Basculement pour la haute disponibilité dans le nuage public

Ce chapitre décrit comment configurer le basculement actif/de secours pour atteindre la haute disponibilité de ASA virtuel dans un environnement de nuage public, comme Microsoft Azure.

À propos du basculement dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA). La haute accessibilité dans le nuage public met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

La liste suivante décrit les composants principaux de la solution de nuage public à haute disponibilité :

- **ASA virtuel actif** : l'ASA virtuel dans la paire à haute disponibilité qui est configuré pour gérer le trafic de pare-feu pour les homologues à haute disponibilité.
- **ASA virtuel en veille** : l'ASA virtuel dans la paire à haute disponibilité qui ne gère pas le trafic du pare-feu et prend le relais comme ASA virtuel actif en cas de défaillance d'un ASA virtuel actif. Il est appelé sauvegarde plutôt que de secours, car il ne prend pas l'identité de son homologue en cas de basculement.
- **Agent à haute disponibilité** : un processus allégé qui s'exécute sur l'ASA virtuel et détermine le rôle de haute disponibilité (actif/sauvegarde) d'un ASA virtuel, détecte les défaillances de son homologue à haute disponibilité et effectue les actions en fonction de son rôle de haute disponibilité.

Sur l'ASA physique et l'ASA virtuel en nuage non public, le système gère les conditions de basculement à l'aide de demandes ARP gratuites, dans lesquelles l'ASA de secours envoie une requête ARP gratuite indiquant qu'il est désormais associé aux adresses IP et MAC actives. La plupart des environnements de nuage public n'autorisent pas le trafic de diffusion de cette nature. Pour cette raison, une configuration à haute disponibilité dans le nuage public nécessite le redémarrage des connexions permanentes lors du basculement.

L'intégrité de l'unité active est surveillée par l'unité de secours pour déterminer si des conditions de basculement spécifiques sont remplies. Si ces conditions sont remplies, le basculement se produit. Le délai de basculement peut varier de quelques secondes à plus d'une minute selon la réactivité de l'infrastructure de nuage public.

À propos du basculement actif/de secours

Dans le basculement actif/sauvegarde, une unité est l'unité active. Elle transmet le trafic. L'unité de sauvegarde ne transmet pas activement le trafic et n'échange aucune information de configuration avec l'unité active. Le basculement actif/de sauvegarde vous permet d'utiliser un périphérique ASA virtuel de sauvegarde pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, elle passe à l'état de sauvegarde pendant que l'unité de sauvegarde passe à l'état actif.

Rôles principal/secondaire et état actif/de secours

Lors de la configuration du basculement actif/de sauvegarde, vous configurez une unité comme principale et l'autre comme secondaire. À ce stade, les deux unités agissent comme deux périphériques distincts pour la configuration des périphériques et des politiques, ainsi que pour les événements, les tableaux de bord, les rapports et la surveillance de l'intégrité.

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité de sauvegarde, à savoir l'unité qui transmet activement le trafic. Bien que les deux unités soient capables de transmettre du trafic, seule l'unité principale répond aux sondes de l'équilibreur de charges et programme toutes les routes configurées pour l'utiliser comme destination de routage. La fonction principale de l'unité de sauvegarde est de surveiller l'intégrité de l'unité principale. L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).

Connexion de basculement

L'ASA virtuel de secours surveille l'intégrité de l'ASA virtuel actif à l'aide d'une connexion de basculement établie sur TCP :

- L'ASA virtuel actif agit comme un serveur de connexion en ouvrant un *port d'écoute*.
- L'ASA virtuel de secours se connecte à l'ASA virtuel actif à l'aide du *port de connexion*.
- En général, le *port d'écoute* et le *port de connexion* sont identiques, sauf si votre configuration requiert une traduction d'adresses réseau entre les unités ASA virtuel.

L'état de la connexion de basculement détecte la défaillance de l'ASA virtuelactif. Lorsque l'ASA virtuel de secours voit la connexion de basculement établie, il considère l'ASA virtuel actif comme *ayant échoué*. De même, si l'ASA virtuel de secours ne reçoit pas de réponse à un message keepalive envoyé à l'unité active, il considère l'ASA virtuel actif comme *ayant échoué*.

