

ASA/PIX : Configuration du basculement actif/actif en mode transparent

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Produits connexes](#)

[Conventions](#)

[Basculement actif/actif](#)

[Basculement actif/actif - Aperçu](#)

[État principal/secondaire et état actif/veille](#)

[Synchronisation d'initialisation et de configuration de périphérique](#)

[Réplication des commandes](#)

[Déclencheurs de basculement](#)

[Opérations de basculement](#)

[Basculement périodique et dynamique](#)

[Basculement périodique](#)

[Basculement dynamique](#)

[Limites de configuration de basculement](#)

[Fonctions non prises en charge](#)

[Configuration du basculement actif/actif avec LAN](#)

[Diagramme du réseau](#)

[Configuration de l'unité principale](#)

[Configuration de l'unité secondaire](#)

[Configurations](#)

[Vérification](#)

[Utilisation de la commande show failover](#)

[Affichage des interfaces surveillées](#)

[Affichage des commandes de basculement dans la configuration en cours](#)

[Tests sur la fonctionnalité de basculement](#)

[Basculement forcé](#)

[Basculement désactivé](#)

[Restauration d'une unité défaillante](#)

[Dépannage](#)

[Messages système de basculement](#)

[L'unité principale a perdu les communications de basculement avec l'autre unité dans l'interface nom_interface](#)

[Messages de débogage](#)

[SNMP](#)

[Délai d'interrogation du basculement](#)

[AVERTISSEMENT : Échec du déchiffrement du message de basculement](#)

[Informations connexes](#)

[Introduction](#)

La configuration de basculement requiert deux appliances de sécurité identiques connectées entre elles par un lien de basculement dédié et éventuellement un lien de basculement dynamique. La santé des interfaces et des unités actives est surveillée pour déterminer si les conditions spécifiques de basculement sont remplies. Si ces conditions sont remplies, le basculement se produit.

Le dispositif de sécurité supporte deux configurations de basculement :

- [Basculement actif/actif](#)
- [Basculement actif/veille](#)

Chaque configuration de basculement a sa propre méthode pour déterminer et exécuter le basculement. Avec le basculement actif/actif, les deux unités peuvent acheminer le trafic réseau. Cela vous permet de configurer l'équilibrage de charge sur votre réseau. Le basculement actif/actif est seulement disponible sur les unités qui fonctionnent en mode de contexte multiple. Avec le basculement actif/veille, seule une unité achemine le trafic tandis que l'autre unité attend en état de veille. Le basculement actif/veille est disponible sur les unités qui fonctionnent en mode de contexte unique ou multiple. Ces deux configurations de basculement supportent le basculement dynamique et le basculement statique (périodique).

Un pare-feu transparent est un pare-feu de couche 2 qui agit comme un *bossoir dans le câble*, ou un *pare-feu furtif*, et n'est pas vu comme un saut de routeur vers les périphériques connectés. L'appliance de sécurité connecte le même réseau sur ses ports intérieurs et extérieurs. Puisque le pare-feu n'est pas un saut de routeur, vous pouvez facilement introduire un pare-feu transparent dans le réseau existant ; il est inutile de réadresser IP. Vous pouvez configurer l'appliance de sécurité adaptable pour être exécutée dans le mode de pare-feu routé par défaut ou le mode pare-feu transparent . Quand vous changez les modes, l'appliance de sécurité adaptable efface la configuration parce que de nombreuses commandes ne sont pas prises en charge dans les deux modes. Si vous avez déjà une configuration chargée, assurez-vous de sauvegarder cette configuration avant de changer de mode ; vous pouvez utiliser cette configuration de secours pour référence quand vous créez une nouvelle configuration. Référez-vous à [Exemple de configuration de pare-feu transparent](#) pour plus d'informations sur la configuration de l'appliance de pare-feu en mode transparent.

Ce document se concentre sur la façon de configurer un basculement actif/actif en mode transparent sur le dispositif de sécurité ASA.

Remarque : le basculement VPN n'est pas pris en charge sur les unités qui s'exécutent en mode **contextuel multiple**. Le basculement VPN est disponible pour les configurations **de basculement actif/veille** uniquement.

Cisco recommande de ne pas utiliser l'interface de gestion pour le basculement, notamment pour le basculement dynamique, où le dispositif de sécurité envoie constamment les informations de connexion d'un dispositif de sécurité à l'autre. L'interface utilisée pour le basculement doit être au moins de la même capacité que les interfaces qui acheminent le trafic habituel, et bien que les

interfaces de l'ASA 5540 soient Gigabit, l'interface de gestion est FastEthernet seulement. L'interface de gestion est conçue pour le trafic de gestion seulement et est spécifiée comme management0/0. Mais vous pouvez utiliser la commande **management-only** afin de configurer n'importe quelle interface pour être une interface de gestion uniquement. En outre, pour Management 0/0, vous pouvez désactiver le mode gestion seule pour que l'interface puisse acheminer le trafic comme toute autre interface. Référez-vous à [Référence des commandes de Cisco Security Appliance, version 8.0](#) pour plus d'informations sur la commande **management-only**.

Ce guide de configuration fournit un exemple de configuration pour inclure une brève introduction à la technologie ASA/PIX 7.x Active/Standby. Référez-vous au [Guide de référence des commandes ASA/PIX pour mieux comprendre la théorie à la base de cette technologie](#).

Conditions préalables

Conditions requises

Configuration matérielle

Les deux unités contenues dans une configuration de basculement doivent avoir la même configuration matérielle. Elles doivent avoir le même modèle, le même nombre et le même type d'interfaces, et la même quantité de RAM.

Remarque : Les deux unités n'ont pas besoin de la même taille de mémoire Flash. Si vous utilisez des unités avec différentes tailles de mémoire flash dans votre configuration de basculement, assurez-vous que l'unité avec la mémoire flash la plus petite a assez d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Sinon, la synchronisation de la configuration de l'unité avec la mémoire flash la plus grande et de l'unité avec la mémoire flash la plus petite échoue.

Configuration logicielle requise

Les deux unités présentes dans une configuration de basculement doivent être en mode opérationnel (routé ou transparent, contexte unique ou multiple). Elles doivent avoir la même version logicielle majeure (premier numéro) et mineure (second numéro), mais vous pouvez utiliser différentes versions du logiciel dans un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 7.0(1) vers la version 7.0(2) sans que le basculement ne se désactive. Cisco recommande de mettre à niveau les deux unités à la même version pour assurer la compatibilité à long terme.

