OSPF

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF).

À propos d'OSPF

OSPF est un protocole de routage de passerelle intérieure qui utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin. OSPF propage des publicités d'état de liens plutôt que des mises à jour de la table de routage. Comme seuls les LSA sont échangés au lieu des tableaux de routage complets, les réseaux OSPF convergent plus rapidement que les réseaux IPS.

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP sont les suivants :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.
- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. ASA calcule le coût d'une interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'ASA peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

ASA prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de ASA en tant que routeur désigné ou routeur de secours désigné L'ASA peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par les attaquants pour détourner des informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage du LSA ABR de type 3 vous permet d'avoir des zones privée et publique distinctes, l'ASA agissant comme un ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.

Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'ASA comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais OSPF n'est exécuté que dans les zones publiques, les routages vers les réseaux publics peuvent être redistribués à l'intérieur du réseau privé, soit par défaut, soit comme LSA externes de

type AS externes. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par ASA. De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface ASA.

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'ASA.

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF des paquets Hello rapides offre un moyen de configurer l'envoi de paquets Hello à des intervalles inférieurs à une seconde. Une telle configuration accélérerait la convergence dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la prise en charge d'OSPF pour les paquets Fast Hello

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

À propos de la prise en charge OSPF pour les paquets Hello rapides

Les concepts clés liés à la prise en charge OSPF pour les paquets Fast Hello et aux avantages des paquets OSPF Fast Hello sont décrits ci-dessous :

Intervalle Hello et intervalle mort OSPF

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée. Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Fast Hello OSPF

Les paquets Hello OSPF rapides sont des paquets Hello envoyés à des intervalles de moins d'une seconde. Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 3.

Les paquets OSPF fast Hello sont obtenus à l'aide de la commande ospf dead-interval. L'intervalle mort est défini à 1 seconde et la valeur Hello-multiplier est définie sur le nombre de paquets Hello que vous souhaitez envoyer pendant cette 1 seconde, fournissant ainsi des paquets Hello inférieurs à la seconde ou « rapides ».

Lorsque des paquets Hello rapides sont configurés sur l'interface, l'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0. L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Avantages des paquets Fast Hello OSPF

L'avantage de la fonctionnalité OSPF Fast Hello Packets est que votre réseau OSPF connaîtra un temps de convergence plus rapide que sans les paquets rapides Hello. Cette fonctionnalité vous permet de détecter les voisins perdus en moins d'une seconde. Elle est particulièrement utile dans les segments de réseau local, où la perte de voisin peut ne pas être détectée par la couche physique et la couche de liaison de données de l'Open System Interconnection (OSI).

Différences d'implémentation entre OSPFv2 et OSPFv3

OSPFv3 n'est pas rétrocompatible avec OSPFv2. Pour utiliser OSPF en vue d'acheminer le trafic IPv4 et IPv6, vous devez exécuter simultanément OSPFv2 et OSPFv3. Ils coexistent, mais n'interagissent pas entre eux.

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d'adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l'adresse locale de lien IPv6 pour la découverte de voisin et d'autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l'authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Directives pour OSPF

Directives relatives au mode contextuel

OSPFv2 prend en charge les modes à contexte unique et multiple.

- Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus OSPFv2 sous le processus OSPFv2 pour faire apparaître le voisinage OSPFv2 sur une interface partagée.
- OSPFv2 inter-contexte sur des interfaces distinctes est pris en charge.

(Pour la topologie point à point) En mode de contexte multiple, vous pouvez configurer des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Pour une formation de contiguïté OSPF réussie, lorsque vous supprimez et reconfigurez OSPF sur une interface partagée, exécutez les commandes dans l'ordre suivant :

- Supprimez la configuration OSPF en utilisant `no router <ospf name>`, puis supprimez la configuration OSPF point à point de non-diffusion sur l'interface en utilisant `no ospf network point-to-point non-broadcast`.
- Lorsque vous reconfigurez OSPF sur l'interface partagée, configurez le routeur OSPF en utilisant `router <ospf name>`, puis configurez l'interface avec `ospf network point-to-point non-broadcast`.

OSPFv3 prend en charge le mode unique uniquement.

Directives d'authentification par chaîne de clé

OSPFv2 prend en charge l'authentification par chaîne de clés en mode unique et multiple, en modes physique et virtuel. Cependant, en mode multiple, vous pouvez configurer la chaîne de clés uniquement en mode contextuel.

- Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. L'authentification de zone OSPF avec chaîne de clé n'est pas prise en charge.
- L'authentification MD5 existante sans plage temporelle dans OSPFv2 est toujours prise en charge avec les nouvelles clés alternées.
- Bien que la plateforme prenne en charge les algorithmes cryptographiques SHA1 et MD5, seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Directives sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives Failover (basculement)

OSPFv2 et OSPFv3 prennent en charge le Failover (basculement) sans état.

Directives IPv6

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'ASA installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.
- Les paquets OSPFv3 peuvent être filtrés à l'aide des listes de contrôle d'accès IPv6 dans la commande **capture**.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Directives de mise en grappe

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, le comportement suivant se produit :
  - En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle.
  - En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et directives OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

Désactivez la capacité d'opacité sur l'ASA pour vous assurer que la relation de voisin reste stable :

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Directives de redistribution de routage

- La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge. Toutefois, la redistribution des cartes de routage avec la liste de préfixes IPv6 sur OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.

- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage).

  Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.
- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée.

  Actuellement, vous ne pouvez pas afficher la table de routage effective ou la table de routage du système.
- OSPFv3 abandonne la mise à jour LS si la taille des paquets dépasse 8190. Par conséquent, le voisinage est interrompu. Ainsi, configurez le commutateur avec la commande « ospfv3 mtu-ignore » pour éviter la fin du voisinage.

Configurer le protocole OSPFv2

Cette section décrit comment activer un processus OSPFv2 sur l'ASA.

Après avoir activé le protocole OSPFv2, vous devez définir une carte de routage. Pour en savoir plus, consultez Définir une carte de routage. Ensuite, vous générez une route par défaut. Pour en savoir plus, consultez Configurer une route statique.

Après avoir défini une carte de routage pour le processus OSPFv2, vous pouvez la personnaliser selon vos besoins particuliers. Pour savoir comment personnaliser le processus OSPFv2 sur l'ASA, consultez Personnaliser le protocole OSPFv2, à la page 13.

Pour activer le protocole OSPFv2, vous devez créer un processus de routage OSPFv2, spécifier la plage d'adresses IP associées au processus de routage, puis attribuer les ID de zone associés à cette plage d'adresses IP.

Vous pouvez activer jusqu'à deux instances de processus OSPFv2. Chaque processus OSPFv2 a ses propres zones et réseaux associés.

Pour activer le processus OSPFv2, procédez comme suit.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

S'il n'y a qu'un seul processus OSPF activé sur l'ASA, ce processus est sélectionné par défaut. Vous ne pouvez pas modifier l'ID de processus OSPF lors de la modification d'une zone existante.

Étape 2 Définissez les adresses IP sur lesquelles l'OSPF s'exécute et l'ID de zone pour cette interface :

network *ip_address mask* **area** *area_id*

Exemple :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

Lors de l'ajout d'une nouvelle zone, saisissez l'ID de zone. Vous pouvez spécifier l'ID de zone sous la forme d'un nombre décimal ou d'une adresse IP. Les valeurs décimales valides vont de 0 à 4294967295. Vous ne pouvez pas modifier l'ID de zone lors de la modification d'une zone existante.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 17.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Configurez une chaîne de clés avec un nom :

key chain*key-chain-name*

Exemple :

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

Vous pouvez maintenant définir les paramètres associés à la chaîne de clés.

Étape 2 Configurez l'identifiant de la chaîne de clés :

key*key-id*

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Exemple :

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

Étape 3 Configurez la clé ou le mot de passe de la chaîne de clés :

key-string [**0** | **8**] *key-string-text*

- Utilisez **0** pour indiquer qu'un mot de passe non chiffré suit, comme le montre l'exemple.
- Utilisez **8** pour indiquer qu'un mot de passe chiffré suit.
- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Exemple :

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

Étape 4 Configurez l'algorithme cryptographique pour la chaîne de clés :

cryptographic-algorithm*md5*

Vous devez fournir l'algorithme d'authentification cryptographique. Bien que la plateforme prenne en charge SHA1 et MD5, seul MD5 est pris en charge pour la gestion de la chaîne de clés.

Exemple :

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

Étape 5 (Facultatif) Configurez les paramètres de durée de vie de la chaîne de clés :

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée ou à l'heure absolue à laquelle la durée de vie de l'acceptation/envoi prend fin, ou être infinie.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Exemple :

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

Vous pouvez utiliser la commande **show key chain** pour afficher la configuration de la chaîne de clés de démarrage sur le périphérique; **show run key chain** pour afficher la configuration de la chaîne de clés qui est actuellement en cours d'exécution sur le périphérique.

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#
```

```
ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
```

```
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface.

- Configurer les paramètres d'interface OSPFv2, à la page 17

Configurer l'ID de routeur OSPFv2

L'ID de routeur OSPF est utilisé pour identifier un appareil spécifique dans une base de données OSPF. Deux routeurs d'un système OSPF ne peuvent pas avoir le même ID de routeur.

