Routage par détection de transfert bidirectionnel (BFD)

Ce chapitre décrit comment configurer l'ASA pour utiliser le protocole de routage par détection de transfert bidirectionnel (BFD).

À propos du routage BFD

BFD est un protocole de détection conçu pour fournir des temps de détection de défaillance du chemin d'acheminement rapides pour tous les types de médias, encapsulations, topologies et protocoles de routage. BFD fonctionne en mode point à point de monodiffusion en plus de tout protocole de données transféré entre deux systèmes. Les paquets sont transportés dans la charge utile du protocole d'encapsulation approprié pour le support et le réseau.

BFD fournit une méthode de détection des défaillances cohérente pour les administrateurs réseau en plus de la détection des défaillances du chemin de transfert rapide. Comme l'administrateur réseau peut utiliser BFD pour détecter les défaillances du chemin de transfert à un débit uniforme, plutôt que pour les débits variables, pour les différents mécanismes Hello du protocole de routage, le profilage et la planification du réseau sont plus faciles et le temps de reconversion est uniforme et prévisionnel.

Mode asynchrone BFD et fonction d'écho

La BFD peut fonctionner en mode asynchrone avec ou sans la fonction d'écho activée.

Mode asynchrone

En mode asynchrone, les systèmes envoient périodiquement des paquets de contrôle de la BFD l'un à l'autre, et si un certain nombre de paquets de la ligne ne sont pas reçus par l'autre système, la session est déclarée inactive. Le mode asynchrone pur (sans la fonction d'écho) est utile, car il nécessite deux fois moins de paquets pour atteindre un temps de détection particulier.

Fonction d'écho de la BFD

La fonction d'écho de la BFD envoie des paquets d'écho du moteur de transfert au voisin BFD à saut unique directement connecté. Les paquets écho sont envoyés par le moteur de transfert et redirigés le long du même chemin pour effectuer la détection. La session BFD à l'autre extrémité ne participe pas au transfert réel des paquets écho. Comme la fonction d'écho et le moteur de transfert sont responsables du processus de détection, le nombre de paquets de contrôle de la BFD qui sont envoyés entre les voisins de la BFD est réduit. Puisque le moteur de transfert teste le chemin de transfert sur le système voisin distant sans interagir avec le système distant, la variation du délai entre les paquets est augmentée. Cela se traduit par des délais de détection des défaillances plus rapides.

Lorsque la fonction d'écho est activée, la BFD peut utiliser la minuterie lente pour retarder la session asynchrone et réduire le nombre de paquets de contrôle de BFD envoyés entre les voisins de BFD, ce qui réduit le surdébit de traitement tout en permettant une détection plus rapide des défaillances.

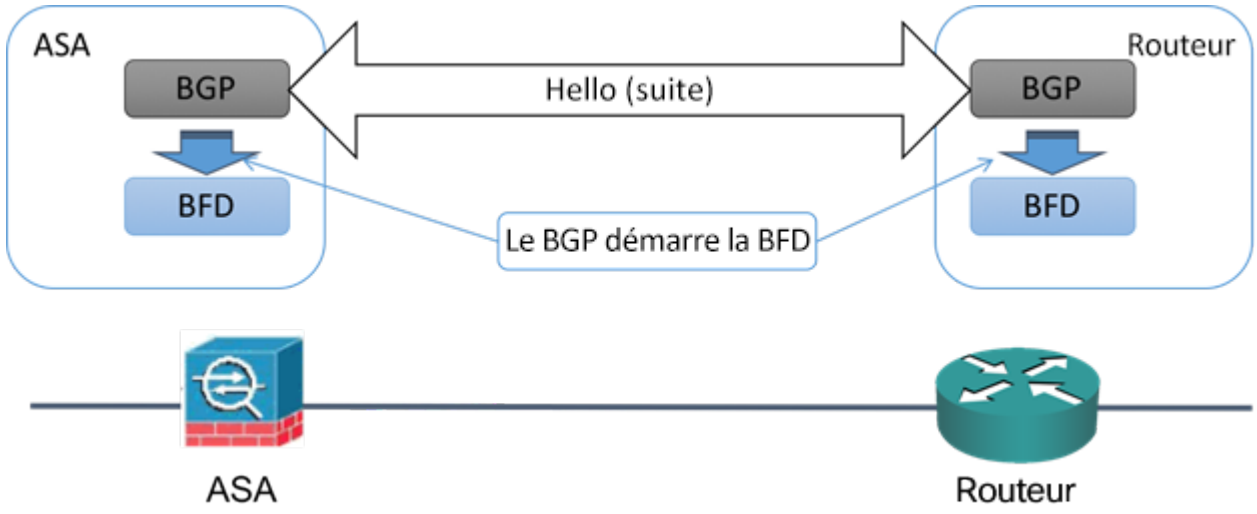
Remarque La fonction d'écho n'est pas prise en charge pour les voisins BFD à multisaut IPv4 ou à saut unique IPv6.