Reportez-vous à la section [Exécution de mises à niveau sans interruption pour les paires de basculement](#) du *Guide de configuration de ligne de commande de l'appliance de sécurité Cisco, version 8.0* pour plus d'informations sur la mise à niveau du logiciel sur une paire de basculement.

Exigences de licence

Sur la plate-forme ASA Security Appliance, au moins une des unités doit avoir une **licence d'utilisation illimitée**.

Remarque : Il peut être nécessaire de mettre à niveau les licences sur une paire de basculement afin d'obtenir des fonctionnalités et des avantages supplémentaires. Référez-vous à [Mise à niveau de clé de licence sur une paire de basculement](#) pour plus d'informations.

Remarque : Les fonctionnalités sous licence (telles que les homologues VPN SSL ou les contextes de sécurité) sur les deux appliances de sécurité qui participent au basculement doivent être identiques.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité ASA avec version 7.x et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Appliance de sécurité PIX avec versions 7.x et postérieures

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Basculement actif/actif

Cette section décrit le basculement actif/veille et comprend les rubriques suivantes :

- [Basculement actif/actif - Aperçu](#)
- [État principal/secondaire et état actif/veille](#)
- [Synchronisation d'initialisation et de configuration de périphérique](#)
- [Réplication des commandes](#)
- [Déclencheurs de basculement](#)
- [Opérations de basculement](#)

Basculement actif/actif - Aperçu

Le basculement actif/actif est uniquement disponible pour les appliances de sécurité en mode de contexte multiple. Dans la configuration de basculement actif/actif, les deux appliances de sécurité peuvent faire passer le trafic réseau.

Dans le cas d'un basculement actif/actif, vous divisez les contextes de sécurité sur l'appliance de sécurité en plusieurs groupes de basculement. Un groupe de basculement est un simple groupe comprenant un ou plusieurs contextes de sécurité. Vous pouvez créer un maximum de deux groupes de basculement sur l'appliance de sécurité. Le contexte admin fait toujours partie du premier groupe de basculement. Tous les contextes de sécurité non affectés font également partie du groupe de basculement 1 par défaut.

Le groupe de basculement forme l'unité de base pour le basculement dans l'unité de base pour le basculement dans le basculement actif/actif. La surveillance de panne, le basculement, et l'état actif/veille d'interface sont tous des attributs d'un groupe de basculement plutôt que de l'unité. Quand un groupe de basculement actif échoue, son état passe en veille tandis que le groupe de basculement en veille devient à son tour actif. Les interfaces dans le groupe de basculement devenant actif tiennent compte des adresses MAC et IP des interfaces du groupe de basculement ayant échoué. Les interfaces dans le groupe de basculement en état de veille remplacent les adresses MAC et IP en veille.

Remarque : une défaillance d'un groupe de basculement sur une unité ne signifie pas que l'unité a échoué. L'unité peut toujours avoir un autre groupe de basculement qui transmet le trafic sur elle.

État principal/secondaire et état actif/veille

Tout comme pour le basculement actif/veille, une unité dans une paire de basculement actif/actif est considérée comme unité principale, et l'autre unité comme unité secondaire. À la différence du basculement actif/veille, cela n'indique pas l'unité qui devient active quand les deux unités démarrent simultanément. Le fait d'être une unité principale ou secondaire intervient à deux niveaux :

- Détermine quelle unité fournit la configuration fonctionnelle à la paire quand les deux unités démarrent simultanément.
- Détermine sur quelle unité chaque groupe de basculement est en état actif quand les unités démarrent simultanément. Chaque groupe de basculement dans la configuration est défini avec une préférence pour l'unité principale ou secondaire. Vous pouvez configurer les deux groupes de basculement à l'état actif sur une seule unité de la paire, avec l'autre unité qui contient les groupes de basculement à l'état veille. Cependant, une configuration plus typique consiste à attribuer à chaque groupe de basculement une préférence de rôle différente pour rendre chacun actif sur une unité différente, et répartir le trafic entre les périphériques. **Remarque** : l'appliance de sécurité **ne** fournit **pas** de services d'équilibrage de charge. L'équilibrage de charge doit être géré par un routeur distribuant du trafic à l'appliance de sécurité.

La détermination de l'unité sur laquelle chaque groupe de basculement deviendra actif s'effectue de la manière suivante :

- Quand une unité démarre et que l'unité paire 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 l'une de ces occurrences : Un basculement s'est produit. Vous forcez manuellement le groupe de basculement sur l'autre unité avec la commande **no failover active**. Vous avez configuré le groupe de basculement avec la commande **preempt**, qui rend automatiquement actif le groupe de basculement sur l'unité souhaitée, dès que celle-ci est disponible.
- Quand les deux unités démarrent en même temps, chaque groupe de basculement devient actif sur son unité attribuée après que les configurations aient été synchronisées.

Synchronisation d'initialisation et de configuration de périphérique

La synchronisation de la configuration se produit quand une unité seule ou les deux unités d'une paire de basculement démarrent. Les configurations sont synchronisées comme suit :

- Quand une unité démarre et que l'unité paire est active (avec deux groupes de basculement actifs), l'unité qui démarre contacte l'unité active pour obtenir la configuration fonctionnelle indépendamment de la préférence principale ou secondaire attribuée à l'unité qui démarre.
- Quand les deux unités démarrent simultanément, l'unité secondaire obtient la configuration fonctionnelle à partir de l'unité principale.

Lorsque la réplication démarre, la console de l'appareil de sécurité sur l'unité qui envoie la configuration affiche le message « Commencer la réplication de configuration : Sending to mate » et, quand la réplication est terminée, le dispositif de sécurité affiche le message « End Configuration Replication to mate. » Lors de la réplication, les commandes entrées sur l'unité qui envoie la configuration ne peuvent pas se répliquer correctement vers l'unité homologue, et les commandes entrées sur l'unité qui reçoit la configuration peuvent être remplacées par la configuration reçue. Ne pas exécuter de commandes sur l'une ou l'autre des unités de la paire de basculement lors du processus de réplication de configuration. La réplication, qui dépend de la taille de la configuration, peut prendre de quelques secondes à plusieurs minutes.