Si un ID de routeur n'est pas configuré manuellement dans le processus de routage OSPF, le routeur configurera automatiquement un ID de routeur déterminé à partir de l'adresse IP la plus élevée d'une interface active. Lors de la configuration d'un ID de routeur, les voisins ne seront pas mis à jour automatiquement jusqu'à ce que le routeur ait échoué ou que le processus OSPF ait été effacé et que la relation de voisin ait été rétablie.

Configurer manuellement l'ID de routeur OSPF

Cette section décrit comment configurer manuellement l'ID de routeur dans le processus OSPFv2 sur l'ASA.

Procédure

Étape 1 Pour utiliser un ID de routeur fixe, utilisez la commande **router-id**.

router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# router-id 193.168.3.3
```

Étape 2 Pour revenir au comportement précédent de l'ID de routeur OSPF, utilisez la commande **no router-id**.

no router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

Comportement de l'ID de routeur lors de la migration

Lors de la migration de la configuration OSPF d'un ASA, par exemple ASA 1 vers un autre ASA, par exemple l'ASA 2, le comportement suivant est observé en matière de sélection de l'ID du routeur :

1. L'ASA 2 n'utilise aucune adresse IP pour l'ID de routeur OSPF lorsque toutes les interfaces sont en mode d'arrêt. Les possibilités de configuration de l'ID de routeur lorsque toutes les interfaces sont à l'état « arrêt admin » ou en mode d'arrêt sont les suivantes :
   - Si l'ASA 2 n'a pas encore d'ID de routeur configuré, vous verrez ce message :

     `%OSPF: Router process 1 is not running, please configure a router-id` (% OSPF : le processus de routeur 1 n'est pas en cours d'exécution, veuillez configurer un identifiant de routeur)

     Après le déploiement de la première interface, l'ASA 2 utilisera l'adresse IP de cette interface comme ID de routeur.
   - Si l'ASA 2 a déjà configuré l'ID de routeur et que toutes les interfaces étaient à l'état « arrêt admin » lorsque la commande « no router-id » a été exécutée, l'ASA 2 utilisera l'ancien ID de routeur. L'ASA 2 utilise l'ancien ID de routeur, même si les adresses IP de l'interface créée sont modifiées, jusqu'à ce que la commande « clear ospf process » soit émise.
2. L'ASA 2 utilise un nouvel ID de routeur, alors que l'ASA 2 avait déjà configuré l'ID de routeur et qu'au moins une des interfaces n'était pas à l'état « arrêt admin » ou en mode d'arrêt lorsque la commande « no router-id » a été émise. L'ASA 2 utilisera le nouvel ID de routeur de l'adresse IP des interfaces même lorsque les interfaces sont à l'état « arrêt/arrêt ».

Configurer les paquets Hello rapides OSPF

Cette section explique comment configurer les paquets OSPF Hello rapides.

Procédure

Étape 1 Configurez une interface :

interface *port-channel number*

Exemple :

```
ciscoasa(config)# interface port-channel 10
```

L'argument *number* indique le numéro de l'interface de canal de port.

Étape 2 Définissez l'intervalle pendant lequel au moins un paquet Hello doit être reçu, sinon le voisin est considéré comme hors service :

ospf dead-interval minimal hello-multiplier *no.of times*

Exemple :

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
```

```
ciscoasa
```

L'argument no. of times indique le nombre de paquets Hello à envoyer chaque seconde. Les valeurs valides sont comprises entre 3 et 20.

Dans cet exemple, la prise en charge OSPF pour les paquets Hello rapides est activée en spécifiant le mot clé minimal et le mot clé hello-multiplier ainsi que sa valeur. Comme le multiplicateur est défini sur 5, cinq paquets Hello seront envoyés chaque seconde.

Personnaliser le protocole OSPFv2

Cette section explique comment personnaliser les processus OSPFv2.

Redistribuer les routes dans OSPFv2

L'ASA peut contrôler la redistribution des routes entre les processus de routage OSPFv2.

Remarque Si vous souhaitez redistribuer une route en définissant quelles routes du protocole de routage spécifié peuvent être redistribuées dans le processus de routage cible, vous devez d'abord générer une route par défaut. Consultez Configurer une route statique, puis définissez une carte de routage en fonction de Définir une carte de routage.

Pour redistribuer les routes statiques, connectées, RIP ou OSPFv2 dans un processus OSPFv2, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Redistribuez les routes connectées dans le processus de routage OSPF :

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

Étape 3 Redistribuez les routes statiques dans le processus de routage OSPF :

redistribute static [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute static subnets
```

Cette commande transmettra toutes les routes statiques à l'OSPF. Pour redistribuer les routes statiques sélectives, assurez-vous de créer une liste d'accès avec la route statique, puis de l'inclure dans une carte de routage :

Exemple :

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

Après avoir créé la carte de routage, incluez-la dans la commande de redistribution comme suit :

Exemple :

```
ciscoasa(config)#router ospf 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

Étape 4 Redistribuez les routes d'un processus de routage OSPF dans un autre processus de routage OSPF :

redistribute ospf pid [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Vous pouvez utiliser les options **match** dans cette commande pour faire correspondre et définir les propriétés du routage, ou vous pouvez utiliser une carte de routage. L'option **subnets** n'a pas d'équivalents dans la commande **route-map**. Si vous utilisez à la fois une carte de routage et les options **match** dans la commande **redistribute**, elles doivent correspondre.

L'exemple montre la redistribution des routes du processus OSPF 1 vers le processus OSPF 2 en faisant correspondre les routes avec une mesure égale à 1. L'ASA redistribue ces routes en tant que LSA externes avec une mesure de 5 et un type de mesure de type 1.

Étape 5 Redistribuez les routes d'un processus de routage RIP dans le processus de routage OSPF :

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Étape 6 Redistribuez les routes d'un processus de routage EIGRP dans le processus de routage OSPF :

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

Exemple :

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer l'ASA pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF.

Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Ajouter une adresse sommaire de route

Pour configurer l'annonce du logiciel sur une route récapitulative pour toutes les routes redistribuées incluses pour une adresse réseau et un masque, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez l'adresse sommaire :

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

Exemple :

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

Dans cet exemple, l'adresse sommaire 10.1.0.0 comprend les adresses 10.1.1.0, 10.1.2.0, 10.1.3.0, etc. Seule l'adresse 10.1.0.0 est annoncée dans une annonce d'état de liaison externe.

Configurer la synthèse des routes entre les zones OSPFv2

La synthèse du routage est le regroupement d'adresses annoncées. Cette fonctionnalité permet d'annoncer une seule route récapitulative à d'autres zones par un routeur de délimitation de zone. Dans OSPF, un routeur de délimitation de zone annonce les réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer le routeur de délimitation de zone pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée.

Pour définir une plage d'adresses pour la synthèse du routage, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF et entrez en mode de configuration du routeur pour ce processus OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il peut s'agir de n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez la plage d'adresses :

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

Exemple :

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

Dans cet exemple, la plage d'adresses est définie entre les zones OSPF.

Configurer les paramètres d'interface OSPFv2

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : **ospf hello-interval**, **ospf dead-interval** et **ospf authentication-key**. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Pour configurer les paramètres d'interface OSPFv2, procédez comme suit :

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf*process-id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez les adresses IP sur lesquelles l'OSPF s'exécute et l'ID de zone pour cette interface :

network*ip-address mask***area***area-id*

Exemple :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

Étape 3 Entrez le mode de configuration d'interface :

interface*interface-name*

Exemple :

```
ciscoasa(config)# interface my_interface
```

Étape 4 Spécifiez le type d'authentification pour une interface :

ospf authentication [**key-chain** *key-chain-name* | **message-digest** | **null**]

Fournissez le nom de la chaîne de clés configurée. Pour en savoir plus sur la configuration de la chaîne de clés, consultez Configurer une chaîne de clés pour l'authentification, à la page 8

Exemple :

```
ciscoasa(config-interface)# ospf authentication message-digest
```

Étape 5 Attribuez un mot de passe à utiliser par les routeurs OSPF voisins sur un segment de réseau qui utilise l'authentification par mot de passe simple OSPF :

ospf authentication-key*key*

Exemple :

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

L'argument *key* peut être n'importe quelle chaîne continue de caractères d'une longueur maximale de 8 octets.

Le mot de passe créé par cette commande est utilisé comme clé qui est insérée directement dans l'en-tête OSPF lorsque le logiciel ASA génère les paquets de protocole de routage. Un mot de passe distinct peut être attribué à chaque réseau par interface. Tous les routeurs voisins sur le même réseau doivent avoir le même mot de passe pour pouvoir échanger des renseignements OSPF.

Étape 6 Spécifiez explicitement le coût d'envoi d'un paquet sur une interface OSPF :

ospf cost*cost*

Exemple :

```
ciscoasa(config-interface)# ospf cost 20
```

Le *coût* est un entier compris entre 1 et 65 535.

Dans cet exemple, le coût est défini sur 20.