Vous pouvez activer la BFD au niveau de l'interface et du protocole de routage. Vous devez configurer la BFD sur les deux systèmes (homologues BFD). Après avoir activé la BFD sur les interfaces et au niveau du routeur pour les protocoles de routage appropriés, une session BFD est créée, les minuteries de la BFD sont négociées et les homologues de la BFD commencent à s'envoyer des paquets de contrôle de la BFD au niveau négocié.

Établissement de la session BFD

L'exemple suivant montre l'ASA et un routeur voisin exécutant le protocole de passerelle frontière (BGP). Au moment où les deux appareils démarrent, aucune session BFD n'est établie entre eux.

Illustration 1 : Session BFD établie



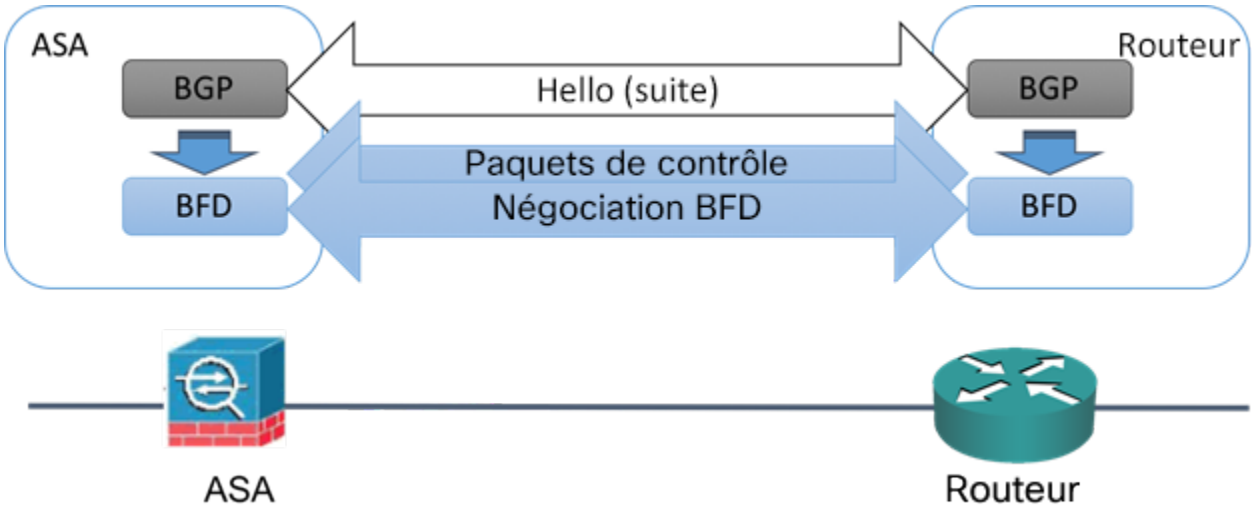
Une fois que le protocole BGP a identifié son voisin BGP, il démarre le processus BFD avec l'adresse IP du voisin. La BFD ne détecte pas ses homologues de manière dynamique. Elle s'appuie sur les protocoles de routage configurés pour lui indiquer quelles adresses IP utiliser et quelles relations d'homologues former.