Sur l'unité qui reçoit la configuration, celle-ci n'existe que dans la mémoire en cours d'exécution. Afin d'enregistrer la configuration dans la mémoire Flash après la synchronisation, entrez la commande **write memory all** dans l'espace d'exécution du système sur l'unité dont le groupe de basculement 1 est actif. La commande est répliquée sur l'unité paire, qui enregistre alors sa configuration dans la mémoire flash. L'utilisation du mot clé **all** avec cette commande entraîne l'enregistrement des configurations du système et du contexte.

Remarque : les configurations de démarrage enregistrées sur des serveurs externes sont accessibles depuis l'une ou l'autre unité sur le réseau et n'ont pas besoin d'être enregistrées séparément pour chaque unité. Alternativement, vous pouvez copier les fichiers de configuration de contextes à partir du disque de l'unité principale vers un serveur externe, puis les copier sur le disque de l'unité secondaire. Ainsi, elles deviennent disponibles lorsque l'unité est relancée.

Réplication des commandes

Une fois que les deux unités fonctionnent, des commandes sont reproduites à partir d'une unité à l'autre comme suit :

- Les commandes entrées dans un contexte de sécurité sont reproduites à partir de l'unité sur laquelle le contexte de sécurité apparaît comme étant actif vers l'unité paire. **Remarque** : le contexte est considéré à l'état actif d'une unité si le groupe de basculement auquel il appartient est à l'état actif de cette unité.
- Les commandes entrées dans l'espace d'exécution du système sont reproduites à partir de l'unité sur laquelle le groupe de basculement 1 est actif, vers l'unité sur laquelle le groupe de basculement 1 est en veille.
- Les commandes entrées dans un contexte de sécurité sont reproduites à partir de l'unité sur laquelle le groupe de basculement 1 est actif, vers l'unité sur laquelle le groupe de basculement 1 est en veille.

Toutes les commandes de configuration et de fichier (**copy**, **rename**, **delete**, **mkdir**, **rmdir**, etc.) sont répliquées, à ces exceptions près. Les commandes **show**, **debug**, **mode**, **firewall** et **failover lan unit** ne sont pas reproduites.

Une erreur dans l'entrée d'une commande et dans le choix de l'unité adéquate pour la

reproduction de commandes entraîne la désynchronisation des configurations. Ces modifications risquent d'être perdues lors de la prochaine synchronisation de la configuration initiale.

Vous pouvez utiliser la commande **write standby** pour resynchroniser les configurations désynchronisées. Pour le basculement actif/écriture standbyActive, la commande **write standby** se comporte comme suit :

- Si vous entrez la commande **write standby** dans l'espace d'exécution du système, la configuration système et les configurations pour tous les contextes de sécurité sur l'appliance de sécurité sont écrits sur l'unité paire. Ceci inclut les informations de configuration pour les contextes de sécurité en veille. Vous devez entrer la commande dans l'espace d'exécution du système de l'unité sur laquelle le groupe de basculement 1 est actif. **Remarque** : Si des contextes de sécurité sont à l'état actif sur l'unité homologue, la commande **write standby** entraîne l'arrêt des connexions actives via ces contextes. Utilisez la commande **failover active** sur l'unité qui fournit la configuration pour vous assurer que tous les contextes sont actifs sur cette unité avant d'entrer la commande **write standby**.
- Si vous entrez la commande **write standby** dans un contexte de sécurité, seule la configuration du contexte de sécurité est écrite sur l'unité paire. Vous devez entrer la commande dans le contexte de sécurité actif de l'unité.

Les commandes reproduites ne sont pas sauvegardées dans la mémoire flash une fois reproduites sur l'unité paire. Elles sont ajoutées à la configuration fonctionnelle. Pour sauvegarder des commandes reproduites dans la mémoire flash sur les deux unités, utilisez la commande **write memory** ou **copy running-config startup-config** sur l'unité à laquelle vous avez apporté les modifications. La commande est reproduite sur l'unité paire et entraîne la sauvegarde de la configuration dans la mémoire flash.

Déclencheurs de basculement

Dans le basculement actif/actif, le basculement peut être déclenché au niveau de l'unité si l'un de ces événements se produit :

- L'unité a une défaillance matérielle.
- L'unité a une panne d'alimentation.
- L'unité a une défaillance logicielle.
- Les commandes **No failover active** ou **failover active** sont entrées dans l'espace d'exécution du système.

Le basculement est déclenché au niveau du groupe de basculement quand l'un de ces événements se produit :

- Echec - Nombre trop élevé d'interfaces surveillées dans le groupe.
- La commande **no failover active group group_id** ou **failover active group group_id** est entrée.

Opérations de basculement

Dans le cas d'une configuration de basculement actif/actif, le basculement se produit au niveau d'un groupe de basculement et non au niveau du système. Par exemple, si vous indiquez 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 tandis que le groupe de basculement 1 devient actif sur l'unité secondaire.

Remarque : lorsque vous configurez le basculement actif/actif, assurez-vous que le trafic combiné des deux unités est dans la capacité de chaque unité.

Ce tableau montre l'opération de basculement pour chaque événement de défaillance. Pour chaque événement d'échec, la stratégie, qu'un basculement se produise ou non, les actions pour le groupe de basculement actif et les actions pour le groupe de basculement de secours sont indiquées.

Événement de défaillance	Politique	Action pour le groupe actif	Action pour le groupe en veille	Notes
Une unité a rencontré une défaillance logicielle ou électrique	Basculement	Passé en veille, marqué comme ayant échoué	Se met en veille. Marque l'unité active comme défaillante	Quand une unité dans une paire de basculement renvoie une erreur, tous les groupes de basculement actifs sur cette unité sont marqués comme ayant échoué et deviennent actifs sur l'unité paire.
Erreur d'interface dans le groupe de basculement actif au-delà du seuil	Basculement	Marquez le groupe actif comme ayant échoué	S'active	Aucune
Erreur d'interface dans le groupe de basculement en veille au-delà du seuil	Pas de basculement	Aucune opération	Marquez le groupe en veille comme ayant échoué	Quand le groupe de basculement en veille est marqué comme ayant échoué, le groupe de basculement actif n'essaye pas de basculer, même si le seuil d'erreur d'interface est dépassé.
Le groupe de	Pas de bascu	Aucune opér	Aucune opérat	À moins d'utiliser la commande preempt , les groupes de

basculement précédemment actif est restauré.	lement	ation	ion	basculement restent actifs sur l'unité sur laquelle ils se trouvent.
Le lien de basculement a eu une défaillance au démarrage	Pas de basculement	S'active	S'active	Si le lien de basculement a une défaillance au démarrage, les deux groupes de basculement sur les deux unités deviennent actifs.
Le lien de basculement dynamique a eu une défaillance	Pas de basculement	Aucune opération	Aucune opération	Les informations d'état sont périmées et les sessions se terminent si un basculement se produit.
Le lien de basculement a échoué pendant l'opération	Pas de basculement	S/O	S/O	Chaque unité marque l'interface de basculement comme ayant échoué. Vous devez restaurer le lien de basculement dès que possible car l'unité ne peut pas relayer l'unité en veille alors que le lien de basculement est défaillant.