Étape 7 Définissez le nombre de secondes qu'un appareil doit attendre avant de déclarer un routeur OSPF voisin parce qu'il n'a pas reçu de paquet Hello :

ospf dead-interval*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf dead-interval 40
```

La valeur doit être la même pour tous les nœuds du réseau.

Étape 8 Spécifiez la durée entre les paquets Hello que l'ASA envoie sur une interface OSPF :

ospf hello-interval*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf hello-interval 10
```

La valeur doit être la même pour tous les nœuds du réseau.

Étape 9 Activez l'authentification MD5 OSPF :

ospf message-digest-key*key-id***md5***key*

Exemple :

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

Les valeurs d'argument suivantes peuvent être définies :

key-id : un identifiant compris entre 1 et 255.

key : un mot de passe alphanumérique de 16 octets maximum.

Généralement, une clé par interface est utilisée pour générer des informations d'authentification lors de l'envoi de paquets et pour authentifier les paquets entrants. Le même identifiant de clé sur le routeur voisin doit avoir la même valeur de clé.

Nous vous conseillons de ne pas conserver plus d'une clé par interface. Chaque fois que vous ajoutez une nouvelle clé, vous devez supprimer l'ancienne clé pour empêcher le système local de continuer à communiquer avec un système malveillant qui connaît l'ancienne clé. La suppression de l'ancienne clé réduit également le surdébit lors du renouvellement.

Étape 10 Définissez la priorité pour aider à déterminer le routeur désigné OSPF pour un réseau :

ospf priority *number-value*

Exemple :

```
ciscoasa(config-interface)# ospf priority 20
```

L'argument *number_value* varie de 0 à 255.

En mode de contexte multiple, pour les interfaces partagées, spécifiez 0 pour vous assurer que le périphérique ne devienne pas le routeur désigné. Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles sur les interfaces partagées.

Étape 11 Spécifiez le nombre de secondes entre les retransmissions de LSA pour les contiguïtés appartenant à une interface OSPF :

ospf retransmit-interval*number-value*

Exemple :

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

La valeur pour *seconds* doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. La plage est comprise entre 1 et 8 192 secondes. La valeur par défaut est de 5 secondes.

Étape 12 Définissez le nombre estimé de secondes nécessaires pour envoyer un paquet de mise à jour d'état de liaison sur une interface OSPF :

ospf transmit-delay*seconds*

Exemple :

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

La valeur *seconds* varie de 1 à 8 192 secondes. La valeur par défaut est de 1 seconde.

Étape 13 Définissez le nombre de paquets Hello envoyés pendant 1 seconde :

ospf dead-interval minimal hello-interval multiplier*nombre entier*

Exemple :

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

Les valeurs valides sont des entiers compris entre 3 et 20.

Étape 14 Spécifiez l'interface comme réseau point à point sans diffusion :

ospf network point-to-point non-broadcast

Exemple :

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

Lorsque vous désignez une interface comme point à point et sans diffusion, vous devez définir manuellement le voisin OSPF; la découverte dynamique de voisin n'est pas possible. Consultez Définir les voisins OSPFv2 statiques, à la page 24 pour de plus amples renseignements. En outre, vous ne pouvez définir qu'un seul voisin OSPF sur cette interface.

Configurer les paramètres de zone OSPFv2

Vous pouvez configurer plusieurs paramètres de zone OSPF. Ces paramètres de zone (indiqués dans la liste des tâches suivante) comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon. Pour réduire davantage le nombre de LSA envoyés dans une zone tampon, vous pouvez utiliser le mot clé **no-summary** de la commande **area stub** sur l'ABR pour l'empêcher d'envoyer une annonce de liaison récapitulative (LSA type 3) dans la zone tampon.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez l'authentification pour une zone OSPF :

area *area-id* authentication

Exemple :

```
ciscoasa(config-rtr)# area 0 authentication
```

Étape 3 Activez l'authentification MD5 pour une zone OSPF :

area *area-id* authentication message-digest

Exemple :

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

Configurer les règles de filtre OSPFv2

Utilisez la procédure suivante pour filtrer les routes ou les réseaux reçus ou transmis dans les mises à jour OSPF.

Procédure

Étape 1 Activez un processus de routage OSPF et passez en mode de configuration du routeur :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

Étape 2 Filtrez les routes ou les réseaux reçus dans les mises à jour OSPF entrantes ou annoncés dans les mises à jour OSPF sortantes :

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

L'argument *acl-number* spécifie le numéro de la liste d'accès IP. La liste d'accès définit les réseaux à recevoir et ceux à supprimer dans les mises à jour de routage.

Pour appliquer le filtre aux mises à jour entrantes, spécifiez **in**. Vous pouvez éventuellement définir une interface pour limiter le filtre aux mises à jour reçues sur cette interface.

Pour appliquer le filtre aux mises à jour sortantes, spécifiez **out**. Vous pouvez éventuellement spécifier un protocole (**bgp**, **eigrp**, **ospf** ou **rip**) avec un numéro de processus (à l'exception du protocole RIP) à appliquer

à la liste de distribution. Vous pouvez également filtrer selon que les homologues et les réseaux ont été appris par les routes **connected** ou **static**.

Exemple :

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

Configurer une NSSA OSPFv2

La mise en œuvre du protocole OSPFv2 d'une zone NSSA est similaire à une zone tampon OSPFv2. NSSA n'inonde pas les LSA externes de type 5 du cœur vers la zone, mais il peut importer des routes externes du système autonome de manière limitée dans la zone.

NSSA importe des routes externes du système autonome de type 7 dans une zone NSSA par redistribution. Ces LSA de type 7 sont traduites en LSA de type 5 par les ABR de NSSA, qui sont inondés dans tout le domaine de routage. La synthèse et le filtrage sont pris en charge pendant la traduction.

Vous pouvez simplifier l'administration si vous êtes un FAI ou un administrateur réseau qui doit connecter un site central à l'aide du protocole OSPFv2 à un site distant qui utilise un protocole de routage différent avec NSSA.

Avant la mise en œuvre de NSSA, la connexion entre le routeur de frontière du site d'entreprise et le routeur distant ne pouvait pas être exécutée en tant que zone tampon OSPFv2, car les routes du site distant ne pourraient pas être redistribuées dans la zone tampon, et deux protocoles de routage devaient être maintenus. Un protocole simple comme RIP était généralement exécuté et gérait la redistribution. Avec NSSA, vous pouvez étendre le protocole OSPFv2 pour couvrir la connexion à distance en définissant la zone entre le routeur d'entreprise et le routeur distant en tant que NSSA.

Veuillez consulter les lignes directrices suivantes avant d'utiliser cette fonctionnalité :

- Vous pouvez définir une route par défaut de type 7 qui peut être utilisée pour atteindre des destinations externes. Une fois configuré, le routeur génère une valeur par défaut de type 7 dans le NSSA ou le routeur de limite de zone NSSA.
- Tous les routeurs d'une même zone doivent convenir que la zone est NSSA; sinon, les routeurs ne peuvent pas communiquer entre eux.

Procédure

Étape 1 Créez un processus de routage OSPF :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il peut s'agir de n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez une zone NSSA :

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

Exemple :

```
ciscoasa(config-rtr)# area 0 nssa
```

Étape 3 Définissez l'adresse sommaire et contribuez à réduire la taille de la table de routage :

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

Exemple :

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

L'utilisation de cette commande pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse.

Dans cet exemple, l'adresse sommaire 10.1.0.0 comprend les adresses 10.1.1.0, 10.1.2.0, 10.1.3.0, etc. Seule l'adresse 10.1.0.0 est annoncée dans une annonce d'état de liaison externe.

Remarque
OSPF ne prend pas en charge l'adresse récapitulative 0.0.0.0 0.0.0.0.

Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3)

Vous pouvez attribuer une plage d'adresses IPv4 pour le regroupement de grappes d'ID de routeur si vous utilisez la mise en grappe d'interfaces individuelles.

Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans la mise en grappe d'interfaces individuelles pour les protocoles OSPFv2 et OSPFv3, saisissez la commande suivante :

Procédure

Spécifiez l'ensemble de grappes d'ID de routeur pour la mise en grappe d'interfaces individuelles :

router-id cluster-pool hostname | A.B.C.D ip_pool

Exemple :

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

Le mot clé **cluster-pool** permet la configuration d'un ensemble d'adresses IP lorsque la mise en grappe d'interfaces individuelles est configurée. Le mot clé **hostname** | **A.B.C.D.** spécifie l'ID du routeur OSPF pour ce processus OSPF. L'argument *ip_pool* spécifie le nom de l'ensemble d'adresses IP.

Remarque
Si vous utilisez la mise en grappe, vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur. Si vous ne configurez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

Définir les voisins OSPFv2 statiques

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv2. Consultez Configurer une route statique pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez le voisinage OSPFv2 :

neighbor *addr* [**interface** if_name]

Exemple :

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

L'argument *addr* est l'adresse IP du voisin OSPFv2. L'argument *if_name* est l'interface utilisée pour communiquer avec le voisin. Si le voisin OSPFv2 ne se trouve pas sur le même réseau que l'une des interfaces connectées directement, vous devez préciser l'interface.

