif/actif, vous divisez les contextes de sécurité sur l'ASA en un maximum de 2 groupes de basculement.

Un groupe de basculement est simplement un groupe logique d'un ou plusieurs contextes de sécurité. Vous pouvez attribuer un groupe de basculement actif sur l'ASA principal et un groupe de basculement 2 actif sur l'ASA secondaire. Lorsqu'un basculement se produit, il se produit au niveau du groupe de basculement. Par exemple, selon le modèle de défaillance d'interface, il est possible que le groupe de basculement 1 bascule vers l'ASA secondaire et que le groupe de basculement 2 bascule vers l'ASA principal. Cet événement peut se produire si les interfaces du groupe de basculement 1 sont inactives sur l'ASA principal, mais actives sur l'ASA secondaire, tandis que les interfaces du groupe de basculement 2 sont inactives sur l'ASA secondaire, mais actives sur l'ASA principal.

Le contexte d'administration est toujours membre du groupe de basculement 1. Tous les contextes de sécurité non attribués sont également membres du groupe de basculement 1 par défaut. Si vous souhaitez bénéficier d'un basculement actif/actif, mais que vous n'êtes pas intéressé par les contextes multiples, la configuration la plus simple serait d'ajouter un contexte supplémentaire et de l'affecter au groupe de basculement 2.

Remarque Lors de la configuration du basculement actif/actif, assurez-vous que le trafic combiné des deux unités entre dans la capacité de chacune d'elles.

Remarque Vous pouvez attribuer les deux groupes de basculement à un seul ASA si vous le souhaitez, mais vous ne profiterez pas de deux ASA actifs.

Rôles principal/secondaire et état actif/de secours pour un groupe de basculement

Comme pour le basculement actif/de secours, une unité d'une paire de basculement actif/actif est désignée comme l'unité principale et l'autre unité, comme l'unité secondaire. Contrairement au basculement actif/de secours, cette désignation n'indique pas quelle unité devient active lorsque les deux unités démarrent simultanément. Au lieu de cela, la désignation principale/secondaire fait deux choses :

- L'unité principale fournit la configuration d'exécution à la paire lorsqu'elles démarrent simultanément.
- Chaque groupe de basculement de la configuration est configuré avec une préférence d'unité principale ou secondaire. Lorsqu'elle est utilisée avec la préemption, cette préférence garantit que le groupe de basculement s'exécute sur la bonne unité après son démarrage. Sans préemption, les deux groupes s'exécutent sur la première unité de démarrage.

Détermination de l'unité active pour les groupes de basculement au démarrage

L'unité sur laquelle un groupe de basculement devient actif est déterminée comme suit :

- Lorsqu'une unité démarre alors que l'unité homologue n'est pas disponible, les deux groupes de basculement deviennent actifs sur l'unité.

- Lorsqu'une unité démarre alors que l'unité homologue est active (avec les deux groupes de basculement à l'état actif), les groupes de basculement restent à l'état actif sur l'unité active, quelle que soit la préférence principale ou secondaire du groupe de basculement jusqu'à ce que l'un des scénarios suivants se produise :
  - Un basculement se produit.
  - Un basculement est forcé manuellement.
  - Une préemption pour le groupe de basculement est configurée, ce qui fait que le groupe de basculement devient automatiquement actif sur l'unité préférée lorsque l'unité devient disponible.

Événements de basculement

Dans une configuration de basculement actif/actif, le basculement se produit sur la base d'un groupe de basculement, et non sur une base de système. Par exemple, si vous désignez les deux groupes de basculement comme actifs sur l'unité principale et que le groupe de basculement 1 échoue, le groupe de basculement 2 reste actif sur l'unité principale pendant que le groupe de basculement 1 devient actif sur l'unité secondaire.

Comme un groupe de basculement peut contenir plusieurs contextes et que chaque contexte peut contenir plusieurs interfaces, il est possible que toutes les interfaces d'un contexte unique tombent en panne sans entraîner la défaillance du groupe de basculement associé.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque événement de défaillance, la politique (que le basculement se produise ou non), les actions pour le groupe de basculement actif et les actions pour le groupe de basculement en veille sont données.

Tableau 5 : Événements de basculement

Défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Une unité subit une défaillance d'alimentation ou de logiciel	Basculement	Devient l'unité de secours Marquer comme défaillante	Devenir active Marquer l'unité active comme défaillante	Lorsqu'une unité d'une paire de basculement tombe en panne, tous les groupes de basculement actifs sur cette unité sont marqués comme défaillants et deviennent actifs sur l'unité homologue.
Défaillance de l'interface sur le groupe de basculement actif supérieure au seuil	Basculement	Marquer le groupe actif comme défaillant	Devenir active	Aucun.
Défaillance de l'interface sur le groupe de basculement en veille supérieure au seuil	Aucun basculement	Aucune action	Marquer le groupe en veille comme défaillant	Lorsque le groupe de basculement en veille est marqué comme défaillant, le groupe de basculement actif ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Le groupe de basculement anciennement actif récupère	Aucun basculement	Aucune action	Aucune action	À moins que la préemption de groupe de basculement ne soit configurée, les groupes de basculement restent actifs sur leur unité actuelle.

Défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active	Devenir active	Si la liaison de basculement est interrompue au démarrage, les deux groupes de basculement sur les deux unités deviennent actifs.
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.
Échec du la liaison de basculement pendant l'opération	Aucun basculement	S.O.	S.O.	Chaque unité marque 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.

Licences pour le basculement

Pour la plupart des modèles, les unités de basculement ne nécessitent pas la même licence sur chaque unité. Si vous avez des licences sur les deux unités, elles se combinent en une seule licence de grappe de basculement d'exécution. Il y a certaines exceptions à cette règle. Consultez le tableau suivant pour connaître les exigences précises en matière de licence pour le basculement.

Modèle	Exigence de licence
ASA virtuel	Consultez Licences de basculement pour l'ASAv.
Firepower 1010	Licence Security Plus sur les deux unités. Consultez Licences de basculement pour Firepower 1010.
Firepower 1100	Consultez Licences de basculement pour Firepower 1100.
Firepower de la série 2100	Consultez Licences de basculement pour Firepower 2100.
Cisco Secure Firewall 3100	Consultez Licences de basculement pour Cisco Secure Firewall 3100.
Firepower 4100/9300	Consultez Licences de basculement pour l'Firepower 4100/9300.
ISA 3000	Licence Security Plus sur les deux unités. **Remarque** Chaque unité doit avoir la même licence de chiffrement.

Remarque Une clé permanente valide est requise; dans de rares cas sur l'ISA 3000, votre clé d'authentification PAK peut être supprimée. Si votre clé est constituée uniquement de 0, vous devez réinstaller une clé d'authentification valide avant que le basculement puisse être activé.

Lignes directrices pour Failover (basculement)

Mode contextuel

- Le mode Actif/Actif est pris en charge uniquement en mode de contexte multiple.
- Pour le mode de contexte multiple, effectuez toutes les étapes dans l'espace d'exécution du système, sauf indication contraire.

Prise en charge des modèles

- Firepower 1010 :
  - Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Failover (basculement). 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. Failover (basculement) 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 Failover (basculement) 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 Failover (basculement) 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 liaison de basculement.
- Firepower 9300 : nous vous recommandons d'utiliser le basculement entre les châssis pour une redondance optimale.
- Les ASA virtuel sur les réseaux infonuagiques publics tels que Microsoft Azure et Amazon Web Services ne sont pas pris en charge par Failover (basculement) standard, car une connectivité de couche 2 est requise. Au lieu de cela, consultez Basculement pour la haute disponibilité dans le nuage public.