[Basculement périodique et dynamique](#)

Le dispositif de sécurité supporte deux types de basculement : périodique et dynamique. Cette section comprend les rubriques suivantes :

- [Basculement périodique](#)
- [Basculement dynamique](#)

[Basculement périodique](#)

Quand un basculement se produit, toutes les connexions actives sont supprimées. Les clients doivent rétablir les connexions quand la nouvelle unité active prend le relais.

[Basculement dynamique](#)

Quand le basculement dynamique est activé, l'unité active transfère continuellement les informations d'état par connexion à l'unité en veille. Lorsqu'un basculement s'est produit, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications utilisateur supportées ne doivent pas nécessairement se reconnecter pour garder la même session de transmission.

Les informations d'état transmises à l'unité en veille incluent les éléments suivants :

- La table de conversion NAT
- Les états des connexions TCP
- Les états des connexions UDP
- La table ARP
- La table des ponts de la couche 2 (quand elle fonctionne en mode pare-feu transparent)
- Les états des connexions HTTP (si la réplication HTTP est activée)
- La table SA ISAKMP et IPSec
- La base des connexions GTP PDP

Les informations transmises à l'unité en veille quand le basculement dynamique est activé incluent les éléments suivants :

- La table des connexions HTTP (sauf si la réplication HTTP est activée)
- La table des authentifications utilisateur (uauth)
- Les tables de routage
- Les informations d'état relatives aux modules des services de sécurité

Remarque : si le basculement se produit au sein d'une session Cisco IP SoftPhone active, l'appel reste actif car les informations d'état de la session d'appel sont répliquées sur l'unité de secours. Quand l'appel est terminé, le client IP SoftPhone perd la connexion avec le gestionnaire d'appels. Cela se produit car il n'y a aucune information de session pour le message de raccrochage CTIQBE sur l'unité en veille. Quand le client IP SoftPhone ne reçoit pas de réponse du gestionnaire d'appels dans un certain délai, il considère le gestionnaire d'appels comme inaccessible et annule son enregistrement.

Limites de configuration de basculement

Vous ne pouvez pas configurer le basculement avec ces types d'adresse IP :

- Adresse IP obtenue via DHCP
- Adresse IP obtenue par PPPoE
- Adresses IPv6

Ces restrictions s'appliquent également dans les cas suivants :

- Le basculement dynamique n'est pas pris en charge sur l'appliance de sécurité adaptative ASA 5505.
- Le basculement actif/actif n'est pas pris en charge sur l'appliance de sécurité adaptative ASA 5505.
- Vous ne pouvez pas configurer le basculement quand Easy VPN Remote est activé sur l'appliance de sécurité adaptative ASA 5505.
- Le basculement VPN n'est pas pris en charge en mode de contexte multiple.

Fonctions non prises en charge

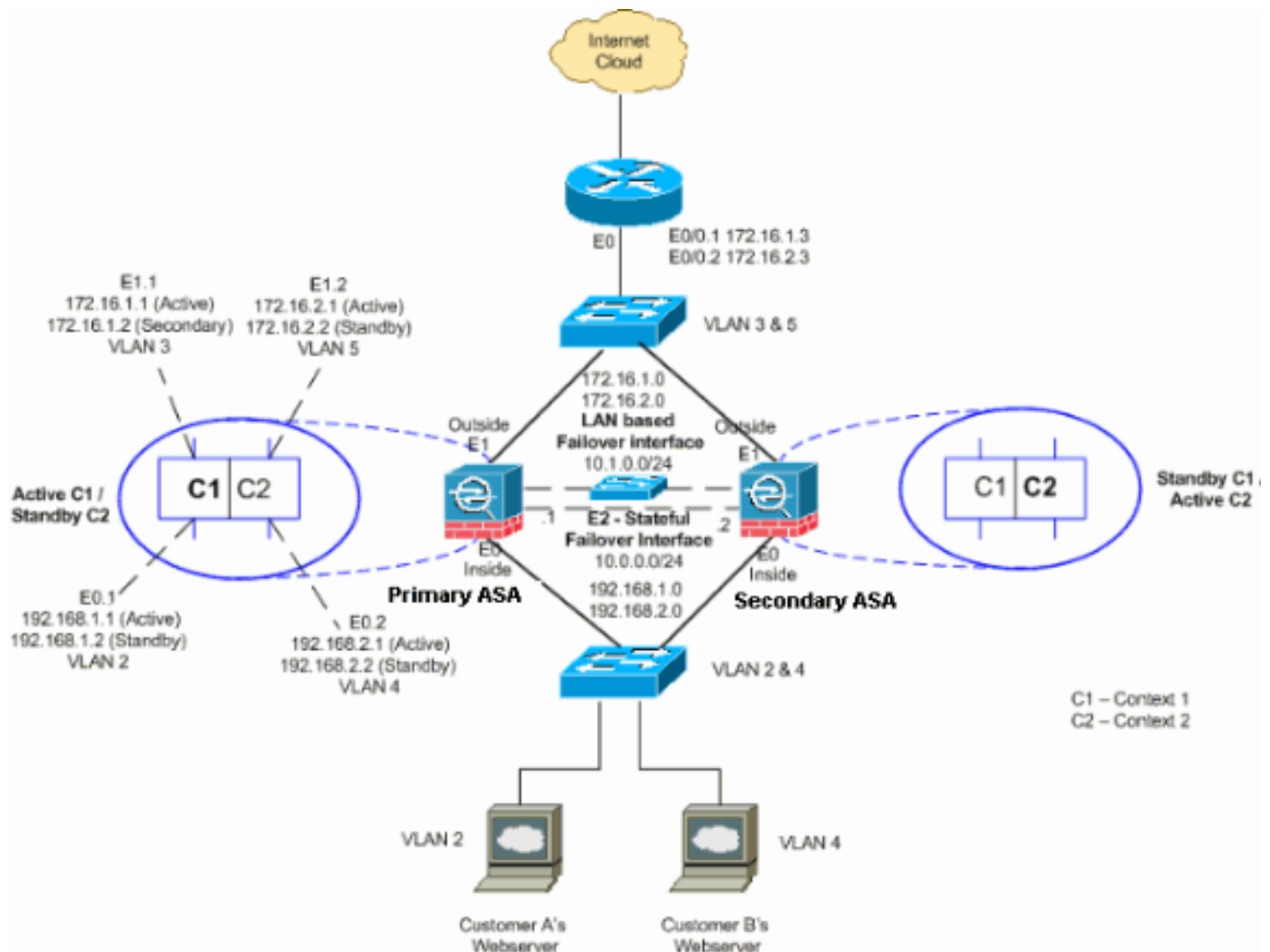
Le mode de contexte multiple ne prend pas en charge les caractéristiques suivantes :