Configurer les minuteries de calcul de routage

Vous pouvez configurer le délai entre le moment où le protocole OSPFv2 reçoit une modification de topologie et le moment où il démarre un calcul SPF. Vous pouvez également configurer le délai de rétention entre deux calculs SPF consécutifs.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les minuteries de calcul de routage :

timers throttle spf *spf-start spf-hold spf-maximum*

Exemple :

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

L'argument *sf-start* est le délai (en millisecondes) entre le moment où OSPF reçoit une modification de topologie et le moment où il démarre un calcul SPF. Il peut s'agir d'un entier compris entre 0 et 600 000.

L'argument *spf-hold* est le temps minimal (en millisecondes) entre deux calculs SPF consécutifs. Il peut s'agir d'un entier compris entre 0 et 600 000.

L'argument spf-maximum est le temps maximal (en millisecondes) entre deux calculs SPF consécutifs. Il peut s'agir d'un entier de 0 à 600 000.

Journaliser les voisins en hausse ou en baisse

Par défaut, un message de journal système est généré lorsqu'un voisin OSPFv2 redevient disponible ou tombe en panne.

Configurez la commande **log-adj-changes** si vous souhaitez connaître l'augmentation ou la baisse des voisins OSPFv2 sans activer la commande **debug ospf adjacency**. La commande **log-adj-changes** fournit une vue de niveau supérieur de la relation avec les homologues avec moins de résultats. Configurez la commande **log-adj-changes detail** si vous souhaitez voir les messages pour chaque changement d'état.

Procédure

Étape 1 Créez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez la journalisation pour les voisins ascendants ou descendants :

log-adj-changes [**detail**]

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 17.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Configurez une chaîne de clés avec un nom :

key chain*key-chain-name*

Exemple :

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

Vous pouvez maintenant définir les paramètres associés à la chaîne de clés.

Étape 2 Configurez l'identifiant de la chaîne de clés :

key*key-id*

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Exemple :

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

Étape 3 Configurez la clé ou le mot de passe de la chaîne de clés :

key-string [**0** | **8**] *key-string-text*

- Utilisez **0** pour indiquer qu'un mot de passe non chiffré suit, comme le montre l'exemple.
- Utilisez **8** pour indiquer qu'un mot de passe chiffré suit.
- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Exemple :

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

Étape 4 Configurez l'algorithme cryptographique pour la chaîne de clés :

cryptographic-algorithm*md5*

Vous devez fournir l'algorithme d'authentification cryptographique. Bien que la plateforme prenne en charge SHA1 et MD5, seul MD5 est pris en charge pour la gestion de la chaîne de clés.

Exemple :

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

Étape 5 (Facultatif) Configurez les paramètres de durée de vie de la chaîne de clés :

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée ou à l'heure absolue à laquelle la durée de vie de l'acceptation/envoi prend fin, ou être infinie.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Exemple :

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

Vous pouvez utiliser la commande **show key chain** pour afficher la configuration de la chaîne de clés de démarrage sur le périphérique; **show run key chain** pour afficher la configuration de la chaîne de clés qui est actuellement en cours d'exécution sur le périphérique.

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#
```

```
ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface.

- Configurer les paramètres d'interface OSPFv2, à la page 17

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3.

Activer OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer la route dans les processus de routage OSPFv3 ciblés.

Procédure

Étape 1 Créez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
```

L'argument *process-id* est une balise utilisée en interne pour ce processus de routage et peut être n'importe quel entier positif. Cette balise ne doit pas nécessairement correspondre à la balise d'un autre appareil; elle est réservée à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez une interface :

interface *interface_name*

Exemple :

```
ciscoasa(config)# interface Gigabitethernet0/0
```

Étape 3 Créez le processus de routage OSPFv3 avec l'ID de processus spécifié et une zone pour le protocole OSPFv3 avec l'ID de zone spécifié :

ipv6 ospf *process-id* **area** *area_id*

Exemple :

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

Configurer les paramètres d'interface OSPFv3

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 10
```

L'argument *process-id* est une balise utilisée en interne pour ce processus de routage et peut être n'importe quel entier positif. Cette balise ne doit pas nécessairement correspondre à la balise d'un autre appareil; elle est réservée à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Créez une zone OSPFv3 :

ipv6 ospf **area** [*area-num*] [**instance**]

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

L'argument *area-num* est la zone pour laquelle l'authentification doit être activée. Il peut s'agir d'une valeur décimale ou d'une adresse IP. Le mot clé **instance** spécifie l'ID d'instance de zone à attribuer à une interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 3 Spécifiez le coût d'envoi d'un paquet sur une interface :

ipv6 ospf cost *interface-cost*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

L'argument *interface-cost* spécifie une valeur d'entier non signée exprimée sous forme de mesure d'état de liaison, dont la valeur peut aller de 1 à 65535. Le coût par défaut est basé sur la bande passante.

Étape 4 Filtrez les LSA sortants vers une interface OSPFv3 :

ipv6 ospf database-filter all out

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

Tous les LSA sortants sont acheminés vers l'interface par défaut.

Étape 5 Définissez la durée en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne :

ipv6 ospf dead-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535. La valeur par défaut est quatre fois l'intervalle défini par la commande **ipv6 ospf hello-interval**.

Étape 6 Spécifiez le type de chiffrement d'une interface :

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
```

```
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

Le mot clé **ipsec** spécifie le protocole de sécurité IP. La paire mot clé-argument **spi** *spi* spécifie l'indice de la politique de sécurité, qui doit être compris entre 256 et 42949667295 et saisi sous forme décimale.

Le mot clé **esp** spécifie la charge utile de sécurité qui s'encapsule. L'argument *encryption-algorithm* spécifie l'algorithme de chiffrement à utiliser avec ESP. Les valeurs valides sont les suivantes :

- aes-cdc : active le chiffrement AES-CDC.
- 3des : active le chiffrement 3DES.
- des : active le chiffrement DES.
- null : spécifie ESP sans chiffrement.

L'argument *key-encryption-type* peut être l'une des deux valeurs suivantes :

- 0 : la clé n'est pas chiffrée.
- 7 : la clé est chiffrée.

L'argument *key* spécifie le nombre utilisé dans le calcul du condensé de message. Le nombre comporte 32 chiffres hexadécimaux (16 octets). La taille de la clé dépend de l'algorithme de chiffrement utilisé. Certains algorithmes, comme AES-CDC, vous permettent de choisir la taille de la clé. L'argument *authentication-algorithm* spécifie l'algorithme d'authentification de chiffrement à utiliser, qui peut être l'une des options suivantes :

- md5 : active le condensé de message 5 (MD5).
- sha1 : active SHA-1.

Le mot clé **null** remplace le chiffrement de zone.

Si le chiffrement OSPFv3 est activé sur une interface et qu'un voisin se trouve dans une zone différente (par exemple, la zone 0) et que vous souhaitez que l'ASA forme des contiguïtés avec cette zone, vous devez modifier la zone sur l'ASA. Après avoir modifié la zone sur l'ASA en 0, un délai de deux minutes est nécessaire avant que la contiguïté OSPFv3 ne se produise.

Étape 7 Spécifiez la réduction des inondations des LSA vers l'interface :

ipv6 ospf flood-reduction

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
```

```
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

Étape 8 Spécifiez l'intervalle en secondes entre les paquets Hello envoyés sur l'interface :

ipv6 ospf hello-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf hello-interval 15
```

La valeur doit être la même pour tous les nœuds d'un réseau spécifique et peut varier de 1 à 65535. L'intervalle par défaut est de 10 secondes pour les interfaces Ethernet et de 30 secondes pour les interfaces de non-diffusion.

Étape 9 Ddésactivez la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD :

ipv6 ospf mtu-ignore

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

La détection des incompatibilités MTU OSPF est activée par défaut.

Étape 10 Définissez le type de réseau OSPF sur un type autre que la valeur par défaut, qui dépend du type de réseau :

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
```

```
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

Le mot clé **point-to-point non-broadcast** définit le type de réseau sur point à point de non-diffusion. Le mot clé **broadcast** définit le type de réseau sur diffusion.

Étape 11 Définissez la priorité du routeur, qui aide à déterminer le routeur désigné pour un réseau :

ipv6 ospf priority *number-value*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

Les valeurs valides sont comprises entre 0 et 255.

Étape 12 Configurez les interconnexions du routeur OSPFv3 avec les réseaux de non-diffusion :

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Étape 13 Spécifiez le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface :

ipv6 ospf retransmit-interval *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
```

```
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 14 Définissez l'estimation du temps en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface.

ipv6 ospf transmit-delay *seconds*

Exemple :

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Configurer les paramètres de routeur OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les paramètres de zone OSPFv3 :

domaine

Exemple :

```
ciscoasa(config-rtr)# area 10
```

Les paramètres pris en charge comprennent l'ID de zone sous la forme d'une valeur décimale de 0 à 4294967295 et l'ID de zone dans le format d'adresse IP **A.B.C.D**.

Étape 3 Définissez une commande à sa valeur par défaut :

par défaut

Exemple :

```
ciscoasa(config-rtr)# default originate
```

Le paramètre **originate** distribue la route par défaut.

Étape 4 Contrôlez la distribution des renseignements par défaut :

default-information

Étape 5 Définissez la distance administrative de la route OSPFv3 en fonction du type de route :

distance

Exemple :