La BFD sur le routeur et la BFD sur l'ASA forment un paquet de contrôle de BFD et commencent à s'envoyer des paquets à un intervalle d'une seconde jusqu'à ce que la session BFD soit établie. Les paquets de contrôle initiaux de l'un ou l'autre des systèmes sont très similaires. Par exemple, les bits Vers, Diag, H, D, P et F sont tous définis sur zéro et l'état est défini sur Down (En panne). Le champ My Discriminator (Mon discriminateur) est défini sur une valeur unique sur le périphérique de transmission. Le champ Your Discriminator (Votre discriminateur) est défini sur zéro, car la session BFD n'a pas encore été établie. Les minuteries TX et RX sont définies aux valeurs trouvées dans la configuration de l'appareil.

Une fois que le périphérique BFD distant a reçu un paquet de contrôle de BFD pendant la phase d'ouverture de session, il copie la valeur du champ My Discriminator (Mon discriminateur) dans son propre champ Your Discriminator (Votre discriminateur) et la transition de l'état Down (En panne) à l'état Init (Initialisation), puis finalement à l'état Up (Opérationnel) se produit. Une fois que les deux systèmes ont vu leurs propres discriminateurs dans les paquets de contrôle de l'autre, la session est officiellement établie.

L'illustration suivante montre la connexion BFD établie.

Illustration 2 : BGP sans session BFD établie



Négociation de la minuterie BFD

Les appareils BFD doivent négocier les minuteries BFD pour contrôler et synchroniser le débit d'envoi des paquets de contrôle BFD. Un périphérique doit s'assurer des éléments suivants avant de pouvoir négocier une minuterie BFD :

- Que son appareil homologue a vu le paquet contenant les minuteries proposées par le périphérique local
- Qu'il n'envoie jamais de paquets de contrôle BFD plus rapidement que l'homologue n'est configuré pour les recevoir
- Que l'homologue n'envoie jamais de paquets de contrôle BFD plus rapidement que le système local n'est configuré pour les recevoir

Les paramètres du champ Your Discriminator (Votre discriminateur) et du bit H suffisent pour indiquer au périphérique local que le périphérique distant a vu ses paquets lors de l'échange initial de la minuterie. Après avoir reçu un paquet de contrôle BFD, chaque système prend l'intervalle RX minimum requis et le compare à son propre intervalle TX minimum souhaité, puis prend la plus grande (la plus lente) des deux valeurs et l'utilise comme débit de transmission pour ses paquets BFD. Le plus lent des deux systèmes détermine le débit de transmission.

Lorsque ces minuteries ont été négociées, elles peuvent être renégociées à tout moment pendant la session sans entraîner de réinitialisation de session. Le périphérique qui modifie ses minuteries règle le bit P sur tous les paquets de contrôle BFD suivants jusqu'à ce qu'il reçoive un paquet de contrôle BFD avec le bit F défini pour le système distant. Cet échange de bits permet d'éviter la perte de paquets pendant le transit.

Remarque Le réglage du bit F par le système distant ne signifie pas qu'il accepte les nouvelles minuteries proposées. Il indique que le système distant a vu les paquets dans lesquels les minuteries ont été modifiées.

Détection de défaillance BFD

Une fois la session BFD et les minuteries négociées, les homologues BFD s'envoient des paquets de contrôle BFD à l'intervalle négocié. Ces paquets de contrôle agissent comme une pulsation très similaire au protocole IGP Hello, sauf que le débit est plus accéléré.

