Services DHCP et DDNS

Ce chapitre décrit comment configurer le serveur DHCP ou le relais DHCP, ainsi que les méthodes de mise à jour du DNS dynamique (DDNS).

À propos des services DHCP et DDNS

Les rubriques suivantes décrivent le serveur DHCP, l'agent de relais DHCP et la mise à jour DDNS.

À propos du serveur DHCPv4

DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Le périphérique ASA peut fournir un serveur DHCP aux clients DHCP connectés aux interfaces ASA. Le serveur DHCP fournit des paramètres de configuration réseau directement aux clients DHCP.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67.

Options de DHCP

DHCP fournit une structure pour la transmission des informations de configuration aux hôtes sur un réseau TCP/IP. Les paramètres de configuration sont transportés dans des éléments étiquetés qui sont stockés dans le champ Options du message DHCP. Les données sont également appelées options. Les renseignements sur le fournisseur sont également stockés dans Options, et tous les postes d'informations sur le fournisseur peuvent être utilisés comme options DHCP.

Par exemple, les téléphones IP Cisco téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un téléphone IP Cisco démarre, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une demande avec l'option 150 ou 66 au serveur DHCP pour obtenir cette information.

- L’option 150 de DHCP fournit les adresses IP d’une liste de serveurs TFTP.
- L’option DHCP 66 fournit l’adresse IP ou le nom d’hôte d’un seul serveur TFTP.
- L’option 3 de DHCP définit la voie de routage par défaut.

Une seule demande peut inclure les deux options 150 et 66. Dans ce cas, le serveur DHCP fournit des valeurs pour les deux options dans la réponse si elles sont déjà configurées sur l’ASA.

Vous pouvez utiliser les options DHCP avancées pour fournir les paramètres DNS, WINS et de nom de domaine aux clients DHCP. L’option DHCP 15 est utilisée pour le suffixe de domaine DNS. Vous pouvez également utiliser le paramètre de configuration automatique DHCP pour obtenir ces valeurs ou les définir manuellement. Lorsque vous utilisez plusieurs méthodes pour définir ces informations, elles sont transmises aux clients DHCP dans l'ordre suivant :

1. Paramètres configurés manuellement.
2. Paramètres des options DHCP avancées
3. Paramètres de configuration automatique de DHCP.

Par exemple, vous pouvez définir manuellement le nom de domaine que vous souhaitez que les clients DHCP reçoivent, puis activer la configuration automatique de DHCP. Bien que la configuration automatique de DHCP découvre le domaine ainsi que les serveurs DNS et WINS, le nom de domaine défini manuellement est transmis aux clients DHCP avec les noms de serveurs DNS et WINS découverts, car le nom de domaine découvert par le processus de configuration automatique de DHCP est remplacé par l’ domaine défini.

À propos du serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6), vous pouvez configurer les ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu’ils envoient des paquets de demande d’information (IR) à l’ASA. Le ASA accepte uniquement les paquets IR et n’affecte pas d’adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d’autres termes, en fonction du préfixe que ASA a reçu à l’aide de la délégation de préfixe.

À propos de l'agent relais DHCP

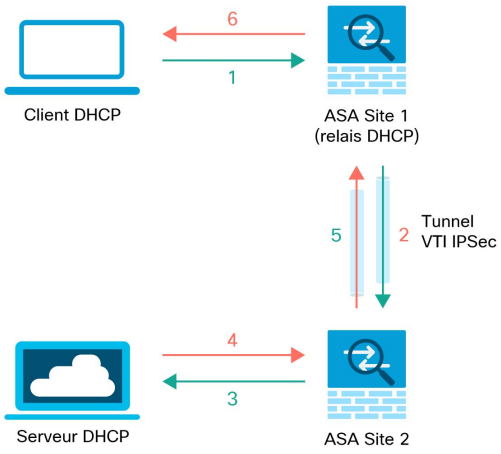
Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n’inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique ASA, car il ne transfère pas le trafic de diffusion. L’agent de relais DHCP vous permet de configurer l’interface du ASA qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via un autre périphérique.

Prise en charge du serveur relais DHCP sur VTI

Vous pouvez configurer un agent de relais DHCP sur une interface ASA pour recevoir et transférer des messages DHCP entre un client DHCP et un serveur DHCP. Cependant, un serveur de relais DHCP pour transférer des messages par l’intermédiaire d’une interface logique n’était pas pris en charge.

La figure suivante montre le processus de découverte du client DHCP et du serveur DHCP qui utilise le relais DHCP sur le VPN VTI. L'agent de relais DHCP, configuré sur l'interface VTI du site 1 de l'ASA, reçoit le paquet DHCPDISCOVER du client DHCP et envoie le paquet par le tunnel VTI. Le site 2 de l'ASA transmet le paquet DHCPDISCOVER au serveur DHCP. Le serveur DHCP répond par un DHCPOFFER au site 2 de l'ASA. L'ASA du site 2 l'envoie au relais DHCP (site 1 de l'ASA), qui l'envoie au client DHCP.