```
ciscoasa(config-rtr)# distance 200
```

Les paramètres pris en charge comprennent la distance administrative avec des valeurs de 1 à 254 et **ospf** pour la distance OSPFv3.

Étape 6 Supprimez l'envoi de messages de journal système avec le paramètre **lsa** lorsque le routeur reçoit une annonce d'état de liaison (LSA) pour les paquets OSPF de multidiffusion (MOSPF) de type 6 :

ignore

Exemple :

```
ciscoasa(config-rtr)# ignore lsa
```

Étape 7 Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif :

log-adjacency-changes

Exemple :

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

Avec le paramètre **detail**, tous les changements d'état sont enregistrés.

Étape 8 Supprimez l'envoi et la réception des mises à jour de routage sur une interface :

passive-interface [*interface_name*]

Exemple :

```
ciscoasa(config-rtr)# passive-interface inside
```

L'argument *interface_name* spécifie le nom de l'interface sur laquelle le processus OSPFv3 est en cours d'exécution.

Étape 9 Configurez la redistribution des routes d'un domaine de routage vers un autre :

redistribute {**connected** | **ospf** | **static**}

Lieu :

- **connected** : spécifie les routes connectées.
- **ospf** : spécifie les routes OSPFv3.
- **static** : spécifie les routes statiques.

Exemple :

```
ciscoasa(config-rtr)# redistribute ospf
```

Étape 10 Créez un ID de routeur fixe pour un processus spécifié :

router-id {*A.B.C.D* | **cluster-pool** | **static**}

Lieu :

A.B.C.D : spécifie l'ID du routeur OSPF sous forme d'adresse IP.

cluster-pool : configure un ensemble d'adresses IP lorsque la mise en grappe d'interfaces individuelles est configurée. Pour en savoir plus sur les ensembles d'adresses IP utilisés dans la mise en grappe, consultez Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3), à la page 23.

Exemple :

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

Étape 11 Configurez les résumés d'adresses IPv6 avec des valeurs valides de 0 à 128 :

summary-prefix *X:X:X:X::X/*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

Le paramètre *X:X:X:X::X/* spécifie le préfixe IPv6.

Étape 12 Ajustez les minuteries de routage :

timers

Les paramètres des minuteries de routage sont les suivants :

- **lsa** : spécifie les minuteries LSA OSPFv3.
- **nsf** : spécifie les minuteries d'attente NSF OSPFv3.
- **pacing** : spécifie les minuteries de régulation OSPFv3.
- **throttle** : spécifie les minuteries de limitation OSPFv3.

Exemple :

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

Configurer les paramètres de zone OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535.

Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez le coût par défaut d'une zone NSSA ou d'une zone tampon :

area *area-id* **default-cost** *cost*

Exemple :

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

Étape 3 Résumez les routes qui correspondent à l'adresse et au masque pour les routeurs de frontière uniquement :

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

Exemple :

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- L'argument *area-id* identifie la zone pour laquelle les routes doivent être résumées. La valeur peut être spécifiée sous la forme d'une décimale ou d'un préfixe IPv6.

- L'argument *ipv6-prefix* spécifie le préfixe IPv6. L'argument *prefix-length* spécifie la longueur du préfixe.
- Le mot clé **advertise** définit l'état de la plage d'adresses à annoncer et génère un LSA récapitulatif de type 3.
- Le mot clé **not-advertise** définit l'état de la plage d'adresses sur DoNotAdvertise.
- Le LSA récapitulatif de type 3 est supprimé et les réseaux des composants restent masqués pour les autres réseaux.
- La paire mot clé-argument **cost** *cost* spécifie la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination.
- Les valeurs valides sont comprises entre 0 et 16 77 77 2015.

Étape 4 Précisez une zone NSSA :

area *area-id* **nssa**

Exemple :

```
ciscoasa(config-rtr)# area 1 nssa
```

Étape 5 Précisez une zone tampon :

area *area-id* **stub**

Exemple :

```
ciscoasa(config-rtr)# area 1 stub
```

Étape 6 Définissez un lien virtuel et ses paramètres :

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

Exemple :

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- L'argument *area-id* identifie la zone pour laquelle les routes doivent être résumées. Le mot clé **virtual link** spécifie la création d'un voisin de lien virtuel.
- L'argument *router-id* spécifie l'ID de routeur associé au voisin de lien virtuel.
- Saisissez la commande **show ospf** ou **show ipv6 ospf** pour afficher l'ID du routeur. Il n'y a pas de valeur par défaut.
- Le mot clé **hello-interval** spécifie le temps en secondes entre les paquets Hello qui sont envoyés sur une interface. L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 10.
- La paire mot clé-argument **retransmit-interval** *seconds* spécifie le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission

est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 8 192. La valeur par défaut est égale à 5.

- La paire mot clé-argument **transmit-delay** *seconds* spécifie le temps estimé en secondes nécessaire pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. La valeur entière doit être supérieure à zéro. Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. La plage de valeurs peut aller de 1 à 8 192. La valeur par défaut est 1.
- La paire mot clé-argument **dead-interval** *seconds* spécifie la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192.
- Le mot clé **ttl-security hops** configure la sécurité de durée de vie (TTL) sur un lien virtuel. La valeur de l'argument *hop-count* peut aller de 1 à 254.

Configurer des interfaces passives OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Supprimez l'envoi et la réception des mises à jour de routage sur une interface :

passive-interface [*interface_name*]

Exemple :

```
ciscoasa(config-rtr)# passive-interface inside
```

L'argument *interface_name* spécifie le nom de l'interface sur laquelle le processus OSPFv3 est en cours d'exécution. Si l'argument *no interface_name* est spécifié, toutes les interfaces du processus OSPFv3 *process_id* sont rendues passives.

Configurer la distance administrative OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez la distance administrative pour les routes OSPFv3 :

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

Exemple :

```
ciscoasa(config-rtr)# distance ospf external 200
```

Le mot clé **ospf** spécifie les routes OSPFv3. Le mot clé **external** spécifie les routes externes de type 5 et de type 7 pour le protocole OSPFv3. Le mot clé **inter-area** spécifie les routes inter-zone pour le protocole OSPVv3. Le mot clé **intra-area** spécifie les routes intra-zone pour le protocole OSPFv3. L'argument *distance* spécifie la distance administrative, qui est un entier compris entre 10 et 254.

Configurer les minuteries mOSPFv3

Vous pouvez définir les minuteries d'arrivée des LSA, de cadence des LSA et de limitation pour le protocole OSPFv3.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de

tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Définissez l'intervalle minimum auquel l'ASA accepte les mêmes LSA de voisins OSPF :

timers lsa arrival *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

L'argument *milliseconds* spécifie le délai minimum en millisecondes qui doit s'écouler entre l'acceptation de la même LSA provenant des voisins. La plage va de 0 à 6 000 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.

Étape 3 Configurez la cadence des paquets LSA :

timers pacing flood *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers lsa flood 20
```

L'argument *milliseconds* spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.

Étape 4 Modifiez l'intervalle auquel les LSA OSPFv3 sont collectés dans un groupe et actualisés, additionnés ou rendus obsolètes :

timers pacing lsa-group *seconds*

Exemple :

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

L'argument *seconds* spécifie le nombre de secondes dans l'intervalle auquel les LSA sont regroupés, actualisés, additionnés ou rendus obsolètes. La plage va de 10 à 1 800 secondes. La valeur par défaut est 240secondes.

Étape 5 Configurez la cadence des paquets de retransmission LSA :

timers pacing retransmission *milliseconds*

Exemple :

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

L'argument *milliseconds* spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont cadencés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.

Étape 6 Configurez la limitation des LSA OSPFv3 :

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

Exemple :

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- L'argument *milliseconds1* spécifie le délai en millisecondes pour générer la première occurrence de LSA. L'argument *milliseconds2* spécifie le délai maximum en millisecondes pour générer le même LSA. L'argument *milliseconds3* spécifie le délai minimum en millisecondes pour générer le même LSA.
- Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.
- Pour *milliseconds1*, la valeur par défaut est 0 milliseconde.
- Pour *milliseconds2* et *milliseconds3*, la valeur par défaut est 5 000 millisecondes.

Étape 7 Configurez la limitation du SPF OSPFv3 :

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

Exemple :

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- L'argument *milliseconds1* spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. L'argument *milliseconds2* spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. L'argument *milliseconds3* spécifie le temps d'attente maximum en millisecondes pour les calculs SPF.
- Pour la limitation SPF, si *milliseconds2* ou *milliseconds3* est inférieur à *milliseconds1*, le protocole OSPFv3 corrige automatiquement la valeur *milliseconds1*. De même, si *milliseconds3* est inférieur à *milliseconds2*, le protocole OSPFv3 corrige automatiquement la valeur *milliseconds2*.
- Pour *milliseconds1*, la valeur par défaut de la limitation SPF est de 5 000 millisecondes.
- Pour *milliseconds2* et *milliseconds3*, la valeur par défaut de la limitation SPF est de 10 000 millisecondes.