Tant que chaque homologue de la BFD reçoit un paquet de contrôle de la BFD dans le cadre de l'intervalle de détection configuré (intervalle RX minimal requis), la session de la BFD reste active et tout protocole de routage associé à la BFD conserve ses contiguïtés. Si un homologue BFD ne reçoit pas de paquet de contrôle dans cet intervalle, il informe tous les clients participant à cette session BFD de la défaillance. Le protocole de routage détermine la réponse appropriée à ces renseignements. La réponse typique est de mettre fin à la session d'appairage du protocole de routage et de reconverger, et ainsi de contourner un homologue défaillant.

Chaque fois qu'un homologue BFD reçoit avec succès un paquet de contrôle BFD dans une session BFD, la minuterie de détection pour cette session est réinitialisée à zéro. La détection des défaillances dépend donc des paquets reçus et NON de la dernière transmission d'un paquet par le récepteur.

Scénarios de déploiement BFD

Les éléments suivants décrivent le fonctionnement de la BFD dans ces scénarios spécifiques.

Basculement

Dans un scénario de basculement, des sessions BFD sont établies et maintenues entre l'unité active et l'unité voisine. Les unités en veille ne maintiennent aucune session BFD avec leurs voisins. Lors d'un basculement, la nouvelle unité active doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités actives et de secours.

Pour un scénario de redémarrage progressif/NSF, le client (BGP IPv4/IPv6) est chargé d'informer son voisin de l'événement. Lorsque le voisin reçoit les renseignements, il conserve la table RIB jusqu'à ce que le basculement soit terminé. Pendant le basculement, les sessions BFD et BGP sont inactives sur l'appareil. Une fois le basculement terminé, une nouvelle session BFD entre les voisins est établie lorsque la session BGP est lancée.

EtherChannel étendu et grappe L2

Dans un scénario de grappe EtherChannel étendu, la session BFD est établie et maintenue entre l'unité principale et son voisin. Les unités subordonnées ne maintiennent aucune session BFD avec leurs voisins. Si un paquet BFD est acheminé vers l'unité subordonnée en raison de l'équilibrage de charges sur le commutateur, l'unité subordonnée doit transférer ce paquet à l'unité principale par la liaison de grappe. Lorsqu'un basculement de grappe se produit, la nouvelle unité principale doit initier l'établissement d'une session avec le voisin, car les renseignements sur la session ne sont pas synchronisés entre les unités principale et subordonnée.

Mode d'interface individuelle et grappe L3

Dans un scénario de grappe en mode d'interface individuelle, les unités individuelles maintiennent leurs sessions BFD avec leurs voisins.

Directives pour le routage BFD

Directives relatives au mode contextuel

Pris en charge en modes de contexte unique et multiple.

Directives sur le mode pare-feu

Pris en charge en mode de pare-feu routé; prise en charge des modes autonome, de basculement et de grappe. La BFD n'est pas prise en charge sur les interfaces de basculement. Dans la mise en grappe, cette fonctionnalité n'est prise en charge que sur l'unité principale. La BFD n'est pas prise en charge en mode transparent.

Directives IPv6

Le mode Echo n'est pas pris en charge pour IPv6.

Directives supplémentaires

Les protocoles BGP IPv4et BGP IPv6 sont pris en charge.

Les protocoles OSPFv2, OSPFv3, IS-IS et EIGRP ne sont pas pris en charge.

La BFD pour les routes statiques n'est pas pris en charge.

La BFD de transfert et de tunnel n'est pas prise en charge.

Remarque Pour un routage optimal, ne configurez pas la BFD lorsque le redémarrage progressif du BGP pour NSF est configuré sur le périphérique.

Configurer BFD

Cette section décrit comment activer et configurer le processus de routage BFD sur votre système.

Procédure

Étape 1 Créer le modèle BFD, à la page 6.

Étape 2 Configurer les interfaces BFD, à la page 8.

Étape 3 Configurer les cartes BFD, à la page 9.