Thèmes connexes

Messages de sondage et Hello

L'ASA virtuel de secours envoie des messages Hello via la connexion de basculement à l'ASA virtuel actif et attend une réponse Hello en retour. La synchronisation des messages utilise un intervalle entre les interrogations, la période entre la réception d'une réponse Hello par l'unité ASA virtuel de secours et l'envoi du message Hello suivant. La réception de la réponse est imposée par un délai d'expiration de réception, appelé délai de rétention. Si la réception de la réponse Hello expire, l'ASA virtuel actif est considéré comme ayant échoué.

Les intervalles d'interrogation et de délai de rétention sont des paramètres configurables; voir Configurer les critères de basculement et les autres paramètres, à la page 12.

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 sauvegarde.
- 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 sauvegarde.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire. Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de sauvegarde, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 1 : Événements de basculement

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité de sauvegarde voit une connexion de basculement se fermer	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Il s'agit du scénario de basculement standard.
L'unité active voit une connexion de basculement se fermer	Aucun basculement	Marquer la sauvegarde comme ayant échoué	S.O.	Le basculement vers une unité inactive ne doit jamais se produire.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité active voit un délai d'expiration TCP sur la liaison de basculement	Aucun basculement	Marquer la sauvegarde comme ayant échoué	Aucune action	Le basculement ne doit pas se produire si l'unité active ne reçoit pas de réponse de l'unité de sauvegarde.
L'unité de sauvegarde voit un délai d'expiration TCP sur la liaison de basculement	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante Essayer d'envoyer la commande de basculement à l'unité active	L'unité de sauvegarde suppose que l'unité active n'est pas en mesure de continuer à fonctionner et prend le relais. Si l'unité active est toujours opérationnelle, mais n'envoie pas de réponse à temps, l'unité de sauvegarde envoie la commande de basculement à l'unité active.
Échec de l'authentification de l'unité active	Aucun basculement	Aucune action	Aucune action	Comme l'unité de sauvegarde modifie les tables de routage, c'est la seule unité qui doit être authentifiée auprès d'Azure. Peu importe si l'unité active est authentifiée auprès d'Azure ou non.
Échec de l'authentification de l'unité de sauvegarde	Aucun basculement	Marquer la sauvegarde comme non authentifiée	Aucune action	Le basculement ne peut pas se produire si l'unité de sauvegarde n'est pas authentifiée auprès d'Azure.
L'unité active lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité active lance le basculement en ferme la connexion de liaison de basculement. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.
L'unité de sauvegarde lance le basculement intentionnel	Basculement	Devenir une sauvegarde	Devenir active	L'unité de sauvegarde lance le basculement en envoyant un message de basculement à l'unité active. Lorsque l'unité active voit le message, elle ferme la connexion et devient l'unité de sauvegarde. L'unité de sauvegarde voit la connexion se terminer et devient l'unité active.

Défaillance	Politique	Action active	Action de sauvegarde	Notes
L'unité précédemment active récupère	Aucun basculement	Devenir une sauvegarde	Marquer le partenaire comme sauvegarde	Le basculement ne doit pas se produire, sauf si cela est absolument nécessaire.
L'unité active voit le message de basculement de l'unité de sauvegarde	Basculement	Devenir une sauvegarde	Devenir active	Peut se produire si un basculement manuel a été lancé par un utilisateur, ou si l'unité de sauvegarde a vu le délai d'expiration TCP, mais l'unité active est en mesure de recevoir des messages de l'unité de sauvegarde.

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

ASA virtuel Basculement pour la haute disponibilité dans le nuage public

Pour assurer la redondance, vous pouvez déployer l'ASA virtuel dans un environnement de nuage public dans une configuration active/de secours à haute accessibilité (HA).

- Pris en charge uniquement sur le nuage public Microsoft Azure; lors de la configuration de la machine virtuelle ASA virtuel, le nombre maximal de vCPU pris en charge est de 8; et la mémoire maximale prise en charge est de 64 Go de RAM. Consultez le Guide de démarrage d'ASA virtuel pour obtenir la liste complète des instances prises en charge.
- Met en œuvre une solution active/de secours sans état qui permet, en cas de défaillance de l'ASA virtuel actif, de déclencher un basculement automatique du système vers l'ASA virtuel de secours.