Définir les voisins OSPFv3 statiques

Vous devez définir des voisins OSPFv3 statiques pour annoncer les routes OSPF sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv3 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv3. Consultez Configurer une route statique pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Activez un processus de routage OSPFv3 et passez en mode de configuration du routeur IPv6.

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez les interconnexions du routeur OSPFv3 avec les réseaux de non-diffusion.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Exemple :

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Réinitialiser les paramètres par défaut OSPFv3

Pour rétablir la valeur par défaut d'un paramètre OSPFv3, procédez comme suit :

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Renvoyez un paramètre facultatif à sa valeur par défaut :

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route | distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Exemple :

```
ciscoasa(config-rtr)# default metric 5
```

- Le mot clé **area** spécifie les paramètres de zone OSPFv3. Le mot clé **auto-cost** spécifie le coût de l'interface OSPFv3 en fonction de la bande passante.
- Le mot clé **default-information** distribue les renseignements par défaut. Le mot clé **default-metric** spécifie la mesure d'une route redistribuée.
- Le mot clé **discard-route** active ou désactive l'installation d'une route rejetée. Le mot clé **distance** spécifie la distance administrative.
- Le mot clé **distribue-list** filtre les réseaux dans les mises à jour de routage.
- Le mot clé **ignore** ignore un événement particulier. Le mot clé **log-adjacency-changes** enregistre les modifications dans l'état de contiguïté.
- Le mot clé **maximum-paths** transfère les paquets sur plusieurs chemins.
- Le mot clé **passive-interface** supprime les mises à jour de routage sur une interface.
- Le mot clé **redistribute** redistribue les préfixes IPv6 à partir d'un autre protocole de routage.
- Le mot clé **router-id** spécifie l'ID de routeur pour le processus de routage indiqué.
- Le mot clé **summary-prefix** spécifie le préfixe récapitulatif IPv6.
- Le mot clé **timers** spécifie les minuteries du protocole OSPFv3.

Envoyer les messages du journal système

Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif.

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif :

log-adjacency-changes [**detail**]

Exemple :

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

Le mot clé **detail** envoie un message de journal système pour chaque état, pas seulement lorsqu'un voisin OSPFv3 est activé ou désactivé.

Supprimer les messages du journal système

Pour supprimer l'envoi des messages de journal système lorsque la route reçoit des paquets LSA de type 6 OSPF multidiffusion (MOSPF) non pris en charge, procédez comme suit :

Procédure

Étape 1 Activez un processus de routage OSPFv2 :

router ospf *process_id*

Exemple :

```
ciscoasa(config-if)# router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Supprimez l'envoi des messages de journal système lorsque le routeur reçoit des paquets LSA de type 6 MOSPF non pris en charge :

ignore lsa mospf

Exemple :

```
ciscoasa(config-rtr)# ignore lsa mospf
```

Calculer les coûts récapitulatifs de la route

Procédure

Restaurez les méthodes utilisées pour calculer les coûts des routes récapitulatives conformément à la RFC 1583 :

compatible rfc1583

Exemple :

```
ciscoasa (config-rtr)# compatible rfc1583
```

Générer une route externe par défaut dans un domaine de routage OSPFv3

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Générez une route externe par défaut dans un domaine de routage OSPFv3 :

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- Le mot clé **always** annonce la route par défaut, que cette dernière existe ou non.
- La paire mot clé-argument **metric** *metric-value* spécifie la mesure utilisée pour générer la route par défaut.
- Si vous ne spécifiez pas de valeur à l'aide de la commande **default-metric**, la valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.
- La paire mot clé-argment **metric-type** *type-value* spécifique le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides peuvent être l'une des valeurs suivantes :
  - 1. Route externe de type 1
  - 2. Route externe de type 2

  La valeur par défaut est la route externe de type 2.
- La paire mot clé-argument **route-map** *map-name* spécifie le processus de routage qui génère la route par défaut si la carte de routage est satisfaite.

Configurer un préfixe de résumé IPv6

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process_id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Configurer un préfixe de résumé IPv6 :

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

L'argument *prefix* est le préfixe de routage IPv6 pour la destination. Le mot clé **not-advertise** supprime les routes qui correspondent à la paire préfixe-masque spécifiée. Ce mot clé s'applique uniquement à OSPFv3. La paire mot clé-argument **tag** *tag-value* spécifie la valeur de balise qui peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage. Ce mot clé s'applique uniquement à OSPFv3.

Redistribuer les routes IPv6

Procédure

Étape 1 Activez un processus de routage OSPFv3 :

ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config-if)# ipv6 router ospf 1
```

L'argument *process-id* est un identifiant utilisé en interne pour ce processus de routage. Il est attribué localement et peut être n'importe quel entier positif compris entre 1 et 65 535. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage administratif interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Redistribuez les routes IPv6 d'un processus OSPFv3 dans un autre :

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Exemple :

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- L'argument *source-protocol* spécifie le protocole source à partir duquel les routes sont redistribuées, qui peuvent être statiques, connectées ou OSPFv3.
- L'argument *process-id* est le numéro attribué administrativement lorsque le processus de routage OSPFv3 est activé.
- Le mot clé **include-connected** permet au protocole cible de redistribuer les routes apprises par le protocole source et les préfixes connectés sur les interfaces sur lesquelles le protocole source fonctionne.
- Le mot clé **level-1** indique que pour le protocole Intermediate System to Intermediate System (IS-IS), les routes de niveau 1 sont redistribuées dans d'autres protocoles de routage IP indépendamment.
- Le mot clé **level-1-2** indique que pour IS-IS, les routes de niveau 1 et de niveau 2 sont redistribuées dans d'autres protocoles de routage IP.
- Le mot clé **level-2** spécifie que pour IS-IS, les routes de niveau 2 sont redistribuées dans d'autres protocoles de routage IP indépendamment.
- Pour la paire mot clé-argument **metric** *metric-value*, lors de la redistribution d'un processus OSPFv3 dans un autre processus OSPFv3 sur le même routeur, la mesure est transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPFv3, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.
- Le mot clé **metric transparent** permet au protocole RIP d'utiliser la mesure de la table de routage pour les routes redistribuées comme mesure RIP.
- La paire mot clé-argment **metric-type** *type-value* spécifique le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides peuvent être l'une des suivantes : 1 pour une route externe de type 1 ou 2 pour une route externe de type 2. Si aucune valeur n'est spécifiée pour le mot clé **metric-type**, l'ASA adopte une route externe de type 2. Pour IS-IS, le type de lien peut être de l'une des options suivantes : interne pour une mesure IS-IS inférieure à 63 ou externe pour une mesure IS-IS supérieure à 64 et inférieure à 128. La valeur par défaut est interne.
- Le mot clé **match** redistribue les routes dans d'autres domaines de routage et est utilisé avec l'une des options suivantes : **external** [**1**|**2**] (externe [1|2]) pour les routes externes au système autonome, mais qui sont importées dans le protocole OSPFv3 en tant que routes externes de type 1 ou de type 2; **internal** (interne) pour les routes internes à un système autonome donné; **nssa-external** [**1**|**2**] (nssa-externe [1|2]) pour les routes externes au système autonome, mais qui sont importées dans le protocole OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 1 ou de type 2.

- La paire mots clé-argument **tag** *tag-value* spécifie la valeur décimale sur 32 bits associée à chaque route externe, qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides vont de 0 à 4294967295.
- Le mot clé **route-map** spécifie la carte de routage à vérifier pour filtrer l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce mot clé n'est pas spécifié, toutes les routes sont redistribuées. Si ce mot clé est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. L'argument *map-tag* identifie une carte de routage configurée.

Configurer le redémarrage progressif

L'ASA peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage.

En mode de haute disponibilité, le processus OSPF redémarre lorsque l'unité active devient inactive et que l'unité en veille devient la nouvelle active. De même, en mode grappe, le processus OSPF redémarre lorsque l'unité de contrôle devient inactive et que l'unité de données est choisie comme nouvelle unité de contrôle. Ces processus de transition OSPF entraînent un retard considérable. Vous pouvez configurer NSF pour éviter la perte de trafic lors du changement d'état du processus OSPF. La fonctionnalité NSF est également utile lorsqu'une mise à niveau logicielle rapide est planifiée.

Le redémarrage progressif est pris en charge sur les protocoles OSPFv2 et OSPFv3. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623). Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Remarque Lorsque des Hello rapides sont configurés pour le protocole OSPFv2, le redémarrage progressif ne se produit pas lorsque l'unité active est rechargée et que l'unité en veille devient active. En effet, le temps nécessaire au changement de rôle est supérieur à l'intervalle de temps mort configuré.

Configurer les capacités

Le mécanisme de redémarrage progressif de Cisco NSF dépend de la capacité de LLS, car il envoie un bloc LLS avec le bit RS défini dans le paquet Hello, pour indiquer l'activité de redémarrage. Le mécanisme IETF NSF dépend de la capacité de LSA opaque lorsqu'il envoie des LSA opaques de type 9 pour indiquer l'activité de redémarrage. Pour configurer les fonctionnalités, saisissez les commandes suivantes :

Procédure

Étape 1 Créez un processus de routage OSPF et entrez en mode de configuration de routeur pour le processus OSPF que vous souhaitez redistribuer :

router ospf *process_id*

Exemple :

```
ciscoasa(config)# router ospf 2
```

L'argument process_id est un identifiant utilisé en interne pour ce processus de routage et peut être n'importe quel entier positif. Cet ID ne doit pas correspondre à l'ID de tout autre appareil; il est exclusivement réservé à un usage interne. Vous pouvez utiliser un maximum de deux processus.