Basculement ASA virtuel pour la haute disponibilité

Lors de la création d'une paire de basculement à l'aide de l'ASA virtuel, il est nécessaire d'ajouter les interfaces de données à chaque ASA virtuel dans le même ordre. Si exactement les mêmes interfaces sont ajoutées à chaque ASA virtuel, mais dans un ordre différent, des erreurs peuvent s'afficher à la console ASA virtuel. La fonctionnalité de basculement peut également être affectée

Directives supplémentaires

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

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

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

- La configuration de la sécurité des ports sur les commutateurs connectés à la paire de basculement ASA 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.
- Vous pouvez surveiller jusqu'à 1 025 interfaces sur une unité, dans tous les contextes.
- Pour un tunnel Failover (basculement) actif/en veille et un tunnel VPN IPsec, vous ne pouvez pas surveiller les unités active et en veille à l'aide de SNMP sur le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et abandonnera le trafic destiné au système NMS. Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.
- Pour le basculement actif/actif, deux interfaces dans le même contexte ne doivent pas être configurées dans le même groupe ASR.
- Pour le basculement actif/actif, vous pouvez définir un maximum de deux groupes de basculement.
- Pour le basculement actif/actif, lors de la suppression de groupes de basculement, vous devez supprimer le groupe de basculement 1 en dernier. Le groupe de basculement1 contient toujours le contexte d'administration. Tout contexte non affecté à un groupe de basculement passe par défaut au groupe de basculement 1. Vous ne pouvez pas supprimer un groupe de basculement auquel des contextes sont affectés explicitement.
- Immédiatement après le basculement, l'adresse source des messages du journal système sera l'adresse de l'interface de basculement pendant quelques secondes.
- Pour une meilleure convergence (pendant un basculement), vous devez fermer les interfaces sur une paire à haute disponibilité qui ne sont associées à aucune configuration ou instance.
- Si vous configurez le chiffrement de basculement en mode d'évaluation, les systèmes utilisent DES pour le chiffrement. Si vous enregistrez ensuite les périphériques à l'aide d'un compte compatible avec l'exportation, ils utiliseront AES après un redémarrage. Ainsi, si un système redémarre pour une raison quelconque, y compris après l'installation d'une mise à niveau, les homologues ne pourront pas communiquer et les deux unités deviendront l'unité active. Nous vous recommandons de ne pas configurer le chiffrement avant d'avoir enregistré les périphériques. Si vous configurez cela en mode d'évaluation, nous vous recommandons de supprimer le chiffrement avant d'enregistrer les périphériques.
- Lorsque vous utilisez SNMPv3 avec basculement, si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité active pour forcer les utilisateurs à se reproduire sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité. Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité active ou directement sur l'unité de secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

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

  Exemple :

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

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

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

- Les unités de Failover (basculement) ne synchronisent pas l'horloge de manière dynamique. Voici quelques exemples d'événements où la synchronisation a lieu :
  - Une nouvelle paire Failover (basculement) est créée.
  - La paire Failover (basculement) est défectueuse et recréée.
  - La communication sur la liaison de basculement a été interrompue et rétablie.
  - L'état de basculement a été modifié manuellement au niveau de l'interface de ligne de commande (CLI) .
- L'activation de Failover (basculement) force la suppression de toutes les routes et leur rajout après le passage de la progression de Failover (basculement) à l'état actif. Vous pourriez subir des pertes de connexion pendant cette phase.
- Si vous activez le basculement sur un périphérique autonome, les interfaces de données tombent en panne lors de la négociation du basculement, interrompant le trafic.
- Dans la configuration Failover (basculement), les connexions de courte durée, généralement qui utilisent le port 53, sont fermées rapidement et ne sont jamais transférées ou synchronisées de la position active à la zone en veille, il peut donc y avoir une différence dans le nombre de connexions sur les deux périphériques Failover (basculement). C'est un comportement attendu pour les connexions de courte durée. Vous pouvez essayer de comparer les connexions qui sont de longue durée (par exemple, plus de 30 à 60 secondes).
- Dans la configuration Failover (basculement), les connexions amorces (demandes de connexion qui n'ont pas encore terminé le processus d'établissement de liaison à trois étapes) sont fermées rapidement et ne sont pas synchronisées entre les périphériques actifs et en veille. Cette conception garantit l'efficacité et

la sécurité du système à haute disponibilité. Pour cette raison, il pourrait y avoir une différence dans le nombre de connexions sur les deux périphériques Failover (basculement), ce qui est attendu.

- Si la liaison LAN de basculement n'est pas connectée dos à dos, mais plutôt connectée par un ou plusieurs commutateurs, une défaillance dans le chemin intermédiaire peut faire que l'unité active perde la connectivité avec l'unité de secours, ce qui entraîne des états actif/veille incohérents. Bien que cela n'ait pas d'incidence sur la fonctionnalité Failover (basculement), il est conseillé de vérifier et de récupérer le chemin de liaison de basculement entre les unités actives et de secours.

  Lorsque la liaison LAN de basculement est inactive, il n'est pas conseillé de déployer une configuration, car elle pourrait ne pas être répliquée sur l'unité homologue.
- Dans OSPF dans l'ASA, si un commutateur à proximité tombe en panne et si l'interface ASA est connectée au même commutateur, les interfaces du pare-feu tombent également en panne avec la défaillance du commutateur. Il s'agit d'un comportement attendu. Cela déclenchera un basculement de haute disponibilité, comme prévu.
- Si l'ASA en veille est connecté à un autre commutateur, par exemple, lorsque l'interface sera activée, les tables de routage seront différentes de celle de l'ASA actif. Cela entraînera une panne de courte durée (environ 15 à 17 secondes) jusqu'à ce que les routes et la contiguïté soient mises à jour.
- En mode transparent, si vous avez des problèmes avec l'unité active qui perd l'adresse MAC du routeur de secours (HSRP), créez un mappage statique pour l'adresse MAC.

Paramètres par défaut pour le basculement

Par défaut, la politique de basculement comprend les éléments suivants :

- Aucune réplication HTTP dans le basculement dynamique.
- La défaillance d'une seule interface entraîne le basculement.
- Le délai d'interrogation de l'interface est de 5 secondes.
- Le délai de rétention de l'interface est de 25 secondes.
- Le délai d'interrogation de l'unité est de 1 seconde.
- Le délai de rétention de l'unité est de 15 secondes.
- Les adresses MAC virtuelles sont désactivées en mode de contexte multiple.
- Supervision de toutes les interfaces physiques.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/veille, configurez les paramètres de basculement de base sur les unités principale et secondaire. Toutes les autres configurations se produisent uniquement sur l'unité principale et sont ensuite synchronisées avec l'unité secondaire.

Configurer l'unité principale pour le basculement actif/de secours

Suivez les étapes de cette section pour configurer l'unité principale dans une configuration de basculement actif/veille. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

- Nous vous conseillons de configurer les adresses IP en veille pour toutes les interfaces, à l'exception des liaisons de basculement et d'état. Si vous utilisez un filtre d'adresse locale de 31 bits pour les connexions point à point, ne configurez pas d'adresse IP en veille. Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Désignez cette unité comme unité principale :

failover lan unit primary

Étape 2 Spécifiez l'interface à utiliser comme liaison de basculement :

failover lan interface *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

Cette interface ne peut pas être utilisée à d'autres fins (sauf, éventuellement, pour la liaison d'état).

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique de données, une sous-interface ou un ID d'interface EtherChannel. Sur Firepower 1010, l'interface est un ID d'interface de pare-feu; vous ne pouvez pas spécifier d'ID de port de commutation ni d'ID de VLAN. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.