Restrictions

- Le basculement se fait de l'ordre des secondes plutôt que des millisecondes.
- La détermination du rôle à haute disponibilité et la capacité de participer en tant qu'unité à haute disponibilité dépendent de la connectivité TCP entre les homologues à haute disponibilité et entre une unité à haute disponibilité et l'infrastructure Azure. Il existe plusieurs situations où un ASA virtuel ne pourra pas participer en tant qu'unité à haute disponibilité :
  - L'incapacité à établir une connexion de basculement avec son homologue à haute disponibilité.
  - L'incapacité à récupérer un jeton d'authentification à partir d'Azure.
  - L'incapacité à s'authentifier auprès d'Azure.
- Il n'y a pas de synchronisation de la configuration de l'unité active avec l'unité de sauvegarde. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Limites de la table de routage de basculement

En ce qui concerne les tables de routage pour la haute disponibilité dans le nuage public :

- Vous pouvez configurer un maximum de 16 tables de routage.
- Dans une table de routage, vous pouvez configurer un maximum de 64 routes.

Dans chaque cas, le système vous alerte lorsque vous avez atteint la limite, en vous recommandant de supprimer une table de routage ou une route et de réessayer.

- ASDM n'est pas pris en charge.
- Aucune prise en charge du VPN d'accès à distance IPSec.

Remarque Consultez le guide de démarrage rapide de Cisco Adaptive Security Virtual Appliance (ASAv) pour obtenir des renseignements sur les topologies VPN prises en charge dans le nuage public.

- Les instances de machine virtuelle ASA virtuel doivent se trouver dans le même ensemble de disponibilité. Si vous êtes un utilisateur ASA virtuel actuel dans Azure, vous ne pourrez pas effectuer de mise à niveau vers la haute disponibilité à partir d'un déploiement existant. Vous devez supprimer votre instance et déployer l'offre ASA virtuel 4 NIC à haute disponibilité depuis le Marché Azure.

Licences pour le basculement dans le nuage public

L'ASA virtuel utilise les licences logicielles Cisco Smart. Une licence Smart est requise pour le fonctionnement normal. Chaque ASA virtuel doit recevoir une licence indépendante avec une licence de plateforme ASA virtuel. Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s. Vous pouvez donc effectuer des tests de connectivité préalables. Consultez la page Licences de fonctionnalités de la gamme Cisco ASA pour connaître les exigences de licence précises pour l'ASA virtuel.

Valeurs par défaut pour le basculement dans le nuage public

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

- Basculement sans état uniquement.
- Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.
- Le numéro de port de contrôle de basculement TCP est 44442.
- Le numéro de port de la sonde d'intégrité de l'équilibreur de charges Azure est 44441.
- Le délai d'interrogation de l'unité est de 5 secondes.
- Le délai de rétention de l'unité est de 15 secondes.
- L'ASA virtuel répond aux sondes d'intégrité sur l'interface principale (Management 0/0).
- L'authentification ASA virtuel avec le principal de service Azure est effectuée sur l'interface principale (Management 0/0).

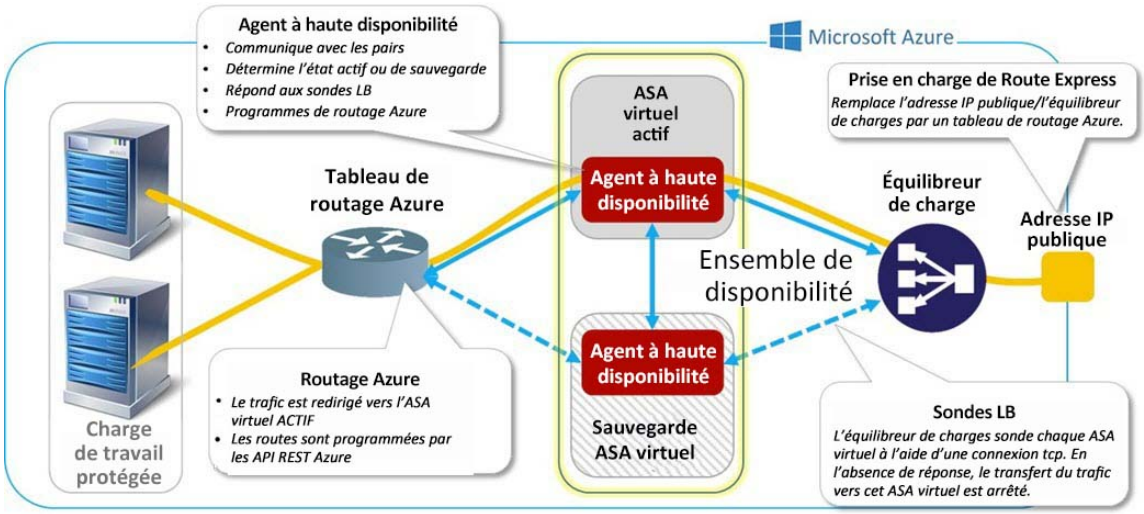
Remarque Consultez Configurer les paramètres de basculement facultatifs, à la page 12 pour connaître les options permettant de modifier le numéro de port de basculement, le numéro de port de la sonde d'intégrité, les délais d'interrogation et l'interface principale.