Étape 2 Activez l'utilisation du bloc de données LLS ou de LSA opaques pour activer NSF :

capability {lls|opaque}

Le mot clé lls est utilisé pour activer la fonctionnalité LLS pour le mécanisme de redémarrage progressif de Cisco NSF.

Le mot clé opaque est utilisé pour activer la capacité de LSA opaque pour le mécanisme de redémarrage progressif IETF NSF.

Configuration du redémarrage progressif pour OSPFv2

Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance ospf. Un périphérique conscient de NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance ospf.

Configurer le redémarrage progressif de Cisco NSF pour OSPFv2

Configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Activez Cisco NSF sur un périphérique compatible avec NSF :

nsf cisco [enforce global]

Exemple :

```
ciscoasa(config-router)# nsf cisco
```

Le mot clé enforce global annule le redémarrage NSF lorsque des périphériques voisins non compatibles avec NSF sont détectés.

Étape 2 Activez le mode d'assistance de Cisco NSF sur le périphérique conscient de NSF :

capability {lls|opaque}

Exemple :

```
ciscoasa(config-router)# capability lls
```

Cette commande est activée par défaut. L'utilisation de la forme no (non) de la commande la désactive.

Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF

Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Activez IETF NSF sur un périphérique compatible avec NSF :

nsf ietf [restart-interval *seconds***]**

Exemple :

```
ciscoasa(config-router)# nsf ietf restart-interval 80
```

Vous pouvez spécifier la durée de l'intervalle de redémarrage progressif, en secondes. Les valeurs valides vont de 1 à 1 800 secondes. La valeur par défaut est 120secondes.

Le redémarrage progressif peut être interrompu si l'intervalle de redémarrage est configuré avec une valeur inférieure au temps nécessaire à la contiguïté. Par exemple, un intervalle de redémarrage inférieur à 30 secondes n'est pas pris en charge.

Étape 2 Activez le mode d'assistance IETF NSF sur le périphérique conscient de NSF :

nsf ietf helper [strict-lsa-checking]

Exemple :

```
ciscoasa(config-router)# nsf ietf helper
```

Le mot clé strict-LSA-checking indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Cette commande est activée par défaut. L'utilisation de la forme no (non) de la commande la désactive.

Configuration du redémarrage progressif pour OSPFv3

La configuration de la fonctionnalité de redémarrage progressif NSF pour OSPFv3 comporte deux étapes : la configuration d'un périphérique pour qu'il soit compatible NSF, puis la configuration d'un périphérique pour qu'il soit conscient de NSF.

Procédure

Étape 1 Activez le traitement IPv6 sur une interface qui n'a pas été configurée avec une adresse IPv6 explicite :

interface physical_interface ipv6 enable

Exemple :

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

L'argument physical_interface identifie l'interface qui participe au protocole NSF OSPFv3.

Étape 2 Activez le redémarrage progressif pour le protocole OSPFv3 sur un appareil compatible NSF :

graceful-restart [restart interval seconds]

Exemple :

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

L'intervalle de redémarrage en secondes spécifie la durée de l'intervalle de redémarrage progressif, en secondes. Les valeurs valides vont de 1 à 1 800 secondes. La valeur par défaut est 120secondes.

Le redémarrage progressif peut être interrompu si l'intervalle de redémarrage est configuré avec une valeur inférieure au temps nécessaire à la contiguïté. Par exemple, un intervalle de redémarrage inférieur à 30 secondes n'est pas pris en charge.

Étape 3 Activez le redémarrage progressif pour le protocole OSPFv3 sur un appareil conscient de NSF :

graceful-restart helper [strict-lsa-checking]

Exemple :

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

Le mot clé strict-LSA-checking indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Le mode d'assistance du redémarrage progressif est activé par défaut.

Configuration de la minuterie d'attente de redémarrage progressif pour OSPF

On s'attend à ce que les routeurs OSPF définissent le bit RS dans l'EO-TLV associé à un paquet Hello lorsqu'on ne sait pas que tous les voisins sont répertoriés dans le paquet, mais que les routeurs qui redémarrent doivent conserver leurs contiguïtés. Cependant, la valeur du bit RS ne doit pas être supérieure aux secondes de RouterDeadInterval. Par conséquent, la commande **timers nsf wait** est introduite pour définir le bit RS dans les paquets Hello inférieurs aux secondes de RouterDeadInterval. La valeur par défaut de la minuterie d'attente de NSF est de 20 secondes.

Avant de commencer

- Pour configurer le délai d'attente de Cisco NSF pour OSPF, le périphérique doit être conscient de NSF ou compatible avec NSF.

Procédure

Étape 1 Entrez en mode de configuration du routeur OSPF.

Exemple :

```
ciscoasa(config)# router ospf
```

Étape 2 Entrez les minuteries et spécifiez nsf.

Exemple :

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

Étape 3 Saisissez l'intervalle d'attente du redémarrage progressif. Cette valeur peut être comprise entre 1 et 65 535.

Exemple :

```
ciscoasa(config-router)# timers nsf wait 200
```

En utilisant l'intervalle d'attente du redémarrage progressif, vous pouvez vous assurer que l'intervalle d'attente n'est pas supérieur à l'intervalle de temps mort du routeur.

Supprimer la configuration OSPFv2

Supprimez la configuration OSPFv2.

Procédure

Supprimez toute la configuration OSPFv2 que vous avez activée.

clear configure router ospf *pid*

Exemple :

```
ciscoasa(config)# clear configure router ospf 1000
```

Une fois la configuration effacée, vous devez reconfigurer OSPF à l'aide de la commande **router ospf**.

Supprimer la configuration OSPFv3

Supprimez la configuration OSPFv3.

Procédure

Supprimez toute la configuration OSPFv3 que vous avez activée :

clear configure ipv6 router ospf *process-id*

Exemple :

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

Une fois la configuration effacée, vous devez reconfigurer OSPFv3 à l'aide de la commande **ipv6 router ospf**.

Exemple de protocole OSPFv2

L'exemple suivant montre comment activer et configurer le protocole OSPFv2 avec différents processus facultatifs :

1. Pour activer le protocole OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. (Facultatif) Pour redistribuer les routes d'un processus OSPFv2 vers un autre processus OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. (Facultatif) Pour configurer les paramètres d'interface OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. (Facultatif) Pour configurer les paramètres de zone OSPFv2, saisissez les commandes suivantes :

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. (Facultatif) Pour configurer les minuteries de calcul de routage et afficher les messages de connexion et de déconnexion du voisinage, saisissez les commandes suivantes :

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. (Facultatif) Pour afficher les paramètres de configuration OSPFv2 actuels, saisissez la commande **show ospf**.

   Voici un exemple de sortie de la commande **show ospf** :

```
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
```

```
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. Pour effacer la configuration OSPFv2, utilisez la commande suivante :