- Protocoles de routage dynamique Les contextes de sécurité prennent uniquement en charge les routes statiques. Vous ne pouvez pas activer OSPF ou RIP en mode de contexte multiple.
- VPN
- Multidiffusion

Configuration du basculement actif/actif avec LAN

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cette section décrit comment configurer le basculement actif/actif avec un lien de basculement Ethernet. Quand vous configurez le basculement basé sur le LAN, vous devez amorcer le périphérique secondaire pour identifier le lien de basculement afin que le périphérique secondaire puisse obtenir la configuration en cours du périphérique principal.

Remarque : au lieu d'un câble Ethernet croisé pour relier directement les unités, Cisco vous recommande d'utiliser un commutateur dédié entre les unités principale et secondaire.

Cette section traite des thèmes suivants :

- [Configuration de l'unité principale](#)
- [Configuration de l'unité secondaire](#)

Configuration de l'unité principale

Suivez ces étapes afin de configurer l'unité principale dans la configuration du basculement actif/actif :

1. Si vous ne l'avez pas déjà fait, configurez les adresses IP actives et en veille pour chaque interface de données (mode routé), ou pour l'interface de gestion d'adresse IP (mode transparent) ou pour l'interface uniquement dédiée à la gestion. L'adresse IP en standby est utilisée sur le dispositif de sécurité qui est l'unité en veille en cours. Elle doit se trouver sur le même sous-réseau que l'adresse IP active. Vous devez configurer les adresses d'interface au sein de chaque contexte. Utilisez la commande **change context pour passer d'un contexte à l'autre**. L'invite de commande devient hostname/context(config-if)#, où context est le nom du contexte actif. Dans le mode multi-contextes transparent du pare-feu, vous devez entrer une adresse IP de gestion pour chaque contexte. **Remarque** : Ne configurez pas d'adresse IP pour le lien de basculement dynamique si vous utilisez une interface de basculement dynamique dédiée. Vous utilisez la commande **failover interface ip** afin de configurer une interface de basculement dynamique dédiée dans une étape ultérieure.

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

Dans l'exemple, l'interface externe pour context1 de l'ASA principal est configurée de cette manière :

```
ASA/context1(config)#ip address 172.16.1.1 255.255.255.0
                          standby 172.16.1.2
```

Pour Context2 :

```
ASA/context2(config)#ip address 192.168.2.1 255.255.255.0
                          standby 192.168.2.2
```

En mode pare-feu routé et pour l'interface de gestion seule, cette commande est entrée dans le mode de configuration d'interface pour chaque interface. En mode pare-feu transparent, cette commande est entrée dans le mode de configuration globale.

2. Configurez les paramètres de base de basculement dans l'espace d'exécution du système. (Appliance de sécurité PIX uniquement) Activer le basculement avec LAN :

```
hostname(config)#failover lan enable
```

Sélectionnez l'unité en tant qu'unité principale.

```
hostname(config)#failover lan unit primary
```

Spécifiez le lien de basculement :

```
hostname(config)#failover lan interface if_name phy_if
```

Dans cet exemple, nous utilisons l'interface Ethernet 3 en tant qu'interface de basculement avec LAN.

```
ASA(config)#failover lan interface LANFailover ethernet3
```

L'argument if_name affecte un nom logique à l'interface spécifiée par l'argument phy_if .

L'argument phy_if peut être le nom du port physique, par exemple Ethernet1, ou une sous-

interface créée précédemment, par exemple Ethernet0/2.3. Sur l'appliance de sécurité adaptative ASA 5505, l'argument `phy_if` spécifie un VLAN. Cette interface ne doit pas être utilisée à d'autres fins, excepté en tant que lien de basculement dynamique. Spécifiez les adresses IP actives et en veille du lien de basculement :

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

Dans cet exemple, nous utilisons 10.1.0.1 comme adresse active et 10.1.0.2 en tant qu'adresse IP en veille pour l'interface de basculement.

```
ASA(config)#failover interface ip LANFailover  
10.1.0.1 255.255.255.0 standby 10.1.0.2
```

L'adresse IP de secours doit être dans le même sous-réseau que l'adresse IP active. Vous n'avez pas besoin d'identifier le masque de sous-réseau de l'adresse IP en standby. L'adresse IP et l'adresse MAC du lien de basculement ne changent pas lors du basculement. L'adresse IP active reste toujours avec l'unité principale, tandis que l'adresse en standby reste avec l'unité secondaire.

Configuration de l'unité secondaire

Lorsque vous configurez le basculement actif/actif sur LAN, vous devez amorcer l'unité secondaire afin de reconnaître le lien de basculement. Ainsi, l'unité secondaire peut accéder à la configuration fonctionnelle et la recevoir à partir de l'unité principale.