À propos de l'ASA virtuel à haute disponibilité dans Microsoft Azure

La figure suivante présente une vue d'ensemble d'un déploiement de l'ASA virtuel à haute disponibilité dans Azure. Une charge de travail protégée se trouve derrière deux instances ASA virtuel dans une configuration de basculement actif/de sauvegarde. Un équilibreur de charges Azure sonde les deux unités ASA virtuel à l'aide d'une liaison TCP tridirectionnelle. L'ASA virtuel actif termine l'établissement de la liaison tridirectionnelle indiquant qu'il est intègre, tandis que l'ASA virtuel de sauvegarde ne répond pas intentionnellement. En ne répondant pas à l'équilibreur de charges, l'ASA virtuel de sauvegarde semble non intègre à l'équilibreur de charges, qui à son tour, ne lui envoie pas de trafic.

Lors du basculement, l'ASA virtuel actif arrête de répondre aux sondes de l'équilibreur de charges et l'ASA virtuel de sauvegarde commence à répondre, ce qui fait que toutes les nouvelles connexions sont envoyées à l'ASA virtuel de sauvegarde. L'ASA virtuel de sauvegarde envoie des demandes API à la structure Azure pour modifier la table de routage, redirigeant ainsi le trafic de l'unité active vers l'unité de sauvegarde. À ce stade, l'ASA virtuel de sauvegarde devient l'unité active et l'unité active devient l'unité de sauvegarde ou est hors ligne, selon la raison du basculement.

Illustration 1 : Déploiement de l'ASA virtuel à haute disponibilité dans Azure



Pour pouvoir passer automatiquement des appels d'API pour modifier les tables de routage Azure, les unités ASA virtuel à haute disponibilité doivent disposer de renseignements d'authentification Azure Active Directory. Azure utilise le concept de principal de service qui, en termes simples, est un compte de service. Un principal de service vous permet de provisionner un compte avec seulement les autorisations et la portée nécessaires pour exécuter une tâche dans un ensemble prédéfini de ressources Azure.

Il y a deux étapes pour permettre à votre déploiement ASA virtuel à haute disponibilité de gérer votre abonnement Azure à l'aide d'un principal de service :

1. Créez une application Azure Active Directory et un principal de service; voir À propos du principal de service Azure, à la page 8.
2. Configurez les instances ASA virtuel pour s'authentifier auprès d'Azure à l'aide d'un principal de service; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 14.

Thèmes connexes

Consultez la documentation d'Azure pour en savoir plus sur l'équilibreur de charges.

À propos du principal de service Azure

Lorsque vous avez une application qui a besoin d'accéder aux ressources d'Azure ou de les modifier, telles que des tables de routage, vous devez configurer une application Azure Active Directory (AD) et lui attribuer les autorisations requises. Il est préférable d'exécuter cette approche sous vos propres informations d'authentification, car :

- Vous pouvez attribuer des autorisations à l'identité de l'application qui sont différentes de vos propres autorisations. En règle générale, ces autorisations se limitent à ce que doit faire l'application.
- Vous n'avez pas besoin de modifier les informations d'authentification de l'application si vos responsabilités changent.
- Vous pouvez utiliser un certificat pour automatiser l'authentification lors de l'exécution d'un script sans surveillance.

Lorsque vous enregistrez une application Azure AD dans le portail Azure, deux objets sont créés dans votre détenteur Azure AD : un objet d'application et un objet de principal de service.

- **Application object** (Objet d'application) : une application Azure AD est définie par son seul et unique objet d'application, qui réside dans le détenteur Azure AD où l'application a été enregistrée, appelé détenteur « local » de l'application.
- **Service principal object** (Objet de principal de service) : l'objet de principal de service définit la politique et les autorisations pour l'utilisation d'une application dans un détenteur spécifique, fournissant la base d'un principal de sécurité pour représenter l'application lors de l'exécution.