Étape 3 Attribuez les adresses IP actives et en veille à la liaison de basculement :

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Ou :

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
```

```
2001:a0a:b00::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Étape 4 Activez la liaison de basculement :

interface *failover_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

Étape 5 (Facultatif) Si vous souhaitez utiliser une interface distincte pour la liaison d'état, spécifiez l'interface.

failover link *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover link folink gigabitethernet0/4
```

Si vous ne spécifiez pas d'interface distincte, la liaison de basculement est utilisée pour la liaison d'état.

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel. Sur Firepower 1010, l'interface est un ID d'interface de pare-feu; vous ne pouvez pas spécifier d'ID de port de commutation ni d'ID de VLAN.

Étape 6 Si vous avez spécifié une liaison d'état distincte, attribuez les adresses IP actives et en veille à cette liaison d'état :

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

Ou :

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Ignorez cette étape si vous partagez la liaison d'état.

Étape 7 Si vous avez spécifié une liaison d'état distincte, activez cette dernière.

interface *state_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

Ignorez cette étape si vous partagez la liaison d'état.

Étape 8 (Facultatif) Effectuez l'une des opérations suivantes pour chiffrer les communications sur les liaisons de basculement et d'état :

- (Privilégié) Établissez des tunnels IPsec LAN à LAN sur les liaisons de basculement et d'état entre les unités pour chiffrer toutes les communications de basculement :

  failover ipsec pre-shared-key [**0** | **8**] *key*

  Exemple :

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  La *clé* peut comporter jusqu'à 128 caractères. Identifiez la même clé sur les deux unités. La clé est utilisée par IKEv2 pour établir les tunnels.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale), la clé est chiffrée dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que la clé est chiffrée à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  La clé partagée **failover ipsec pre-shared-key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

  Vous ne pouvez pas utiliser à la fois le chiffrement IPsec et le chiffrement **failover key** existant. Si vous configurez les deux méthodes, IPsec est utilisé. Cependant, si vous utilisez la phrase secrète principale, vous devez d'abord supprimer la clé de basculement à l'aide de la commande **no failover key** avant de configurer le chiffrement IPsec.

  Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN).

- (Facultatif) Chiffrez la communication de basculement sur les liaisons de basculement et d'état :

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  Exemple :

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

Utilisez un *shared_secret* de 1 à 63 caractères ou une **hex** *key* de 32 caractères. Pour le *shared_secret*, vous pouvez utiliser n'importe quelle combinaison de chiffres, de lettres ou de ponctuation. Le secret partagé ou la clé hexadécimale est utilisé pour générer la clé de chiffrement. Identifiez la même clé sur les deux unités.

Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale), le secret partagé ou la clé hexadécimale est chiffré dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que le secret partagé ou la clé hexadécimale est chiffré à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

Étape 9 Activez le basculement :

failover

Étape 10 Enregistrez la configuration système dans la mémoire flash :

write memory

Exemples

L'exemple suivant configure les paramètres de basculement pour l'unité principale :

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

Configurer l'unité secondaire pour le basculement actif/de secours

La seule configuration requise sur l'unité secondaire concerne la liaison de basculement. L'unité secondaire exige que ces commandes communiquent initialement avec l'unité principale. Une fois que l'unité principale a envoyé sa configuration à l'unité secondaire, la seule différence permanente entre les deux configurations est la commande **basculement LAN unité**, qui identifie chaque unité comme principale ou secondaire.

Avant de commencer

- Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.

- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Saisissez à nouveau les mêmes commandes que sur l'unité principale, *à l'exception* de la commande **basculement LAN unité principale**. Vous pouvez éventuellement la remplacer par la commande **basculement LAN unité secondaire**, mais ce n'est pas nécessaire, car **le paramètre secondaire** est le paramètre par défaut. Consultez Configurer l'unité principale pour le basculement actif/de secours, à la page 28.

Par exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

Étape 2 Après la synchronisation de la configuration de basculement, enregistrez la configuration dans la mémoire flash :

```
ciscoasa(config)# write memory
```

Configurer le basculement actif/actif

Cette section explique comment configurer le basculement actif/actif.

Configurer l'unité principale pour le basculement actif/actif

Suivez les étapes de cette section pour configurer l'unité principale dans une configuration de basculement actif/actif. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

- Activez ou désactivez le mode de contexte multiple conformément à Activer ou désactiver le mode de contexte multiple.
- Nous vous conseillons de configurer les adresses IP en veille pour toutes les interfaces, à l'exception des liaisons de basculement et d'état conformément à Interfaces en mode routage et en mode transparent. Si vous utilisez un filtre d'adresse locale de 31 bits pour les connexions point à point, ne configurez pas d'adresse IP en veille. Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.

- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Désignez cette unité comme unité principale :

failover lan unit primary

Étape 2 Spécifiez l'interface à utiliser comme liaison de basculement :

failover lan interface *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

Cette interface ne peut pas être utilisée à d'autres fins (sauf, éventuellement, pour la liaison d'état).

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel. Pour le Firepower 4100/9300, vous pouvez utiliser n'importe quelle interface de type de données.

Étape 3 Attribuez les adresses IP actives et en veille à la liaison de basculement :

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Ou :

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Étape 4 Activez la liaison de basculement :

interface *failover_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/3
```

```
ciscoasa(config-if)# no shutdown
```

Étape 5 (Facultatif) Si vous souhaitez utiliser une interface distincte pour la liaison d'état, spécifiez l'interface.

failover link *if_name interface_id*

Exemple :

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

Nous vous conseillons d'utiliser une liaison d'état distincte de la liaison de basculement. Si vous ne spécifiez pas d'interface distincte, la liaison de basculement est utilisée pour la liaison d'état.

L'argument *if_name* attribue un nom à l'interface.

L'argument *interface_id* peut être une interface physique, une sous-interface ou un ID d'interface EtherChannel.

Étape 6 Si vous avez spécifié une liaison d'état distincte, attribuez les adresses IP actives et en veille à cette liaison d'état :

Cette adresse doit se trouver sur un sous-réseau inutilisé, différent de la liaison de basculement. Ce sous-réseau peut être de 31 bits (255.255.255.254) avec seulement deux adresses IP. 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne, et vous ne pouvez pas les utiliser pour les liaisons de basculement ou d'état.

L'adresse IP en veille doit se trouver dans le même sous-réseau que l'adresse IP active.

Ignorez cette étape si vous partagez la liaison d'état.

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

Exemple :

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

Ou :

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

Étape 7 Si vous avez spécifié une liaison d'état distincte, activez cette dernière :

interface *state_interface_id*

no shutdown

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

Ignorez cette étape si vous partagez la liaison d'état.

Étape 8 (Facultatif) Effectuez l'une des opérations suivantes pour chiffrer les communications sur les liaisons de basculement et d'état :

- (Privilégié) Établissez des tunnels IPsec LAN à LAN sur les liaisons de basculement et d'état entre les unités pour chiffrer toutes les communications de basculement :

  failover ipsec pre-shared-key [**0** | **8**] *key*

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  La *clé* peut comporter jusqu'à 128 caractères. Identifiez la même clé sur les deux unités. La clé est utilisée par IKEv2 pour établir les tunnels.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale), la clé est chiffrée dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que la clé est chiffrée à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  La clé partagée **failover ipsec pre-shared-key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

  Vous ne pouvez pas utiliser à la fois le chiffrement IPsec et le chiffrement **failover key** existant. Si vous configurez les deux méthodes, IPsec est utilisé. Cependant, si vous utilisez la phrase secrète principale, vous devez d'abord supprimer la clé de basculement à l'aide de la commande **no failover key** avant de configurer le chiffrement IPsec.

  Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN).

- (Facultatif) Chiffrez la communication de basculement sur les liaisons de basculement et d'état :

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  Utilisez un *shared_secret*, de 1 à 63 caractères, ou une **hex** *key* de 32 caractères.

  Pour le *shared_secret*, vous pouvez utiliser n'importe quelle combinaison de chiffres, de lettres ou de ponctuation. Le secret partagé ou la clé hexadécimale est utilisé pour générer la clé de chiffrement. Identifiez la même clé sur les deux unités.

  Si vous utilisez une phrase secrète principale (voir Configurer la phrase secrète principale), le secret partagé ou la clé hexadécimale est chiffré dans la configuration. Si vous copiez à partir de la configuration (par exemple, à partir de la sortie **more system:running-config**), spécifiez que le secret partagé ou la clé hexadécimale est chiffré à l'aide du mot clé **8**. **0** est utilisé par défaut, spécifiant un mot de passe non chiffré.

  Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée.

  Si vous ne configurez pas le chiffrement des liaisons de basculement et d'état, la communication de basculement, y compris tous les mots de passe ou clés de la configuration qui sont envoyés lors de la réplication des commandes, sera en texte clair.