Suivez ces étapes afin de démarrer l'unité secondaire dans la configuration du basculement actif/actif :

1. (Appliance de sécurité PIX uniquement) Activer le basculement avec LAN.

```
hostname(config)#failover lan enable
```

2. Définissez l'interface de basculement. Utilisez les paramètres que vous avez utilisés pour l'unité principale : Spécifiez l'interface à utiliser comme interface de basculement.

```
hostname(config)#failover lan interface if_name phy_if
```

```
ASA(config)#failover lan interface LANFailover ethernet3
```

L'argument `if_name` affecte un nom logique à l'interface spécifiée par l'argument `phy_if`. L'argument `phy_if` peut être le nom du port physique, par exemple Ethernet1, ou une sous-interface créée précédemment, par exemple Ethernet0/2.3. Sur l'appliance de sécurité adaptative ASA 5505, l'argument `phy_if` spécifie un VLAN. Affectez l'adresse active et l'adresse en veille au lien de basculement :

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

```
ASA(config)#failover interface ip LANFailover 10.1.0.1  
255.255.255.0 standby 10.1.0.2
```

Remarque : Entrez cette commande exactement comme vous l'avez entrée sur l'unité principale lorsque vous avez configuré l'interface de basculement. L'adresse IP de secours doit être dans le même sous-réseau que l'adresse IP active. Vous n'avez pas besoin d'identifier le masque de sous-réseau de l'adresse en standby. Activez l'interface.

```
hostname(config)#interface phy_if
```

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

3. Désignez cette unité comme l'unité secondaire.

```
hostname(config)#failover lan unit secondary
```

Remarque : Cette étape est facultative car, par défaut, les unités sont désignées comme secondaires, sauf si elles ont été configurées autrement.

4. Activez le basculement.

```
hostname(config)#failover
```

Une fois le basculement activé, l'unité active envoie la configuration figurant dans la mémoire en cours à l'unité en veille. Lors de la synchronisation de la configuration, les messages **Beginning configuration replication: Sending to mate** et **End Configuration Replication to mate** apparaissent sur la console de l'unité active. **Remarque :** Émettez d'abord la commande **failover** sur le périphérique principal, puis émettez-la sur le périphérique secondaire. Une fois la commande **failover** exécutée sur le périphérique secondaire, le périphérique secondaire extrait immédiatement la configuration du périphérique principal et se met *en veille*. Le périphérique ASA principal demeure opérationnel, achemine le trafic normalement et se marque comme étant le périphérique *actif*. À partir de là, chaque fois qu'une défaillance se produit sur le périphérique actif, le périphérique en veille s'active.

5. Après que le fonctionnement configuration ait complété la reproduction, entrez dans ceci commande pour sauvegarder configuration à la mémoire flash :

```
hostname(config)#copy running-config startup-config
```

6. S'il y a lieu, forcez n'importe quel groupe de basculement actif sur le principal à l'état actif sur l'unité secondaire. Pour forcer un groupe de basculement à devenir actif sur l'unité secondaire, entrez cette commande dans l'espace d'exécution du système sur l'unité principale :

```
hostname#no failover active group group_id
```

L'argument `group_id` permet de spécifier le groupe que vous souhaitez activer sur l'unité secondaire.

Configurations

Ce document utilise les configurations suivantes :

Configuration ASA principale - Context1

```
ASA/context1(config)#show running-config
: Saved
:
ASA Version 7.2(3)

!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

```

!
interface inside_context1
  nameif inside
  security-level 100
  !--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
  nameif outside
  security-level 0
  !--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc

```



```
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
```

Configuration ASA principale - Context2

```
ASA/context2(config)#show running-config
: Saved
:
ASA Version 7.2(3)

!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
 !--- Configure the active and standby IP's for the
 logical inside !--- interface of the context2. ip
 address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
 !--- Configure the active and standby IP's for the
 logical outside !--- interface of the context2. ip
 address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
```

```
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:000000000000000000000000000000000000
: end
```

ASA principal

```
ASA(config)#show running-config
: Saved
:
ASA Version 7.2(3) <system>
!
  !--- Use the firewall transparent command !--- in
global configuration mode in order to !--- set the
firewall mode to transparent mode.

firewall transparent
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
  vlan 2
!
interface Ethernet0.2
  vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
  vlan 3
!
interface Ethernet1.2
  vlan 5
```

```
!  
!--- Configure "no shutdown" in the stateful failover  
interface as well as !--- LAN Failover interface of both  
Primary and secondary ASA/PIX. interface Ethernet2  
description STATE Failover Interface  
!  
interface Ethernet3  
  description LAN Failover Interface  
!  
interface Ethernet4  
  shutdown  
!  
interface Ethernet5  
  shutdown  
!  
class default  
  limit-resource All 0  
  limit-resource ASDM 5  
  limit-resource SSH 5  
  limit-resource Telnet 5  
!  
  
ftp mode passive  
pager lines 24  
failover  
failover lan unit primary  
!--- Command to assign the interface for LAN based  
failover failover lan interface LANFailover Ethernet3  
!--- Configure the Authentication/Encryption key  
failover key *****  
failover link stateful Ethernet2  
!--- Configure the active and standby IP's for the LAN  
based failover failover interface ip LANFailover  
10.1.0.1 255.255.255.0 standby 10.1.0.2  
failover interface ip stateful 10.0.0.1 255.255.255.0  
standby 10.0.0.2  
failover group 1  
failover group 2  
  secondary  
no asdm history enable  
arp timeout 14400  
console timeout 0  
  
admin-context admin  
context admin  
  config-url flash:/admin.cfg  
!  
  
context context1  
  allocate-interface Ethernet0.1 inside_context1  
  allocate-interface Ethernet1.1 outside_context1  
  config-url flash:/context1.cfg  
  join-failover-group 1  
!  
  
context context2  
  allocate-interface Ethernet0.2 inside_context2  
  allocate-interface Ethernet1.2 outside_context2  
  config-url flash:/context2.cfg  
  join-failover-group 2  
!  
  
prompt hostname context  
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
```

```
: end
```

ASA secondaire

```
ASA#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover key *****
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

Vérification

Utilisation de la commande show failover

Cette section décrit la sortie de la commande **show failover** . Sur chaque unité, vous pouvez vérifier l'état de basculement avec la commande **show failover** .