Azure fournit des instructions sur la création d'une application et d'un principal de service Azure AD dans la *documentation d'Azure Resource Manager*. Consultez les rubriques suivantes pour obtenir des instructions complètes :

- Utiliser le portail pour créer une application et un principal de service Azure Active Directory qui peuvent accéder aux ressources
- Utiliser Azure PowerShell pour créer un principal de service pour accéder à la ressource

Remarque Après avoir configuré le principal de service, procurez-vous le **Directory ID** (ID de répertoire), l'**Application ID** (ID d'application) et la **Secret key** (Clé secrète). Ces éléments sont requis pour configurer les informations d'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 14.

Exigences de configuration pour ASA virtuel haute disponibilité dans Azure

Pour déployer une configuration similaire à celle décrite dans #unique_409 unique_409_Connect_42_fig_cgx_dlh_h1b, vous avez besoin des éléments suivants :

- Renseignements d'authentification Azure (voir À propos du principal de service Azure, à la page 8) :
  - ID de répertoire
  - ID d'application
  - Clé secrète
- Renseignements sur les routes Azure (voir Configurer les tableaux de routage Azure, à la page 15) :
  - ID d'abonnement Azure
  - Groupe de ressources de la table de routage
  - Noms de tables
  - Préfixe d'adresse
  - Adresse du saut suivant
- Configuration de l'ASA (voir Configurer le basculement actif/de secours, à la page 10, Valeurs par défaut pour le basculement dans le nuage public, à la page 6) :
  - Adresses IP actives ou de secours
  - Port de communication de l'agent à haute disponibilité
  - Port de sonde de l'équilibreur de charges
  - Intervalles entre interrogations

Remarque Configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Configurer le basculement actif/de secours

Pour configurer le basculement actif/de secours, configurez les paramètres de basculement de base sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

Avant de commencer

- Déployez votre paire ASA virtuel à haute disponibilité dans un ensemble de disponibilité Azure.
- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

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/de sauvegarde. Ces étapes fournissent la configuration minimum nécessaire pour activer le basculement sur l'unité principale.

Avant de commencer

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

Exemple

L'exemple suivant montre comment configurer les paramètres de basculement pour l'unité principale/active :

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

L'adresse IP homologue que vous saisissez ici doit être l'adresse IP de l'interface de gestion sur l'homologue à haute disponibilité de l'ASA virtuel.

Prochaine étape

Configurez les paramètres supplémentaires au besoin :

- Configurez l'unité de sauvegarde; voir Configurer l'unité secondaire pour le basculement actif/de secours, à la page 11.
- Configurez l'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 14.
- Configurez les renseignements sur les routes Azure; voir Configurer les tableaux de routage Azure, à la page 15.
- Passez en revue les paramètres supplémentaires; voir Configurer les critères de basculement et les autres paramètres, à la page 12.

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

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

Avant de commencer

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

Procédure

Étape 1 Désignez cette unité comme unité de secours :

failover cloud unit secondary

Étape 2 Attribuez l'adresse IP active à la liaison de basculement :

failover cloud peer ip *ip-address* [**port** *port-number*]

Cette adresse IP est utilisée pour établir une connexion de contrôle de basculement TCP avec l'homologue à haute disponibilité. Le port est utilisé lors de la tentative d'ouverture d'une connexion de basculement avec l'homologue à haute disponibilité, qui peut déjà être l'unité active. La configuration du port ici peut être nécessaire si la NAT est en place entre les homologues à haute disponibilité. Dans la plupart des cas, vous n'aurez pas besoin de configurer le port.

L'adresse IP homologue que vous saisissez ici doit être l'adresse IP de l'interface de gestion sur l'homologue à haute disponibilité de l'ASA virtuel.

Exemple

L'exemple suivant montre comment configurer les paramètres de basculement pour l'unité secondaire/de secours :

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

Prochaine étape

Configurez les paramètres supplémentaires au besoin :

- Configurez l'authentification Azure; voir Configurer les informations d'authentification pour un principal de service Azure, à la page 14.
- Configurez les renseignements sur les routes Azure; voir Configurer les tableaux de routage Azure, à la page 15.
- Passez en revue les paramètres supplémentaires; voir Configurer les critères de basculement et les autres paramètres, à la page 12.

Configurer les paramètres de basculement facultatifs

Vous pouvez personnaliser les paramètres de basculement selon vos besoins.

Configurer les critères de basculement et les autres paramètres

Consultez Valeurs par défaut pour le basculement dans le nuage public, à la page 6 pour connaître les paramètres par défaut pour de nombreux paramètres que vous pouvez modifier dans cette section.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.

Procédure

Étape 1 Spécifiez le port TCP à utiliser pour la communication avec l'homologue à haute disponibilité :

failover cloud port control *port-number*

Exemple :

```
ciscoasa(config)# failover cloud port control 4444
```

L'argument *port-number* attribue un numéro au port TCP utilisé pour la communication homologue à homologue.