Étape 9 Créez un groupe de basculement 1 :

failover group 1

primary

preempt [*delay*]

Exemple :

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

En règle générale, vous affectez le groupe 1 à l'unité principale et le groupe 2 à l'unité secondaire. Les deux groupes de basculement deviennent actifs sur l'unité qui démarre en premier (même s'il semble qu'ils démarrent simultanément, une unité devient active en premier), malgré le paramètre principal ou secondaire du groupe. La commande **preempt** active le groupe de basculement sur l'unité désignée automatiquement lorsque cette unité est disponible.

Vous pouvez saisir une valeur *delay* facultative, qui spécifie le nombre de secondes pendant lesquelles le groupe de basculement reste actif sur l'unité actuelle avant de devenir automatiquement actif sur l'unité désignée. Cette valeur peut être comprise entre 1 et 1 200.

Si le basculement dynamique est activé, la préemption est retardée jusqu'à ce que les connexions soient répliquées à partir de l'unité sur laquelle le groupe de basculement est actuellement actif.

Si vous basculez manuellement, la commande **preempt** est ignorée.

Étape 10 Créez le groupe de basculement 2 et affectez-le à l'unité secondaire :

failover group 2

secondary

preempt [*delay*]

Exemple :

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

Étape 11 Entrez en mode de configuration de contexte pour un contexte donné et affectez le contexte à un groupe de basculement :

context *nom*

join-failover-group {**1** | **2**}

Exemple :

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

Répétez cette commande pour chaque contexte.

Toutes les contextes non affectés sont automatiquement affectés au groupe de basculement 1. Le contexte d'administration est toujours membre du groupe de basculement 1; vous ne pouvez pas l'affecter au groupe 2.

Étape 12 Activez le basculement :

failover

Étape 13 Enregistrez la configuration système dans la mémoire flash :

write memory

Exemples

L'exemple suivant configure les paramètres de basculement pour l'unité principale :

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

Configurer l'unité secondaire pour le basculement actif/actif

La seule configuration requise sur l'unité secondaire concerne la liaison de basculement. L'unité secondaire exige que ces commandes communiquent initialement avec l'unité principale. Une fois que l'unité principale a envoyé sa configuration à l'unité secondaire, la seule différence permanente entre les deux configurations est la commande **basculement LAN unité**, qui identifie chaque unité comme principale ou secondaire.

Avant de commencer

- Activez ou désactivez le mode de contexte multiple conformément à Activer ou désactiver le mode de contexte multiple.
- Vous ne pourrez pas activer le basculement si des interfaces sont configurées pour DHCP.
- Ne configurez pas d'argument **nameif** pour les liaisons de basculement et d'état.
- Effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Saisissez à nouveau les mêmes commandes que sur l'unité principale, *à l'exception* de la commande **basculement LAN unité principale**. Vous pouvez éventuellement la remplacer par la commande **basculement LAN unité secondaire**, mais ce n'est pas nécessaire, car **le paramètre secondaire** est le paramètre par défaut. Vous n'avez pas non plus besoin de saisir les commandes **failover group** et **join-failover-group**, car elles sont répliquées à partir de l'unité principale. Consultez Configurer l'unité principale pour le basculement actif/actif, à la page 32.

Par exemple :

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

Étape 2 Après la synchronisation de la configuration de basculement à partir de l'unité principale, enregistrez la configuration dans la mémoire flash :

ciscoasa(config)# **write memory**

Étape 3 Si nécessaire, forcez le groupe de basculement 2 à être actif sur l'unité secondaire :

failover active group 2

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement à votre guise.

Configurer les critères de basculement et les autres paramètres

Consultez Paramètres par défaut pour le basculement, à la page 27 pour connaître les paramètres par défaut pour de nombreux paramètres que vous pouvez modifier dans cette section. Pour le mode actif/actif, vous définissez la plupart des critères par groupe de basculement.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte multiple.

- Pour la détection de transfert bidirectionnel (BFD) des fonctions de surveillance de l'intégrité des unités, consultez les limites suivantes :
  - Firepower 9300 et 4100 uniquement.
  - Actif/Veille uniquement.
  - Mode routé uniquement

Procédure

Étape 1 Modifiez les délais d'interrogation et de rétention de l'unité :

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

Exemple :

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

La plage **polltime** est comprise entre 1 et 15 secondes ou entre 200 et 999 millisecondes. La plage **holdtime** est comprise entre 1 et 45 secondes ou entre 800 et 999 millisecondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 3 fois le délai d'interrogation de l'unité. Grâce à un délai d'interrogration plus court, l'ASA peut détecter les défaillances et déclencher le basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des basculements inutiles lorsque le réseau est temporairement congestionné.

Si une unité n'entend pas le paquet Hello sur l'interface de communication de basculement pendant une période d'interrogation, des tests supplémentaires sont effectués par les interfaces restantes. S'il n'y a toujours aucune réponse de l'unité homologue pendant le délai de rétention, l'unité est considérée comme défaillante et, si l'unité défaillante est l'unité active, l'unité en veille prend le relais en tant qu'unité active.

En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 2 Configurez la BFD pour la surveillance de l'intégrité de l'unité.

La surveillance régulière de l'unité peut déclencher de fausses alarmes lorsque l'utilisation du CPU est élevée. La méthode BFD est distribuée, de sorte qu'un CPU élevé n'affecte pas son fonctionnement.

a) Définissez un modèle de BFD à utiliser pour la détection de l'état de basculement :

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

Exemple :

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

Le **min-tx** spécifie le débit auquel les paquets de contrôle de la BFD sont envoyés à l'homologue de basculement. La plage va de 50 à 999 millisecondes. Le **min-rx** spécifie le débit auquel les paquets de contrôle de la BFD doivent être reçus de l'homologue de basculement. La plage va de 50 à 999 millisecondes. Le **multiplier** spécifie le nombre de paquets de contrôle BFD consécutifs qui doivent

être manqués par un homologue de basculement avant que la BFD ne déclare que l'homologue n'est pas disponible. La valeur doit être comprise entre 3 et 50.

Vous pouvez également configurer l'écho et l'authentification pour ce modèle; voir Créer le modèle BFD.

b) Activez la BFD pour la surveillance de l'intégrité :

failover health-check bfd *template_name*

Exemple :

```
ciscoasa(config)# failover health-check bfd failover-temp
```

Étape 3 Modifiez le délai d'interrogation sur l'état de la liaison d'interface :

failover polltime link-state msec *poll_time*

Exemple :

```
ciscoasa(config)# failover polltime link-state msec 300
```

La plage est comprise entre 300 et 799 millisecondes. Par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez personnaliser le délai d'interrogation. Par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement.

En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 4 Définissez le taux de réplication de session en connexions par seconde :

failover replication rate *conns*

Exemple :

```
ciscoasa(config)# failover replication rate 20000
```

Le débit minimum et maximum est déterminé par votre modèle. La valeur par défaut est le taux maximum. En mode actif/actif, vous définissez ce débit pour le système; vous ne pouvez pas définir ce débit par groupe de basculement.

Étape 5 Désactivez la possibilité d'apporter des modifications à la configuration directement sur l'unité ou le contexte en veille :

failover standby config-lock

Par défaut, les configurations sur l'unité/le contexte de veille sont autorisées avec un message d'avertissement.

Étape 6 (Mode actif/actif uniquement) Spécifiez le groupe de basculement que vous souhaitez personnaliser :

failover group {**1** | **2**}

Exemple :

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

Étape 7 Activez la réplication de l'état HTTP :

- Pour le mode actif/veille :

  failover replication http

- Pour le mode actif/actif :

  replication http

Pour permettre l'inclusion des connexions HTTP dans la réplication des renseignements d'état, il est nécessaire d'activer la réplication HTTP. Nous vous conseillons d'activer la réplication de l'état HTTP.

Remarque
En raison d'un retard lors de la suppression des flux HTTP de l'unité de secours lors de l'utilisation du basculement, la sortie **show conn count** pourrait afficher des numéros différents sur l'unité active par rapport à l'unité de secours; si vous attendez plusieurs secondes et réexécutez la commande, vous verrez le même nombre sur les deux unités.