Créer le modèle BFD

Cette section décrit les étapes requises pour créer un modèle de BFD et passer en mode de configuration de la BFD.

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une interface unique. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à sauts multiples. Vous pouvez activer Echo sur un seul saut uniquement.

Procédure

Étape 1 Activez la BFD comme protocole de routage sur l'ASA en créant le modèle de BFD, à saut unique ou à multisaut :

bfd-template [single-hop | multi-hop] *template_name*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)#
```

- **single-hop** : spécifie un modèle de BFD à saut unique.
- **multi-hop** : spécifie un modèle de BFD à multisaut.
- *template-name* : spécifie le nom du modèle. Le nom du modèle ne peut pas contenir d'espaces.

La commande **bfd-template** vous permet de créer le modèle de BFD et de passer en mode de configuration de la BFD.

Étape 2 (Facultatif) Configurez Echo sur un modèle de BFD à saut unique :

bfd-template single-hop *template_name*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa (config-bfd)# echo
```

Vous pouvez activer le mode Echo sur un modèle à saut unique. L'écho de la BFD n'est pas pris en charge pour les sessions BFD IPv6.

Étape 3 Configurez les intervalles dans le modèle de BFD :

interval [**both** *milliseconds* | **microseconds {both | min-tx}** *microseconds* | **min-tx** *milliseconds*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both** : capacité minimale d'intervalle de transmission et de réception.
- *milliseconds* : intervalle en millisecondes. La plage se situe entre 50 et 999.
- **microseconds** : spécifie l'intervalle BFD en microsecondes pour **both** et **min-tx**.
- *microseconds* : la plage se situe entre 50 000 et 999 000.
- **min-tx** : capacité minimale d'intervalle de transmission.

Les valeurs d'intervalle BFD spécifiées dans le modèle de BFD ne sont pas spécifiques à une interface unique. Vous pouvez appliquer des modèles de BFD individuels par interface. Consultez Configurer les interfaces BFD, à la page 8.

Étape 4 Configurez l'authentification dans le modèle de BFD :

authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1} [0|8] *word* **key-id** *id*

Exemple :

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication** : spécifie le type d'authentification.
- **md5** : authentification Message Digest 5 (MD5).
- **meticulous-md5** : authentification MD5 à clé précise.
- **meticulous-sha-1** : authentification SHA-1 à clé précise.
- **sha-1** : authentification SHA-1 à clé.
- **0|8** : 0 spécifie qu'un mot de passe NON CHIFFRÉ suivra. Le numéro 8 indique qu'un mot de passe CHIFFRÉ suivra.
- *word* : le mot de passe (clé) de la BFD, qui est un mot de passe/une clé à un chiffre de 29 caractères maximum. Les mots de passe commençant par un chiffre suivi d'un espace blanc ne sont pas pris en charge. Par exemple, « 0 pass » et « 1 » ne sont pas valides.
- **key-id** : ID de la clé d'authentification.
- *id* : ID de clé partagée qui correspond à la valeur de clé. La valeur est comprise entre 0 et 255 caractères.

Vous pouvez configurer l'authentification dans des modèles à saut unique et multisaut. Nous vous conseillons de configurer l'authentification pour renforcer la sécurité. Vous devez configurer l'authentification sur chaque

paire source-destination BFD et les paramètres d'authentification doivent correspondre sur les deux périphériques.

Configurer les interfaces BFD

Vous pouvez lier un modèle BFD à une interface, configurer les paramètres de session BFD de référence par interface et activer le mode écho par interface.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#
```

Étape 2 Appliquez un modèle BFD à une interface :

bfd template *template-name*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# bfd template TEMPLATE1
```

Même si vous n'avez pas créé de modèle à l'aide de la commande **bfd-template**, vous pouvez configurer le nom du modèle sous une interface, mais le modèle est considéré comme non valide tant que vous ne l'avez pas défini. Vous n'avez pas à reconfigurer le nom du modèle. Il devient automatiquement valide.