Cela permet de configurer le port TCP de connexion de basculement sur lequel accepter les connexions lorsque l'unité est active. Il s'agit du port ouvert sur l'ASA virtuel actif auquel l'ASA virtuel de secours se connecte.

Remarque
Nous vous conseillons de conserver la valeur par défaut de 44442, qui est la valeur par défaut pour les deux homologues à haute disponibilité. Si vous modifiez la valeur par défaut d'un homologue à haute disponibilité, il est conseillé d'apporter la même modification à l'autre unité à haute disponibilité.

Étape 2 Modifiez les délais d'interrogation et de rétention de l'unité :

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

Exemple :

```
ciscoasa(config)# failover polltime 10 holdtime 30
```

La plage **polltime** est comprise entre 1 et 15 secondes. Le délai de rétention détermine le délai entre le moment où un paquet Hello est manqué et le moment où l'unité est marquée comme défaillante. La plage **holdtime** est comprise entre 3 et 60 secondes. Vous ne pouvez pas saisir une valeur de délai de rétention inférieure à 3 fois le délai de sondage des unités. 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.

Étape 3 Spécifiez le port TCP utilisé pour les sondes d'intégrité de l'équilibreur de charges Azure :

failover cloud port probe *port-number*

Exemple :

```
ciscoasa(config)# failover cloud port probe 4443
```

Si votre déploiement utilise un équilibreur de charges Azure, l'ASA virtuel actif doit répondre aux sondes TCP de l'équilibreur de charges pour que les connexions entrantes soient dirigées vers l'unité active.

Étape 4 Spécifiez une interface secondaire pour les sondes d'intégrité de l'équilibreur de charges Azure :

failover cloud port probe *port-number* **interface** *if-name*

Exemple :

```
ciscoasa(config)# failover cloud port probe 4443 interface inside
```

Les sondes TCP utilisées dans le nuage à haute disponibilité ont l'adresse IP source de 168.63.129.16. Cette adresse est l'adresse IP publique virtuelle d'Azure. Cette adresse est l'adresse source des paquets DHCP Azure et est l'adresse du serveur de noms DNS dans Azure.

Par défaut, l'ASA virtuel répond aux sondes par lesquelles 168.63.129.16 est accessible, selon les tables de routage de l'ASA. Cela finit par être l'interface principale (Management0/0) en raison de la présence de la route par défaut.

Pour prendre en charge les équilibreurs de charges sur des interfaces autres que Management0/0, vous devez configurer une autre interface pour la sonde de port. Vous devez également configurer deux routes statiques : une pour l'interface principale et une pour l'interface configurée pour les sondes de l'équilibreur de charges.

Étape 5 Ajoutez des routes statiques pour l'interface principale et l'interface configurée pour les sondes de l'équilibreur de charges :

route *if-name dest_ip mask gateway_ip* **[distance]**

Exemple :

```
ciscoasa(config)# route outside 168.63.129.16 255.255.255.255 10.22.0.1 1
ciscoasa(config)# route inside 168.63.129.16 255.255.255.255 10.22.1.1 2
```

L'argument *distance* correspond à la distance administrative de la route. La valeur par défaut est **1** si vous ne spécifiez pas de valeur. La distance administrative est un paramètre utilisé pour comparer les routes entre différents protocoles de routage. Lorsque plusieurs routes existent vers la même destination (168.63.129.16), la distance administrative de la route détermine la priorité.

La route statique de l'interface principale (extérieure) avec la distance administrative de 1 établit l'interface principale comme interface préférée pour les paquets destinés à 168.63.129.16, mais permet également à l'interface configurée pour les sondes de l'équilibreur de charges d'envoyer des paquets à 168.63.129.16.

Remarque
Le mécanisme de réponse aux sondes consiste à créer un connecteur TCP sur une interface. Le nuage à haute disponibilité utilise la recherche de routes pour 168.63.129.16 pour décider sur quelle interface créer le

connecteur. Cela finit par être l'interface principale en raison de la présence de la route par défaut. Sans la route statique de l'interface configurée pour les sondes, l'ASA ne répondrait pas aux paquets TCP envoyés par l'équilibreur de charges.