Étape 8 Définissez le seuil de basculement lorsque les interfaces tombent en panne :

- Pour le mode actif/veille :

  failover interface-policy *num* [%]

  Exemple :

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- Pour le mode actif/actif :

  interface-policy *num* [%]

  Exemple :

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

Par défaut, la défaillance d'une interface entraîne le basculement.

Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 1 025.

Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.

Étape 9 Modifiez les délais d'interrogation et de rétention de l'interface :

- Pour le mode actif/veille :

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  Exemple :

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- Pour le mode actif/actif :

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  Exemple :

```
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
```

- *polltime* : définit la durée d'attente entre l'envoi d'un paquet Hello à l'homologue. Les valeurs valides pour le délai d'interrogation vont de 1 à 15 secondes ou, si le mot clé facultatif **msec** est utilisé, de 500 à 999 millisecondes. La valeur par défaut est de 5 secondes.
- **holdtime***time* : définit le temps (sous forme de calcul) entre le dernier message Hello reçu de l'unité homologue et le début des tests d'interface pour déterminer l'intégrité de l'interface. Il définit également la durée de chaque test d'interface comme délai d'attente/16. Les valeurs valides sont comprises entre 5 et 75 secondes. La valeur par défaut est de 5 fois le délai d'interrogation. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à cinq fois le délai d'interrogation.

  Pour calculer le temps avant le début des tests d'interface (y) :

  1. x = (*durée d'attente*/*durée d'interrogation*)/2, arrondi à l'entier le plus proche. (0,4 et moins sont arrondis à l'unité inférieure; 0,5 et plus sont arrondis à l'unité supérieure).
  2. y = x**durée d'interrogation*

  Par exemple, si vous utilisez la délai d'attente par défaut de 25 et le délai d'interrogation de 5, alors y = 15 secondes.

Étape 10 Configurez l'adresse MAC virtuelle d'une interface :

- Pour le mode actif/veille :

  failover mac address *phy_if active_mac standby_mac*

  Exemple :

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- Pour le mode actif/actif :

  mac address *phy_if active_mac standby_mac*

  Exemple :

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

L'argument *phy_if* est le nom physique de l'interface, tel que gigabitethernet0/1.

Les arguments *active_mac* et *standby_mac* sont des adresses MAC au format H.H.H, où H est un chiffre hexadécimal de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE.

L'adresse *active_mac* est associée à l'adresse IP active de l'interface, et l'adresse *standby_mac* est associée à l'adresse IP en veille pour l'interface.

Vous pouvez également définir l'adresse MAC à l'aide d'autres commandes ou méthodes, mais nous vous conseillons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible.

Utilisez la commande **show interface** pour afficher l'adresse MAC utilisée par une interface.

Étape 11 (Mode actif/actif uniquement) Répétez cette procédure pour l'autre groupe de basculement.

Configurer la supervision de l'interface

Par défaut, la supervision est activée sur toutes les interfaces physiques, ou pour le Firepower 1010, toutes les interfaces VLAN.Les ports de commutation Firepower 1010 ne sont pas admissibles à la surveillance d'interface.

Vous pourriez souhaiter empêcher les interfaces connectées à des réseaux moins critiques d'affecter votre politique de basculement.

Vous pouvez superviser jusqu'à 1 025 interfaces sur une unité (dans tous les contextes en mode de contexte multiple).

Avant de commencer

En mode de contexte multiple, configurez les interfaces dans chaque contexte.

Procédure

Activez ou désactivez la surveillance de l'intégrité pour une interface :

[**no**] **monitor-interface** {*if_name*}

Exemple :

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

Configurer la prise en charge des paquets routés asymétriques (mode actif/actif)

Lorsqu'elle fonctionne en mode de basculement actif/actif, une unité peut recevoir un paquet de retour pour une connexion provenant de son unité homologue. Comme l'ASA qui reçoit le paquet n'a aucune information de connexion pour le paquet, le paquet est abandonné. Cet abandon se produit le plus généralement lorsque les deux ASA d'une paire de basculement actif/actif sont connectés à des fournisseurs de services différents et que la connexion sortante n'utilise pas d'adresse NAT.

Vous pouvez empêcher l'abandon des paquets de retour en autorisant les paquets routés de manière asymétrique. Pour ce faire, vous attribuez les interfaces similaires sur chaque ASA au même groupe ASR. Par exemple, les deux ASA se connectent au réseau interne sur l'interface interne, mais se connectent à des fournisseurs de services Internet distincts sur l'interface externe. Sur l'unité principale, affectez le contexte actif externe à l'interface au groupe ASR 1; sur l'unité secondaire, affectez le contexte actif en dehors de l'interface au même groupe ASR 1. Lorsque l'unité principale externe reçoit un paquet pour lequel elle n'a aucune information de session, elle vérifie les renseignements de session pour les autres interfaces dans les contextes de veille

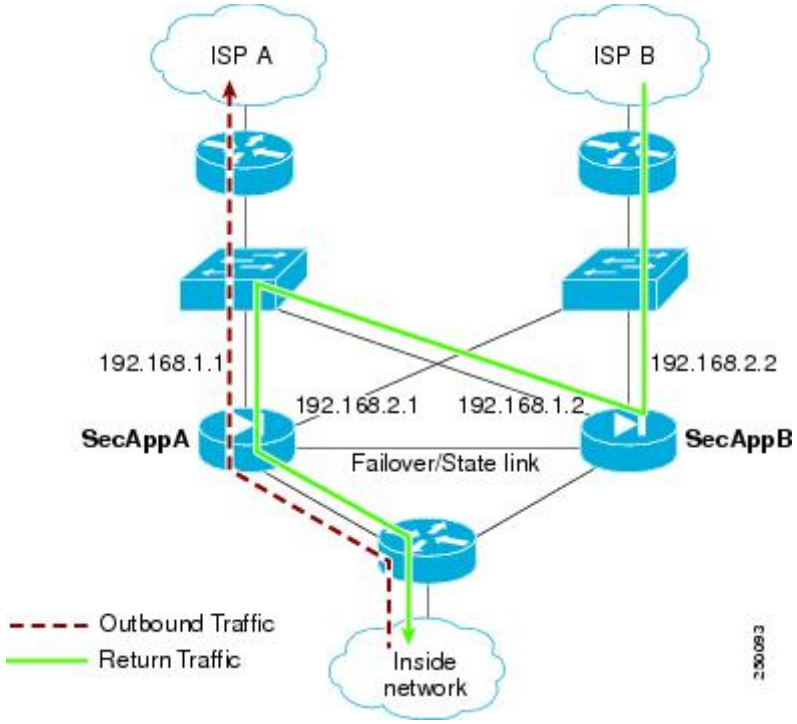
qui sont dans le même groupe; dans ce cas, le groupe ASR 1. Si elle ne trouve aucune correspondance, le paquet est abandonné. Si elle trouve une correspondance, l'une des actions suivantes se produit :

- Si le trafic entrant provient d'une unité homologue, tout ou partie de l'en-tête de couche 2 est réécrit et le paquet est redirigé vers l'autre unité. Cette redirection se poursuit tant que la session est active.
- Si le trafic entrant provient d'une interface différente sur la même unité, une partie ou la totalité de l'en-tête de couche 2 est réécrit et le paquet est réinjecté dans le flux.

Remarque Cette fonctionnalité ne fournit pas de routage asymétrique; elle restaure les paquets routés de manière asymétrique vers la bonne interface.

La figure suivante montre un exemple de paquet routé de manière asymétrique.

Illustration 6 : Exemple ASR



1. Une session sortante passe par l'ASA avec le contexte SecAppA actif. Elle quitte l'interface en dehors du FAI-A (192.168.1.1).
2. En raison d'un routage asymétrique configuré quelque part en amont, le trafic de retour passe par l'interface externe du FAI-B (192.168.2.2) sur l'ASA avec le contexte SecAppB actif.
3. Normalement, le trafic de retour serait abandonné, car il n'y a aucune information de session pour le trafic sur l'interface 192.168.2.2. Cependant, l'interface est configurée dans le cadre du groupe ASR 1. L'unité recherche la session sur toute autre interface configurée avec le même ID de groupe ASR.
4. Les renseignements de session se trouvent sur l'interface externe du FAI-A (192.168.1.2), qui est en état de veille sur l'unité avec SecAppB. Le basculement dynamique a répliqué les renseignements de session de SecAppA à SecAppB.