Étape 3 Configurez les paramètres de session BFD :

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval** *milliseconds* : spécifie le débit auquel les paquets de contrôle BFD sont envoyés aux homologues BFD. La plage va de 50 à 999 millisecondes.
- **min_rx** *milliseconds* : spécifie le débit auquel les paquets de contrôle BFD doivent être reçus des homologues BFD. La plage va de 50 à 999 millisecondes.
- **multiplier** *multiplier-value* : indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que la BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50.

Étape 4 Activez le mode d'écho de la BFD sur une interface :

bfd echo

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

Le mode écho est activé par défaut, mais n'est pas pris en charge dans les sessions IPv6 de la BFD. Lorsque le mode écho est activé, les valeurs minimum du niveau de transmission écho et de l'intervalle de transmission requis sont tirées de la configuration **bfd interval** *milliseconds* **min_rx** *milliseconds*.

Remarque
Avant d'utiliser le mode d'écho de la BFD, vous devez désactiver les messages de redirection ICMP à l'aide de la commande **no ip redirects**. Cela permet d'éviter une utilisation élevée du processeur.

Configurer les cartes BFD

Vous pouvez créer une carte BFD contenant des destinations que vous pouvez associer à un modèle multisaut. Vous devez disposer d'un modèle BFD multisaut déjà configuré.

Procédure

Étape 1 Créez un modèle BFD multisaut. Reportez-vous à Créer le modèle BFD, à la page 6 pour connaître la procédure.

Étape 2 Associez le modèle BFD multisaut à une carte de destinations :

bfd map {ipv4 | ipv6} *destination/cdir source/cdire template-name*

Exemple :

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** : configure une adresse IPv4.
- **ipv6** : configure une adresse IPv6.
- *destination/cdir* : spécifie le préfixe et la longueur du préfixe de destination. Le format est A.B.C.D/<0-32>.
- *source/cdir* : spécifie le préfixe et la longueur du préfixe de destination. Le format est X:X:X;X::X/<0-128>.
- *template-name* : spécifie le nom du modèle multisaut associé à cette carte BFD.

Étape 3 (Facultatif) Configurez la valeur des minuteries lentes de la BFD :

bfd slow-timers [*milliseconds*]

Exemple :

```
ciscoasa(config)# bfd slow-timers 14000
ciscoasa(config-bfd)#
```

milliseconds : (Facultatif) La valeur des minuteries lentes de la BFD. La plage se situe entre 1 000 et 30 000. La valeur par défaut est de 1 000.

Supervision BFD

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage BFD. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

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

- **show bfd neighbors**

  Affiche une liste ligne par ligne des contiguïtés BFD existantes.

- **show bfd summary**

  Affiche les renseignements de base sur la BFD, les clients BFD ou les sessions BFD.

- **show bfd drops**

  Affiche le nombre de paquets abandonnés dans la BFD.

- **show bfd map**

  Affiche les cartes BFD configurées.

- **show running-config bfd**

  Affiche la carte BFD et d'autres configurations liées à la BFD.

- **show running-config bfd-template**

  Affiche les configurations liées au modèle BFD.

Historique du routage BFD

Tableau 1 : Historique des fonctionnalités du routage BFD

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du routage BFD	9.6(2)	L'ASA prend désormais en charge le protocole de routage BFD. Une prise en charge a été ajoutée pour la configuration des modèles, des interfaces et des cartes BFD. La prise en charge du protocole de routage BGP pour utiliser BFD a également été ajoutée. Nous avons ajouté les commandes suivantes : **bfd echo, bfd interval, bfd map, bfd slow-timers, bfd-template, clear bfd counters, clear conf bfd, neighbor fall-over bfd, show bfd drops, show bfd map, show bfd neighbors, show bfd summary, show running-config bfd**

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.