Configurer les informations d'authentification pour un principal de service Azure

Vous pouvez permettre à vos homologues à haute disponibilité ASA virtuel d'accéder aux ressources d'Azure, telles que des tables de routage, ou de modifier ces ressources à l'aide d'un principal de service Azure. Vous devez configurer une application Azure Active Directory (AD) et lui attribuer les autorisations requises. Les commandes suivantes permettent à l'ASA virtuel de s'authentifier auprès d'Azure à l'aide d'un principal de service. Consultez le chapitre Azure du guide de démarrage rapide d'ASA virtuel pour en savoir plus sur le principal de service Azure.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.

Procédure

Étape 1 Configurez l'ID d'abonnement Azure pour le principal de service Azure :

failover cloud subscription-id *subscription-id*

Exemple :

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

L'ID d'abonnement Azure est nécessaire pour modifier les tables de routage Azure, par exemple, lorsque l'utilisateur de haute disponibilité en nuage souhaite diriger des routes internes vers l'unité active.

Étape 2 Configurez les informations d'authentification du principal de service Azure :

failover cloud authentication {**application-id** | **directory-id** | **key**}

Pour modifier les tables de routage Azure lors d'un basculement, vous devez obtenir une *clé d'accès* auprès de l'infrastructure Azure avant de pouvoir accéder aux tables de routage. Vous obtenez la *clé d'accès* en utilisant un ID d'application, un ID de répertoire et une clé secrète pour le principal de service Azure qui contrôle la paire à haute accessibilité.

Étape 3 Configurez l'ID d'application du principal de service Azure :

failover cloud authentication application-id *appl-id*

Exemple :

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

Vous avez besoin de cet ID d'application lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

Étape 4 Configurez l'ID de répertoire du principal de service Azure :

failover cloud authentication directory-id *dir-id*

Exemple :

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

Vous avez besoin de cet ID de répertoire lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure.

Étape 5 Configurez l'ID de clé secrète du principal de service Azure :

failover cloud authentication key *secret-key* [**encrypt**]

Exemple :

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

Vous avez besoin de cette clé secrète lorsque vous demandez une clé d'accès auprès de l'infrastructure Azure. Si le mot clé **encrypt** est présent, la clé secrète est chiffrée dans la commande **running-config**.

Configurer les tableaux de routage Azure

La configuration de la table de routage comprend des renseignements sur les routes définies par l'utilisateur Azure qui doivent être mises à jour lorsque l'ASA virtuel assume le rôle actif. Lors du basculement, vous souhaitez diriger des routes internes vers l'unité active, qui utilise les renseignements de la table de routage configurée pour diriger automatiquement les routes vers elle-même.

Remarque Vous devez configurer tous les renseignements de la table de routage Azure sur les unités actives et de sauvegarde.

Avant de commencer

- Configurez ces paramètres dans l'espace d'exécution du système en mode de contexte unique.
- Configurez ces paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire.
- Ayez les renseignements sur votre environnement Azure à disposition, y compris votre ID d'abonnement Azure et vos informations d'authentification Azure pour le principal du service.

Procédure

Étape 1 Configurez une table de routage Azure qui nécessite une mise à jour lors d'un basculement :

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

Exemple :

```
ciscoasa(config)# failover cloud route-table inside-rt
```

(Facultatif) Pour mettre à jour des routes définies par l'utilisateur dans plusieurs abonnement Azure, incluez le paramètre **subscription-id**.

Exemple :

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

Le paramètre **subscription-id** au niveau de la commande **route-table** remplace l'ID d'abonnement Azure spécifié au niveau global. Si vous entrez la commande **route-table** sans préciser d'ID d'abonnement Azure, le paramètre global **subscription-id** est utilisé. Consultez Configurer les informations d'authentification pour un principal de service Azure, à la page 14 pour en savoir pl sur l'ID d'abonnement Azure.

Remarque
Lorsque vous saisissez la commande **route-table**, l'ASA virtuel passe en mode **cfg-fover-cloud-rt** .

Étape 2 Configurez un groupe de ressources Azure pour une table de routage :

rg *resource-group*

Exemple :

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Vous avez besoin d'un groupe de ressources pour les demandes de mise à jour de la table de routage dans Azure.

Étape 3 Configurez une route qui nécessite une mise à jour lors d'un basculement :

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

Exemple :

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

Le préfixe d'adresse est configuré comme un préfixe d'adresse IP, une barre oblique (« / ») et un masque réseau numérique. Par exemple, *192.120.0.0/16*.