5. Au lieu d'être abandonné, l'en-tête de couche 2 est réécrit avec les renseignements pour l'interface 192.168.1.1 et le trafic est redirigé hors de l'interface 192.168.1.2, où il peut ensuite revenir par l'interface de l'unité à partir de laquelle il provient (192.168.1.1. sur SecAppA). Ce transfert se poursuit au besoin jusqu'à la fin de la session.

Avant de commencer

- Basculement dynamique : transmet les renseignements relatifs à l'état de session sur les interfaces du groupe de basculement actif au groupe de basculement de secours.
- HTTP de réplication : les renseignements relatifs à l'état de session HTTP ne sont pas transmis au groupe de basculement de secours et ne sont donc pas présents sur l'interface de secours. Pour que l'ASA puisse réacheminer les paquets HTTP routés de manière asymétrique, vous devez répliquer les renseignements relatifs à l'état HTTP.
- Effectuez cette procédure dans chaque contexte actif sur les unités principale et secondaire.
- Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR.

Procédure

Étape 1 Sur l'unité principale, spécifiez l'interface pour laquelle vous souhaitez autoriser les paquets routés de manière asymétrique :

interface *phy_if*

Exemple :

```
primary/admin(config)# interface gigabitethernet 0/0
```

Étape 2 Définissez le numéro de groupe ASR de l'interface :

asr-group *num*

Exemple :

```
primary/admin(config-ifc)# asr-group 1
```

Les valeurs valides pour *num* vont de 1 à 32.

Étape 3 Sur l'unité secondaire, spécifiez l'interface similaire pour laquelle vous souhaitez autoriser les paquets routés de manière asymétrique :

interface *phy_if*

Exemple :

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

Étape 4 Définissez le numéro de groupe ASR de l'interface pour qu'il corresponde à l'interface de l'unité principale :

asr-group *num*

Exemple :

```
secondary/ctx1(config-ifc)# asr-group 1
```

Exemples

Les deux unités ont la configuration suivante (les configurations affichent seulement les commandes pertinentes). Le périphérique étiqueté SecAppA dans le diagramme est l'unité principale de la paire de basculement.

Configuration système de l'unité principale

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

Configuration du contexte SecAppA

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
```

```
monitor-interface outside
```

Configuration du contexte SecAppB

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

Gérer Failover (basculement)

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

Forcer le basculement

Pour forcer l'unité en veille à devenir active, procédez comme suit.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *en veille*. L'unité en veille devient l'unité active.

Si vous spécifiez le **groupe** *group_id*, cette commande force un basculement lorsqu'elle est saisie sur l'unité *en veille* pour le groupe de basculement actif/actif spécifié. L'unité en veille devient l'unité active du groupe de basculement.

- Pour le mode actif/veille sur l'unité en veille :

  failover active

- Pour le mode actif/actif sur l'unité en veille :

  failover active [**group** *group_id*]

  Exemple :

  ```
  standby# failover active group 1
  ```

Étape 2 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *active*. L'unité active devient l'unité en veille.

Si vous spécifiez le **groupe** *group_id*, cette commande force un basculement lorsqu'elle est saisie sur l'unité *active* pour le groupe de basculement spécifié. L'unité active devient l'unité en veille du groupe de basculement.

- Pour le mode actif/veille sur l'unité active :

  no failover active

- Pour le mode actif/actif sur l'unité active :

  no failover active [**group** *group_id*]

  Exemple :

```
active# no failover active group 1
```

Désactiver le basculement

La désactivation du basculement sur une ou les deux unités permet de maintenir l'état actif et de veille de chaque unité jusqu'à ce que vous rechargiez. Pour une paire de basculement actif/actif, les groupes de basculement restent à l'état actif sur l'unité où ils sont actifs, quelle que soit l'unité pour laquelle ils sont configurés en priorité.

Affichez les caractéristiques suivantes lorsque vous désactivez le basculement :

- L'unité ou le contexte en veille reste en mode veille pour que les deux unités ne commencent pas à transmettre du trafic (cela s'appelle un état de pseudo-veille).
- L'unité ou le contexte en veille continue d'utiliser ses adresses IP en veille même s'il n'est plus connecté à une unité ou un contexte actif.
- L'unité ou le contexte en veille continue d'écouter une connexion sur la liaison de basculement. Si le basculement est réactivé sur l'unité ou le contexte actif, l'unité ou le contexte en veille reprend son état de veille ordinaire après avoir resynchronisé le reste de sa configuration.
- N'activez pas le basculement manuellement sur l'unité en veille; consultez plutôt Forcer le basculement, à la page 47. Si vous activez le basculement sur l'unité en veille, vous verrez un conflit d'adresses MAC qui peut perturber le trafic IPv6.
- Pour vraiment désactiver le basculement, enregistrez la configuration sans basculement dans la configuration de démarrage, puis rechargez.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Désactivez le basculement :

no failover

Étape 2 Pour désactiver complètement le basculement, enregistrez la configuration et rechargez :

write memory

reload

Restaurer une unité défaillante

Pour restaurer une unité défaillante à un état sans échec, effectuez la procédure suivante.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système.

Procédure

Étape 1 Restaurez une unité défaillante à un état sans échec :

- Pour le mode actif/veille :

  failover reset

- Pour le mode actif/actif :

  failover reset [**group** *group_id*]

  Exemple :