ASA principal

```
ASA(config-subif)#show failover
```

```
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:45 UTC Jan 17 2009
Group 2 last failover at: 06:12:43 UTC Jan 17 2009
```

```
This host:      Primary
Group 1        State:          Active
                Active time:    359610 (sec)
Group 2        State:          Standby Ready
                Active time:    3165 (sec)
```

```
context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal
context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal
```

```
Other host:    Secondary
Group 1        State:          Standby Ready
                Active time:    0 (sec)
Group 2        State:          Active
                Active time:    3900 (sec)
```

```
context1 Interface inside (192.168.1.2): Normal
context1 Interface outside (172.16.1.2): Normal
context2 Interface inside (192.168.2.1): Normal
context2 Interface outside (172.16.2.1): Normal
```

```
Stateful Failover Logical Update Statistics
```

```
Link : stateful Ethernet2 (up)
```

Stateful Obj	xmit	xerr	rcv	rerr
General	48044	0	48040	1
sys cmd	48042	0	48040	1
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	0	0	0	0
ARP tbl	2	0	0	0
Xlate_Timeout	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	72081
Xmit Q:	0	1	48044

ASA secondaire

ASA(config)#show failover

```

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:46 UTC Jan 17 2009
Group 2 last failover at: 06:12:41 UTC Jan 17 2009

```

```

This host:      Secondary
Group 1        State:          Standby Ready
                Active time:    0 (sec)
Group 2        State:          Active
                Active time:    3975 (sec)

```

```

context1 Interface inside (192.168.1.2): Normal
context1 Interface outside (172.16.1.2): Normal
context2 Interface inside (192.168.2.1): Normal
context2 Interface outside (172.16.2.1): Normal

```

```

Other host:    Primary
Group 1        State:          Active
                Active time:    359685 (sec)
Group 2        State:          Standby Ready
                Active time:    3165 (sec)

```

```

context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal
context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal

```

Stateful Failover Logical Update Statistics

```

Link : stateful Ethernet2 (up)
Stateful Obj  xmit      xerr      rcv      rerr
General      940        0         942      2
sys cmd      940        0         940      2
up time      0          0         0        0
RPC services 0          0         0        0
TCP conn     0          0         0        0
UDP conn     0          0         0        0
ARP tbl      0          0         2        0
Xlate_Timeout 0          0         0        0

```

```

Logical Update Queue Information
                Cur      Max      Total
Recv Q:         0       1       1419
Xmit Q:         0       1       940

```

Utilisez la commande **show failover state** pour vérifier l'état.

ASA principal

```
ASA(config)#show failover state
```

```

                State          Last Failure Reason    Date/Time
This host -    Primary
  Group 1      Active
  Group 2      Standby Ready  None
Other host -   Secondary
  Group 1      Standby Ready  None
  Group 2      Active          None

```

```
====Configuration State====
```

```
    Sync Done
```

```
====Communication State====
```

```
    Mac set
```

Unité secondaire

```
ASA(config)#show failover state
```

```

                State          Last Failure Reason    Date/Time
This host -    Secondary
  Group 1      Standby Ready  None
  Group 2      Active          None
Other host -   Primary
  Group 1      Active          None
  Group 2      Standby Ready  None

```

```
====Configuration State====
```

```
    Sync Done - STANDBY
```

```
====Communication State====
```

```
    Mac set
```

Pour vérifier les adresses IP de l'unité de basculement, utilisez **show failover interface** command.

Unité principale

```
ASA(config)#show failover interface
```

```
    interface stateful Ethernet2
```

```
        System IP Address: 10.0.0.1 255.255.255.0
```

```
        My IP Address      : 10.0.0.1
```

```
        Other IP Address   : 10.0.0.2
```

```
    interface LANFailover Ethernet3
```

```
        System IP Address: 10.1.0.1 255.255.255.0
```

```
        My IP Address      : 10.1.0.1
```

```
        Other IP Address   : 10.1.0.2
```

Unité secondaire

```
ASA(config)#show failover interface
```

```
    interface LANFailover Ethernet3
```

```
System IP Address: 10.1.0.1 255.255.255.0
My IP Address      : 10.1.0.2
Other IP Address   : 10.1.0.1
interface stateful Ethernet2
System IP Address: 10.0.0.1 255.255.255.0
My IP Address      : 10.0.0.2
Other IP Address   : 10.0.0.1
```

Affichage des interfaces surveillées

Pour afficher l'état des interfaces surveillées : En mode de contexte unique, entrez la commande `show monitor-interface` en mode de configuration globale. En mode de contexte multiple, entrez la commande `show monitor-interface` dans un contexte.

Remarque : afin d'activer la surveillance de l'état sur une interface spécifique, utilisez la commande [monitor-interface](#) en mode de configuration globale :

```
monitor-interface <if_name>
```

ASA principal

```
ASA/context1(config)#show monitor-interface
This host: Secondary - Active
  Interface inside (192.168.1.1): Normal
  Interface outside (172.16.1.1): Normal
Other host: Secondary - Standby Ready
  Interface inside (192.168.1.2): Normal
  Interface outside (172.16.1.2): Normal
```

ASA secondaire

```
ASA/context1(config)#show monitor-interface
This host: Secondary - Standby Ready
  Interface inside (192.168.1.2): Normal
  Interface outside (172.16.1.2): Normal
Other host: Secondary - Active
  Interface inside (192.168.1.1): Normal
  Interface outside (172.16.1.1): Normal
```

Remarque : si vous n'entrez pas d'adresse IP de basculement, la commande **show failover** affiche 0.0.0.0 pour l'adresse IP et la surveillance des interfaces reste en *attente*. Vous devez définir une adresse IP de basculement pour faire fonctionner le basculement. Référez-vous à [show failover](#) pour plus d'informations sur différents états pour le basculement.

Affichage des commandes de basculement dans la configuration en cours

Pour afficher les commandes de basculement dans la configuration en cours, entrez la commande suivante :

```
hostname(config)#show running-config failover
```

Toutes les commandes de **basculement sont affichées**. Sur les unités qui fonctionnent en mode de contexte multiple, entrez la commande `show running-config failover` dans l'espace d'exécution

du système. Entrez la commande **show running-config all failover** pour afficher les commandes de basculement dans la configuration en cours et pour inclure les commandes dont vous n'avez pas changé la valeur par défaut.