```
ciscoasa(config)# clear configure router ospf pid
```

Exemples de protocole OSPFv3

L'exemple suivant montre comment activer et configurer le protocole OSPFv3 au niveau de l'interface :

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

Voici un exemple de sortie de la commande **show running-config ipv6** :

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

Voici un exemple de sortie de la commande **show running-config interface** :

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

Les exemples suivants montrent comment configurer des interfaces spécifiques au protocole OSPFv3 :

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
```

```
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
12345678901234567890123456789012

ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

Pour un exemple de configuration d'une liaison virtuelle OSPFv3, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

Supervision OSPF

Vous pouvez afficher des statistiques spécifiques, comme le contenu des tables de routage IP, des caches et des bases de données. Vous pouvez également utiliser les renseignements fournis pour déterminer l'utilisation des ressources et résoudre les problèmes de réseau. Vous pouvez également afficher des renseignements sur l'accessibilité des nœuds et découvrir le chemin de routage emprunté par les paquets de votre périphérique à travers le réseau.

Pour superviser ou afficher diverses statistiques de routage OSPFv2, saisissez l'une des commandes suivantes :

Commande	Objectif
show ospf [*process-id* [*area-id*]]	Affiche des renseignements généraux sur les processus de routage OSPFv2.
show ospf border-routers	Affiche les entrées de la table de routage OSPFv2 interne vers l'ABR et l'ASBR.
show ospf [*process-id* [*area-id*]] database	Affiche des listes de renseignements concernant la base de données OSPFv2 pour un routeur en particulier.

Commande	Objectif
show ospf flood-list *if-name*	Affiche une liste des LSA en attente d'être inondés sur une interface (pour observer la cadence des paquets OSPFv2). Les paquets de mise à jour OSPFv2 sont automatiquement cadencés afin qu'ils ne soient pas envoyés à moins de 33 millisecondes d'intervalle. Sans cadence, certains paquets de mise à jour pourraient se perdre dans des situations où la liaison est lente, un voisin ne pourrait pas recevoir les mises à jour assez rapidement ou le routeur pourrait manquer d'espace tampon. Par exemple, sans cadence, des paquets pourraient être abandonnés si l'une des topologies suivantes existe : • Un routeur rapide est connecté à un routeur plus lent sur une liaison point à point. • Pendant l'inondation, plusieurs voisins envoient simultanément des mises à jour à un seul routeur. La cadence est également utilisée entre les renvois pour accroître l'efficacité et réduire au minimum les retransmissions perdues. Vous pouvez également afficher les LSA en attente d'envoi depuis une interface. La cadence permet d'envoyer plus efficacement les paquets de mise à jour et de retransmission OSPFv2. Il n'y a aucune tâche de configuration pour cette fonctionnalité; elle se produit automatiquement.
show ospf interface [*if_name*]	Affiche les renseignements sur l'interface liés au protocole OSPFv2.
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	Affiche les renseignements sur le voisin OSPFv2 par interface.
show ospf request-list *neighbor if_name*	Affiche une liste de tous les LSA demandés par un routeur.
show ospf retransmission-list *neighbor if_name*	Affiche une liste de tous les LSA en attente de renvoi.
show ospf [*process-id*] summary-address	Affiche une liste de tous les renseignements de redistribution des adresses sommaires configurées dans le cadre d'un processus OSPFv2.
show ospf [*process-id*] **traffic**	Affiche une liste des différents types de paquets envoyés ou reçus par une instance OSPFv2 spécifique.
show ospf [*process-id*] virtual-links	Affiche les renseignements sur les liens virtuels liés au protocole OSPFv2.

Commande	Objectif
show route cluster	Affiche des renseignements supplémentaires sur la synchronisation des routes OSPFv2 dans la mise en grappe.

Pour superviser ou afficher diverses statistiques de routage OSPFv3, saisissez l'une des commandes suivantes :

Commande	Objectif
show ipv6 ospf [*process-id* [*area-id*]]	Affiche des renseignements généraux sur les processus de routage OSPFv3.
show ipv6 ospf [*process-id*] **border-routers**	Affiche les entrées de la table de routage OSPFv3 interne vers l'ABR et l'ASBR.
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	Affiche des listes de renseignements concernant la base de données OSPFv3 pour un routeur en particulier.
show ipv6 ospf [*process-id* [*area-id*]] **events**	Affiche les renseignements sur les événements OSPFv3.

Commande	Objectif
show ipv6 ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	Affiche une liste des LSA en attente d'être inondés sur une interface (pour observer la cadence des paquets OSPFv3). Les paquets de mise à jour OSPFv3 sont automatiquement cadencés afin qu'ils ne soient pas envoyés à moins de 33 millisecondes d'intervalle. Sans cadence, certains paquets de mise à jour pourraient se perdre dans des situations où la liaison est lente, un voisin ne pourrait pas recevoir les mises à jour assez rapidement ou le routeur pourrait manquer d'espace tampon. Par exemple, sans cadence, des paquets pourraient être abandonnés si l'une des topologies suivantes existe : • Un routeur rapide est connecté à un routeur plus lent sur une liaison point à point. • Pendant l'inondation, plusieurs voisins envoient simultanément des mises à jour à un seul routeur. La cadence est également utilisée entre les retransmissions pour accroître l'efficacité et réduire au minimum les retransmissions perdues. Vous pouvez également afficher les LSA en attente d'envoi depuis une interface. La cadence permet d'envoyer plus efficacement les paquets de mise à jour et de retransmission OSPFv3. Il n'y a aucune tâche de configuration pour cette fonctionnalité; elle se produit automatiquement.
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	Affiche les renseignements sur l'interface liés au protocole OSPFv3.
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	Affiche les renseignements sur le voisin OSPFv3 par interface.
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	Affiche une liste de tous les LSA demandés par un routeur.
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	Affiche une liste de tous les LSA en attente de renvoi.
show ipv6 ospf statistic [*process-id*] [**detail**]	Affiche diverses statistiques OSPFv3.
show ipv6 ospf [*process-id*] summary-prefix	Affiche une liste de tous les renseignements de redistribution des adresses sommaires configurées dans le cadre d'un processus OSPFv3.

Commande	Objectif
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	Affiche les renseignements sur les minuteries OSPFv3.
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	Affiche les statistiques relatives au trafic OSPFv3.
show ipv6 ospf virtual-links	Affiche les renseignements sur les liens virtuels liés au protocole OSPFv3.
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	Affiche le numéro de séquence de la table de routage IPv6, l'état de la minuterie de reconvergence IPv6 et le numéro de séquence des entrées de routage IPv6 dans une grappe.

Historique OSPF

Tableau 1 : Historique des fonctionnalités OSPF

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF	7.0(1)	Une prise en charge a été ajoutée pour les données de routage, l'authentification, la redistribution et la supervision des informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF). Nous avons introduit la commande suivante : **route ospf**
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage OSPFv2 est pris en charge en mode de contexte multiple.
Mise en grappe	9.0(1)	Pour OSPFv2 et OSPFv3, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges EtherChannel étendu sont pris en charge dans l'environnement de mise en grappe. Nous avons introduit ou modifié les commandes suivantes : **show route cluster**, **show ipv6 route cluster**, **debug route cluster, router-id cluster-pool**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPFv3 pour IPv6	9.0(1)	Le routage OSPFv3 est pris en charge pour IPv6. Nous avons introduit ou modifié les commandes suivantes : **ipv6 ospf**, **ipv6 ospf area**, **ipv6 ospf cost, ipv6 ospf database-filter all out, ipv6 ospf dead-interval, ipv6 ospf encryption, ipv6 ospf hello-interval, ipv6 ospf mtu-ignore, ipv6 ospf neighbor, ipv6 ospf network, ipv6 ospf flood-reduction, ipv6 ospf priority, ipv6 ospf retransmit-interval, ipv6 ospf transmit-delay, ipv6 router ospf, ipv6 router ospf area, ipv6 router ospf default, ipv6 router ospf default-information, ipv6 router ospf distance, ipv6 router ospf exit, ipv6 router ospf ignore, ipv6 router ospf log-adjacency-changes, ipv6 router ospf no, ipv6 router ospf passive-interface, ipv6 router ospf redistribute, ipv6 router ospf router-id, ipv6 router ospf summary-prefix, ipv6 router ospf timers, area encryption, area range, area stub, area nssa, area virtual-link, default, default-information originate, distance, ignore lsa mospf, log-adjacency-changes, redistribute, router-id, summary-prefix, timers lsa arrival, timers pacing flood, timers pacing lsa-group, timers pacing retransmission, timers throttle, show ipv6 ospf, show ipv6 ospf border-routers, show ipv6 ospf database, show ipv6 ospf events, show ipv6 ospf flood-list, show ipv6 ospf graceful-restart, show ipv6 ospf interface, show ipv6 ospf neighbor, show ipv6 ospf request-list, show ipv6 ospf retransmission-list, show ipv6 ospf statistic, show ipv6 ospf summary-prefix, show ipv6 ospf timers, show ipv6 ospf traffic, show ipv6 ospf virtual-links, show ospf, show running-config ipv6 router, clear ipv6 ospf, clear configure ipv6 router, debug ospfv3, ipv6 ospf neighbor**.
Prise en charge OSPF pour les Hellos rapides	9.2(1)	OSPF prend en charge la fonctionnalité Paquets Hello rapides, ce qui permet d'obtenir une configuration qui accélère la convergence dans un réseau OSPF. Nous avons modifié la commande suivante : **ospf dead-interval**
Minuteries	9.2(1)	De nouvelles minuteries OSPF ont été ajoutées; les anciennes ont été rendues obsolètes. Nous avons introduit les commandes suivantes : timers lsa arrival, timers pacing, timers throttle Nous avons supprimé les commandes suivantes : Timers spf, timers lsa-grouping-pacing
Filtrage des routes à l'aide de la liste d'accès	9.2(1)	Le filtrage des routes à l'aide d'ACL est désormais pris en charge. Nous avons introduit la commande suivante : distribute-list
Améliorations de la surveillance OSPF	9.2(1)	Des informations supplémentaires sur la surveillance OSPF ont été ajoutées. Nous avons modifié les commandes suivantes : show ospf events, show ospf rib, show ospf statistics, show ospf border-routers [detail], show ospf interface brief
OSPF redistribue le BGP	9.2(1)	La fonctionnalité de redistribution OSPF a été ajoutée. Nous avons ajouté la commande suivante : redistribute bgp

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.3(1)	La prise en charge des protocoles OSPFv2 et OSPFv3 pour NSF a été ajoutée. Nous avons ajouté les commandes suivantes : capability, nsf cisco, nsf cisco helper, nsf ietf, nsf ietf helper, nsf ietf helper strict-lsa-checking, graceful-restart, graceful-restart helper, graceful-restart helper strict-lsa-checking
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.13(1)	La minuterie d'attente NSF a été ajoutée. Nous avons ajouté une nouvelle commande pour définir la minuterie de l'intervalle de redémarrage NSF. Cette commande a été introduite pour s'assurer que l'intervalle d'attente n'est pas plus long que l'intervalle de temps mort du routeur. Nous avons introduit la commande suivante : **timers nsf wait <seconds>**

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.