```
ciscoasa(config)# failover reset group 1
```

La restauration d'une unité défaillante à un état sans échec ne la rend pas automatiquement active; les unités restaurées restent en état de veille jusqu'à ce qu'elles soient activées par le basculement (forcé ou naturel). Une exception est un groupe de basculement (mode actif/actif uniquement) configuré avec une préemption de basculement. S'il était précédemment actif, un groupe de basculement devient actif s'il est configuré avec la préemption et si l'unité sur laquelle il a échoué est l'unité préférée.

Si vous spécifiez le **groupe** *group_id*, cette commande restaure un groupe de basculement actif/actif défaillant à un état sans échec.

Étape 2 (Mode actif/actif uniquement) Pour réinitialiser le basculement au niveau du groupe de basculement :

a) Dans le système, choisissez **Monitoring (Supervision) > Failover (Basculement) > Failover Group (Groupe de basculement)#**, où # correspond au numéro du groupe de basculement que vous souhaitez contrôler.
b) Cliquez sur **Reset Basculement** (Réinitialiser le basculement).

Resynchroniser la configuration

Si vous saisissez la commande write standby sur l'unité active, l'unité en veille efface sa configuration en cours d'exécution (à l'exception des commandes de basculement utilisées pour communiquer avec l'unité active) et l'unité active envoie sa configuration complète à l'unité en veille.

Pour le mode de contexte multiple, lorsque vous saisissez la commande **write standby** dans l'espace d'exécution du système, tous les contextes sont répliqués. Si vous saisissez la commande **write standby** dans un contexte, la commande ne réplique que la configuration du contexte.

Les commandes répliquées sont stockées dans la configuration en cours d'exécution.

Tester la fonctionnalité de basculement

Pour tester la fonctionnalité de basculement, effectuez la procédure suivante.

Procédure

Étape 1 Vérifiez que votre unité active transmet le trafic comme prévu à l'aide du protocole FTP (par exemple) pour envoyer un fichier entre des hôtes sur différentes interfaces.

Étape 2 Forcez un basculement en saisissez la commande suivante sur l'unité active :

Mode actif/veille

ciscoasa(config)# **no failover active**

Mode actif/actif

ciscoasa(config)# **no failover active group** *group_id*

Étape 3 Utilisez FTP pour envoyer un autre fichier entre les deux mêmes hôtes.

Étape 4 Si le test a échoué, saisissez la commande **show failover** pour vérifier l'état du basculement.

Étape 5 Lorsque vous avez terminé, vous pouvez rétablir l'état actif de l'unité en saisissant la commande suivante sur l'unité nouvellement active :

Mode actif/veille

ciscoasa(config)# **no failover active**

Mode actif/actif

ciscoasa(config)# **failover active group** *group_id*

Remarque
Lorsqu'une interface ASA tombe en panne, le basculement est toujours considéré comme un problème d'unité. Si l'ASA détecte qu'une interface est en panne, le basculement se produit immédiatement, sans attendre le délai de rétention de l'interface. Le délai de rétention de l'interface n'est utile que lorsque l'ASA considère que son état est OK, bien qu'il ne reçoive pas de paquets Hello de l'homologue. Pour simuler le délai de rétention de l'interface, fermez le réseau VLAN sur le commutateur pour empêcher les homologues de recevoir des paquets Hello les uns des autres.

Exécution de la commande à distance

L'exécution de commandes à distance vous permet d'envoyer des commandes saisies dans la ligne de commande à un homologue de basculement donné.

Envoyer une commande

Étant donné que les commandes de configuration sont répliquées de l'unité ou du contexte actif vers l'unité ou le contexte en veille, vous pouvez utiliser la commande **failover exec** pour saisir des commandes de configuration sur l'unité appropriée, quelle que soit l'unité à laquelle vous êtes connecté. Par exemple, si vous êtes connecté à l'unité en veille, vous pouvez utiliser la commande **failover exec active** pour envoyer les modifications de configuration à l'unité active. Ces modifications sont ensuite répliquées sur l'unité en veille. N'utilisez pas la commande **failover exec** pour envoyer des commandes de configuration à l'unité ou au contexte en veille; ces modifications de configuration ne sont pas répliquées sur l'unité active et les deux configurations ne seront plus synchronisées.

La sortie des commandes de configuration, d'exécution et **show** est affichée dans la session de terminal actuelle. Vous pouvez donc utiliser la commande **failover exec** pour émettre des commandes **show** sur une unité homologue et afficher les résultats dans le terminal actuel.

Vous devez disposer des privilèges suffisants pour exécuter une commande sur l'unité locale afin d'exécuter la commande sur l'unité homologue.

Procédure

Étape 1 Si vous êtes en mode de contexte multiple, utilisez la commande **changeto context***name* pour passer au contexte que vous souhaitez configurer. Vous ne pouvez pas modifier les contextes sur l'homologue de basculement avec la commande **failover exec**.

Étape 2 Utilisez la commande suivante pour envoyer des commandes à l'unité de basculement spécifiée :

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

Utilisez le mot clé **active** ou **standby** pour que la commande soit exécutée sur l'unité spécifiée, même s'il s'agit de l'unité actuelle. Utilisez le mot clé **mate** pour que la commande soit exécutée sur l'homologue de basculement.

Les commandes qui provoquent un changement de mode de commande ne modifient pas l'invite de la session en cours. Vous devez utiliser la commande **show failover exec** pour afficher le mode de commande dans lequel la commande est exécutée. Consultez la section Modifier les modes de commande, page 7-53 pour en savoir plus.

Modifier les modes de commande

La commande **failover exec** conserve un état de mode de commande distinct du mode de commande de votre session de terminal. Par défaut, le mode de commande **failover exec** démarre en mode de configuration globale pour le périphérique indiqué. Vous pouvez modifier ce mode de commande en envoyant la commande appropriée (comme la commande **interface**) à l'aide de la commande **failover exec**. L'invite de session ne change pas lorsque vous changez de mode à l'aide de **failover exec**.

Par exemple, si vous êtes connecté au mode de configuration globale de l'unité active d'une paire de basculement et que vous utilisez la commande **failover exec active** pour passer en mode de configuration d'interface, l'invite du terminal reste en mode de configuration globale, mais les commandes saisies à l'aide de **failover exec** sont saisies en mode de configuration d'interface.

Les exemples suivants montrent la différence entre le mode de session de terminal et le mode de commande **failover exec**. Dans l'exemple, l'administrateur change le mode **failover exec** sur l'unité active au mode de configuration d'interface pour l'interface GigabitEthernet0/1. Après cela, toutes les commandes saisies à l'aide de **failover exec active** sont envoyées au mode de configuration d'interface pour l'interface GigabitEthernet0/1. L'administrateur utilise ensuite l'exécution du basculement pour attribuer une adresse IP à cette interface. Bien que l'invite indique le mode de configuration globale, le mode **failover exec active** est en mode de configuration d'interface.

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

La modification des modes de commande pour votre session actuelle avec le périphérique n'affecte pas le mode de commande utilisé par la commande **failover exec**. Par exemple, si vous êtes en mode de configuration d'interface sur l'unité active et que vous n'avez pas modifié le mode de commande **failover exec**, la commande suivante sera exécutée en mode de configuration globale. Il en résulte que votre session avec le périphérique reste en mode de configuration d'interface, tandis que les commandes saisies à l'aide de **failover exec active** sont envoyées en mode de configuration de routeur pour le processus de routage indiqué.

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

Utilisez la commande **show failover exec** pour afficher le mode de commande sur le périphérique indiqué dans lequel les commandes envoyées avec la commande **failover exec** sont exécutées. La commande **show failover exec** prend les mêmes mots clés que la commande **failover exec** : **active**, **mate** ou **standby**. Le mode **failover exec** pour chaque périphérique est suivi séparément.

Par exemple, voici une sortie de la commande **show failover exec** saisie sur l'unité de secours :

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

Questions de sécurité

La commande **failover exec** utilise la liaison de basculement pour envoyer des commandes à l'unité homologue et recevoir la sortie de l'exécution de la commande. Vous devez activer le chiffrement sur la liaison de basculement pour éviter les attaques clandestines ou d'intermittence.

Limites de l'exécution de la commande à distance

Lorsque vous utilisez des commandes à distance, vous êtes soumis aux limites suivantes :

- Si vous mettez à niveau une unité en utilisant la procédure de mise à niveau sans temps d'arrêt et pas l'autre, les deux unités doivent exécuter un logiciel qui prend en charge la commande **failover exec**.
- L'aide à l'exécution des commandes et au contexte n'est pas disponible pour les commandes dans l'argument *cmd_string*.
- En mode de contexte multiple, vous pouvez seulement envoyer des commandes au contexte homologue sur l'unité homologue. Pour envoyer des commandes à un contexte différent, vous devez d'abord passer à ce contexte sur l'unité à laquelle vous êtes connecté.
- Vous ne pouvez pas utiliser les commandes suivantes avec la commande **failover exec** :
  - **changeto**
  - **debug** (**undebug**)
- Si l'unité en veille est en état d'échec, elle peut toujours recevoir des commandes de la commande **failover exec** si la défaillance est causée par une défaillance de la carte de service; dans le cas contraire, l'exécution de la commande à distance échouera.