Exemple

Exemple de configuration complète :

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

Activer le basculement actif/de secours

Vous activez le basculement actif/de secours après avoir configuré les paramètres sur les unités principale et secondaire. Il n'y a pas de synchronisation de la configuration de l'unité principale avec l'unité secondaire. Chaque unité doit être configurée individuellement avec des configurations similaires pour gérer le trafic de basculement.

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

Suivez les étapes de cette section pour activer l'unité principale dans une configuration de basculement actif/de secours.

Avant de commencer

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

Procédure

Étape 1 Activez le basculement :

ciscoasa(config)# failover

Étape 2 Enregistrez la configuration système dans la mémoire flash :

ciscoasa(config)# write memory

Exemple

L'exemple suivant montre une configuration complète pour l'unité principale :

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44
```

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

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

Prochaine étape

Activez l'unité secondaire.

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

Suivez les étapes de cette section pour activer l'unité secondaire dans une configuration de basculement actif/de secours.

Avant de commencer

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

Procédure

Étape 1 Activez le basculement :

ciscoasa(config)# **failover**

Étape 2 Enregistrez la configuration système dans la mémoire flash :

ciscoasa(config)# **write memory**

Exemple

L'exemple suivant montre une configuration complète pour l'unité secondaire :

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

```
ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

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

Gérer le basculement dans le nuage public

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

Forcer le basculement

Pour forcer l'unité en veille à devenir active, exécutez la commande suivante.

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Étape 1 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *en veille* :

failover active

Exemple :

```
ciscoasa# failover active
```

L'unité en veille devient l'unité active.

Étape 2 Forcez un basculement lorsque vous avez saisi la commande sur l'unité *active* :

no failover active

Exemple :

```
ciscoasa# no failover active
```

L'unité active devient l'unité en veille.

Mettre à jour les routes

Si l'état des routes dans Azure est incohérent avec l'ASA virtuel dans le rôle *actif*, vous pouvez forcer les mises à jour de routes sur l'ASA virtuel à l'aide de la commande EXEC suivante :

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Mettez à jour les routes sur l'unité *active* :

failover cloud update routes

Exemple :

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

Cette commande est uniquement valide sur l'ASA virtuel dans le rôle *actif*. Si l'authentification échoue, la sortie de la commande sera `Route changes failed`.

Valider l'authentification Azure

Pour un déploiement réussi de l'ASA virtuel à haute disponibilité dans Azure, la configuration du principal de service doit être complète et précise. Sans l'autorisation Azure appropriée, les unités ASA virtuel ne pourront pas accéder aux ressources pour gérer le basculement et effectuer des mises à jour de routage. Vous pouvez tester votre configuration de basculement pour détecter les erreurs liées aux éléments suivants de votre principal de service Azure :

- ID de répertoire
- ID d'application
- Clé d'authentification

Avant de commencer

Utilisez cette commande dans l'espace d'exécution du système en mode de contexte unique.

Procédure

Testez les éléments d'authentification Azure dans votre configuration ASA virtuel à haute disponibilité :

test failover cloud authentication

Exemple :

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

Si l'authentification échoue, la sortie de la commande sera `Authentication Failed` (Échec d'authentification).

Si l'ID de répertoire ou l'ID d'application n'est pas configuré correctement, Azure ne reconnaîtra pas la ressource mentionnée dans la demande REST pour obtenir un jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

Si l'ID de répertoire ou l'ID d'application sont corrects, mais que la clé d'authentification n'est pas configurée correctement, Azure n'accordera pas l'autorisation de générer le jeton d'authentification. L'historique des événements pour cette entrée de condition indiquera :

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

Superviser le basculement dans le nuage public

Cette section explique comment superviser l'état du basculement.

État de basculement

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

- **show failover**

  Affiche des renseignements sur l'état de basculement de l'unité. Les valeurs des éléments de configuration qui n'ont pas été configurés afficheront *non configuré*.

  Les renseignements de mise à jour du routage sont présentés uniquement pour l'unité active.

- **show failover history**

  Affiche l'historique des événements de basculement avec un horodatage, un niveau de gravité, un type d'événement et un texte d'événement.

Messages de basculement

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 messages de journal système sont compris entre 1045xx et 1055xx.

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

Voici des exemples de journaux système générés lors d'un basculement :

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
```

```
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

Chaque journal système lié à un déploiement dans le nuage public est précédé du rôle de l'unité : (Principal) ou (Secondaire).

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.

Historique de basculement dans le nuage public

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Basculement actif/de sauvegarde sur Microsoft Azure	9.8(200)	Cette fonctionnalité a été introduite.

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.