Tests sur la fonctionnalité de basculement

Complétez ces étapes afin de tester la fonctionnalité de basculement :

1. Testez que votre unité active ou votre groupe de basculement transmet le trafic comme prévu avec FTP, par exemple, pour envoyer un fichier entre les hôtes sur différentes interfaces.
2. Forcez un basculement vers l'unité en veille avec la commande suivante : Pour le basculement actif/actif, entrez cette commande sur l'unité sur laquelle le groupe de basculement, qui contient l'interface qui connecte vos hôtes est actif :

```
hostname(config)#no failover active group group_id
```

3. Utilisez FTP afin d'envoyer un autre fichier entre les deux mêmes hôtes.
4. Si le test a échoué, entrez la **commande show failover** afin de vérifier l'état du basculement.
5. Lorsque vous avez fini, vous pouvez restaurer l'unité ou le groupe de basculement dans son état actif avec la commande : Pour le basculement actif/actif, entrez cette commande sur l'unité sur laquelle le groupe de basculement, qui contient l'interface qui connecte vos hôtes est actif :

```
hostname(config)#failover active group group_id
```

Basculement forcé

Pour forcer l'unité en veille à s'activer, entrez l'une des commandes suivantes :

Entrez cette commande dans l'espace d'exécution du système de l'unité pour laquelle le groupe de basculement est en veille :

```
hostname#failover active group group_id
```

Sinon, entrez cette commande dans l'espace d'exécution du système de l'unité pour laquelle le groupe de basculement est actif :

```
hostname#no failover active group group_id
```

Lorsque vous entrez cette commande dans le système, l'espace d'exécution entraîne l'activation de tous les groupes de basculement :

```
hostname#failover active
```

Basculement désactivé

Pour désactiver le basculement, entrez la commande suivante :

```
hostname(config)#no failover
```

Si vous désactivez le basculement sur une paire actif/veille, l'état actif et en veille de chaque unité est conservé jusqu'à ce que vous redémarriez. Par exemple, l'unité en veille reste en mode de veille, et donc les deux unités ne commencent pas à acheminer le trafic. Pour activer l'unité en veille (même avec le basculement désactivé), référez-vous à la section [Basculement forcé](#).

Si vous désactivez le basculement sur une paire actif/actif, les groupes de basculement restent à l'état actif sur l'unité sur laquelle ils sont actuellement actifs, quelle que soit l'unité qu'ils doivent préférer selon leur configuration. La commande **No failover** peut être entrée dans l'espace d'exécution du système.

[Restauration d'une unité défaillante](#)

Pour rétablir un groupe de basculement actif/actif ayant échoué vers l'état non-échoué, veuillez entrer la commande suivante :

```
hostname(config)#failover reset group group_id
```

Si vous remettez une unité défaillante dans un état non défaillant, elle ne s'active pas automatiquement. Les unités ou groupes restaurés demeurent en état de veille jusqu'à ce que le basculement (forcé ou naturel) les active. Cela ne concerne pas un groupe de basculement configuré avec la commande **preempt**. Un groupe de basculement auparavant actif s'active s'il est configuré avec la commande **preempt** et si l'unité sur laquelle il a eu une défaillance est son unité préférée.

[Dépannage](#)

Quand un basculement se produit, les deux dispositifs de sécurité envoient des messages système. Cette section comprend les rubriques suivantes :

1. [Messages système de basculement](#)
2. [Messages de débogage](#)
3. [SNMP](#)

[Messages système de basculement](#)

Le dispositif de sécurité émet un certain nombre de messages système relatifs au basculement au niveau de priorité 2, ce qui indique un état critique. Pour afficher ces messages, référez-vous à [Configuration de journalisation et messages du journal système des dispositifs de sécurité Cisco pour activer la journalisation et consulter les descriptions des messages système](#).

Remarque : Au sein de la commutation, le basculement s'arrête logiquement, puis déclenche les interfaces, ce qui génère des messages syslog **411001** et **411002**. Cette activité est normale.

[L'unité principale a perdu les communications de basculement avec l'autre unité dans l'interface nom_interface](#)

Ce message de basculement s'affiche si l'unité de la paire de basculement ne peut plus communiquer avec l'autre unité de la paire. Principal peut aussi être répertorié comme Secondaire pour l'unité secondaire.

(L'unité principale) a perdu les communications de basculement avec l'autre unité dans l'interface nom_interface

Vérifiez que le réseau connecté à l'interface spécifiée fonctionne correctement.

[Messages de débogage](#)

Pour consulter les messages de débogage, entrez la commande **debug fover**. [Référez-vous à Référence de commandes des dispositifs de sécurité Cisco version 7.2 pour plus d'informations.](#)

Remarque : Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du processeur, elle peut affecter considérablement les performances du système. Par conséquent, n'utilisez les commandes **debug fover** que pour résoudre des problèmes spécifiques ou dans des sessions de dépannage avec le personnel d'assistance technique Cisco.

[SNMP](#)

Pour recevoir les interruptions SNMP syslog relatives au basculement, configurez les agents SNMP pour qu'ils envoient des interruptions SNMP aux stations de gestion SNMP, définissez un hôte syslog et compilez la MIB syslog Cisco sur votre station de gestion SNMP. Référez-vous aux commandes **snmp-server** et **logging** dans le [Guide de référence des commandes des dispositifs de sécurité Cisco pour plus d'informations.](#)

[Délai d'interrogation du basculement](#)

Pour spécifier les délais d'interrogation et de mise en suspens des unités de basculement, utilisez la commande **failover polltime** dans le mode de configuration globale.

`failover polltime unit msec [time]` représente le délai alloué pour vérifier l'existence de l'unité en veille avec les messages d'interrogation hello.

De même, `failover holdtime unit msec [time]` représente l'intervalle défini durant lequel une unité doit recevoir un message hello sur le lien de basculement et après lequel l'autre unité est déclarée défaillante.

Référez-vous à [failover polltime pour plus d'informations.](#)

[AVERTISSEMENT : Échec du déchiffrement du message de basculement](#)

Message d'erreur :

`Failover message decryption failure. Please make sure both units have the same failover shared key and crypto license or system is not out of memory`

Ce problème provient de la configuration de la clé de basculement. Pour résoudre ce problème, supprimez la clé de basculement et configurez la nouvelle clé partagée.

Informations connexes

- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Logiciels pare-feu Cisco PIX](#)
- [Configuration de basculement de Firewall Services Module \(FWSM\)](#)
- [Dépannage du basculement FWSM](#)
- [Fonctionnement du basculement sur le pare-feu Cisco Secure PIX](#)
- [Support et documentation techniques - Cisco Systems](#)