- Vous ne pouvez pas utiliser la commande **failover exec** pour passer du mode d'exécution privilégié au mode de configuration globale sur l'homologue de basculement. Par exemple, si l'unité actuelle est en mode d'exécution privilégié et que vous saisissez **failover exec mate configure terminal**, la sortie **show failover exec mate** affichera que la session d'exécution de basculement est en mode de configuration globale. Cependant, la saisie des commandes de configuration pour l'unité homologue à l'aide de **failover exec** échouera jusqu'à ce que vous passiez en mode de configuration globale sur l'unité actuelle.
- Vous ne pouvez pas saisir des commandes d'exécution de basculement récursives, telles que la commande **failover exec mate failover exec mate**.
- Les commandes qui nécessitent une entrée ou une confirmation de l'utilisateur doivent utiliser l'option **noconfirm**. Par exemple, pour recharger le partenaire, saisissez :

  failover exec mate reload noconfirm

Surveillance de Failover (basculement)

Cette section vous permet de surveiller l'état de Failover (basculement).

Messages de basculement

Lorsqu'un basculement se produit, les deux ASA envoient des messages système.

Messages de journal système de basculement

L'ASA émet un certain nombre de messages de journal système liés au basculement au niveau de priorité 2, ce qui indique une condition critique. Pour afficher ces messages, consultez le guide des messages du journal système. 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.

Remarque Pendant le basculement, l'ASA s'éteint de manière logique, puis affiche des interfaces, générant les messages de journal système 411001 et 411002. Il s'agit d'une activité normale.

Messages de débogage de basculement

Pour afficher les messages de débogage, saisissez la commande **debug fover**. Consultez la référence de commande pour en savoir plus.

Remarque Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du CPU, elle peut affecter considérablement les performances du système. Par conséquent, les commandes **debug fover** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de sessions de dépannage effectuées avec le TAC de Cisco.

Interruptions de basculement SNMP

Pour recevoir des alertes SNMP de journal système pour le basculement, configurez l'agent SNMP pour envoyer des alertes SNMP aux stations de gestion SNMP, définissez un hôte de journal système et compilez la MIB de journal système Cisco dans votre station de gestion SNMP.

Supervision de l'état du basculement

Pour superviser l'état du basculement, saisissez l'une des commandes suivantes :

- **afficher le basculement**

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

- **show failover group**

  Affiche des renseignements sur l'état de basculement du groupe de basculement. Les renseignements affichés sont similaires à ceux de la commande **show failover**, mais limités au groupe spécifié.

- **show monitor-interface**

  Affiche des renseignements sur l'interface supervisée.

- **show running-config failover**

  Affiche les commandes de basculement dans la configuration en cours d'exécutionn.

Historique de basculement

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de secours	7.0(1)	Cette fonctionnalité a été introduite.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/actif	7.0(1)	Cette fonctionnalité a été introduite.
Prise en charge d'une valeur hexadécimale pour la clé de basculement	7.0(4)	Vous pouvez maintenant spécifier une valeur hexadécimale pour le chiffrement de la liaison de basculement. Nous avons modifié la commande suivante : **failover key hex**.
Prise en charge de la phrase secrète principale pour la clé de basculement	8.3(1)	La clé de basculement prend désormais en charge la phrase secrète principale, qui chiffre la clé partagée dans la configuration de démarrage. Si vous copiez le secret partagé d'un ASA à un autre, par exemple à partir de la commande **more system:running-config**, vous pouvez copier et coller la clé partagée chiffrée avec succès. **Remarque** Le secret partagé **failover key** s'affiche comme ***** dans la sortie **show running-config**; cette clé masquée ne peut pas être copiée. Nous avons modifié la commande suivante : **failover key** [**0** | **8**].
Ajout de la prise en charge d'IPv6 pour le basculement.	8.2(2)	Nous avons modifié les commandes suivantes : **failover interface ip**, **show failover**, **ipv6 address**, **show monitor-interface**.
Modifiez la préférence de l'unité de groupe de basculement lors du démarrage « simultané ».	9.0(1)	Les versions logicielles antérieures permettaient un démarrage « simultané » de sorte que les groupes de basculement ne devaient pas exiger que la commande **preempt** devienne active sur l'unité préférée. Cependant, cette fonctionnalité a maintenant été modifiée, de sorte que les deux groupes de basculement deviennent actifs sur la première unité de démarrage.
Prise en charge des tunnels IPsec LAN à LAN pour chiffrer les communications de liaison de basculement et d'état	9.1(2)	Au lieu d'utiliser le chiffrement propriétaire pour la clé de basculement (la commande **failover key**), vous pouvez désormais utiliser un tunnel IPsec LAN à LAN pour le chiffrement de la liaison de basculement et d'état. **Remarque** Les tunnels de basculement LAN à LAN ne sont pas pris en compte dans la licence IPsec (autre VPN). Nous avons introduit ou modifié les commandes suivantes : **failover ipsec pre-shared-key**, **show vpn-sessiondb**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Désactiver la surveillance de l'intégrité d'un module matériel	9.3(1)	Par défaut, l'ASA surveille l'intégrité d'un module matériel installé tel que le module ASA FirePOWER. Si vous ne souhaitez pas qu'une défaillance du module matériel déclenche le basculement, vous pouvez désactiver la surveillance du module. Nous avons modifié la commande suivante : **monitor-interface service-module**
Verrouiller les modifications de configuration sur l'unité de veille ou le contexte de veille dans une paire de basculement	9.3(2)	Vous pouvez désormais verrouiller les modifications de configuration sur l'unité de veille (basculement actif/veille) ou sur le contexte de veille (basculement actif/actif) afin de ne pas pouvoir apporter des modifications sur l'unité de veille en dehors de la synchronisation normale de la configuration. Nous avons introduit la commande suivante : **failover standby config-lock**
Activer l'utilisation de l'interface de gestion Management 1/1 comme liaison de basculement sur l'ASA 5506H	9.5(1)	Sur l'ASA 5506H uniquement, vous pouvez maintenant configurer l'interface de gestion Management 1/1 comme liaison de basculement. Cette fonctionnalité vous permet d'utiliser toutes les autres interfaces du périphérique comme interfaces de données. Notez que si vous utilisez cette fonctionnalité, vous ne pouvez pas utiliser le module ASA Firepower, ce qui nécessite que l'interface de gestion Management 1/1 reste une interface de gestion normale. Nous avons modifié les commandes suivantes : **failover lan interface, failover link**
Les améliorations de la NAT de classe opérateur sont désormais prises en charge dans le basculement et la mise en grappe d'ASA	9.5(2)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Cette fonctionnalité est désormais prise en charge dans les déploiements de basculement et de grappe ASA. Nous avons modifié la commande suivante : **show local-host**
Temps de synchronisation amélioré pour les ACL dynamiques de Secure Client (services client sécurisés) lors de l'utilisation du basculement actif/veille	9.6(2)	Lorsque vous utilisez Secure Client (services client sécurisés) sur une paire de basculement, le temps de synchronisation des ACL dynamiques (dACLs) associées avec l'unité de veille est maintenant amélioré. Auparavant, avec de grandes dACLs, le temps de synchronisation pouvait prendre des heures pendant lesquelles l'unité de veille était occupée à synchroniser au lieu de fournir une sauvegarde à haute disponibilité. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement avec état pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple	9.6(2)	Le basculement avec état est maintenant pris en charge pour les connexions Secure Client (services client sécurisés) dans le mode de contexte multiple. Nous n'avons pas modifié de commandes.
L'interrogation de la surveillance de l'état de la liaison de l'interface pour le basculement est désormais configurable pour une détection plus rapide	9.7(1)	Par défaut, chaque ASA d'une paire de basculement vérifie l'état de liaison de ses interfaces toutes les 500 ms. Vous pouvez maintenant configurer l'intervalle entre interrogations, entre 300 ms et 799 ms; par exemple, si vous définissez le délai d'interrogation à 300 ms, l'ASA peut détecter une défaillance d'interface et déclencher le basculement plus rapidement. Nous avons introduit la commande suivante : **failover polltime link-state**
Prise en charge de la détection de transfert bidirectionnel (BFD) pour la surveillance de l'intégrité du basculement actif/veille sur les périphériques Firepower 9300 et 4100.	9.7(1)	Vous pouvez activer la détection de transfert bidirectionnel (BFD) pour la vérification de l'intégrité du basculement entre deux unités d'une paire active/veille sur les périphériques Firepower 9300 et 4100. L'utilisation de la BFD pour la vérification de l'intégrité est plus fiable que la méthode de vérification de l'intégrité par défaut et utilise moins de CPU. Nous avons introduit la commande suivante : **failover health-check bfd**
Désactiver le délai de basculement	9.15(1)	Lorsque vous utilisez des groupes de ponts ou DAD IPv6, lorsqu'un basculement se produit, la nouvelle unité active attend jusqu'à 3 000 ms que l'unité de veille termine les tâches de mise en réseau et passe à l'état de veille. Ensuite, l'unité active peut commencer à transmettre du trafic. Pour éviter ce délai, vous pouvez désactiver le délai d'attente afin que l'unité active commence à transmettre le trafic avant l'unité de veille. Commandes nouvelles ou modifiées : **failover wait-disable**
Fonction d'optimisation Config-Sync pour un appairage haute disponibilité	9.18(1)	La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en cours de jonction correspond, l'unité à joindre ignore la configuration de synchronisation complète et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

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.