Illustration 1 : Serveur relais DHCP sur VTI



La même procédure est suivie pour les exigences DHCPREQUEST et DHCPACK/NACK.

Lignes directrices pour les services DHCP et DDNS

Cette section comprend des directives et des limites que vous devez vérifier avant de configurer les services DHCP et DDNS.

Mode contextuel

- Le serveur sans état DHCPv6 n'est pas pris en charge en mode contexte multiple.

Mode pare-feu

- Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur DHCP est pris en charge en mode de pare-feu transparent sur une interface de membre de groupe de ponts. En mode routé, le serveur DHCP est pris en charge sur l'interface BVI, pas sur l'interface des membres du groupe de ponts. Les BVI doivent avoir un nom pour que le serveur DHCP puisse fonctionner.
- DDNS n'est pas pris en charge en mode de pare -feu transparent ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur sans état DHCPv6 n'est pas pris en charge en mode de pare-feu transparent ou en mode routé sur l'interface de BVI ou de membre du groupe de ponts.

Mise en grappe

- Le serveur sans état DHCPv6 n'est pas pris en charge par la mise en grappe.

IPv6

Prend en charge IPv6 pour le serveur sans état DHCP et le relais DHCP.

Serveur DHCPv4

- L'ensemble DHCP disponible maximal est de 256 adresses.
- Vous pouvez configurer un serveur DHCP sur n'importe quelle interface avec un nom et une adresse IP, comme une interface physique, une sous-interface ou une BVI en mode routé.
- Vous ne pouvez configurer qu'un seul serveur DHCP sur chaque interface. Chaque interface peut avoir son propre ensemble d'adresses à utiliser. Cependant, les autres paramètres DHCP, tels que les serveurs DNS, le nom de domaine, les options, le délai de ping et les serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.
- Vous ne pouvez pas configurer une interface en tant que client DHCP si un serveur DHCP est également activé sur cette interface; vous devez utiliser une adresse IP statique.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Vous pouvez réserver une adresse DHCP pour une interface. ASA attribue une adresse spécifique de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client.
- L'ASA ne prend pas en charge les serveurs DHCP QIP pour une utilisation avec le service mandataire DHCP.
- Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Serveur PD DHCPv6

Le serveur sans état DHCPv6 ne peut pas être configuré sur une interface où l'adresse DHCPv6, le client de délégation de préfixe ou le relais DHCPv6 est configuré.

Relais DHCP

- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv4, avec un maximum de 4 serveurs par interface.
- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv6. Les serveurs propres à une interface pour IPv6 ne sont pas pris en charge.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu ou le mode routé sur l'interface des BVI ou celle des membres du groupe de ponts. Vous pouvez, cependant, autoriser le trafic DHCP en utilisant une règle d'accès. Pour autoriser les demandes et les réponses DHCP par l'intermédiaire du ASA, vous devez configurer deux règles d'accès, une qui autorise les demandes DHCP

de l'interface interne vers l'extérieur (port de destination d'UDP 67) et une qui autorise les réponses du serveur de l'autre côté (port de destination UDP 68).

- Pour IPv4, les clients doivent être connectés directement à ASA et ne peuvent pas envoyer de demandes par un autre agent de relais ou un routeur. Pour IPv6, ASA prend en charge les paquets d'un autre serveur de relais.
- Les clients DHCP doivent se trouver sur des interfaces différentes des serveurs DHCP vers lesquels ASA relaye les demandes.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.

Service DDNS

Le DDNS du pare-feu prend uniquement en charge le service DynDNS. Par conséquent, assurez-vous que le DDNS est configuré avec l'URL de mise à jour dans la syntaxe suivante :

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

Configurer le serveur DHCP

Cette section décrit comment configurer un serveur DHCP fourni par l'ASA.

Procédure

Étape 1 Activer le serveur DHCPv4, à la page 5.
Étape 2 Configurer les options DHCPv4 avancées, à la page 7.
Étape 3 Configurer le serveur sans état DHCPv6, à la page 9.

Activer le serveur DHCPv4

Pour activer le serveur DHCP sur une interface ASA, procédez comme suit :

Procédure

Étape 1 Créez un ensemble d'adresses DHCP pour une interface. L'ASA attribue à un client une des adresses de cet ensemble à utiliser pendant une période donnée. Ces adresses sont les adresses locales et non traduites pour le réseau connecté directement.

dhcpd address *ip_address_start-ip_address_end if_name*

Exemple :

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

L'ensemble d'adresses doit se trouver sur le même sous-réseau que l'interface ASA. En mode transparent, spécifiez une interface de membres de groupe de ponts. En mode routé, spécifiez une interface routée ou un BVI; ne spécifiez pas l'interface des membres du groupe de ponts.

Étape 2 (Facultatif) (Mode routé) Configurez automatiquement les valeurs DNS, WINS et des noms de domaine obtenues à partir d'une interface exécutant un client DHCP ou PPPoE, ou à partir d'un serveur VPN.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Exemple :

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

Si vous spécifiez les paramètres DNS, WINS ou des noms de domaine à l'aide des commandes suivantes, ils remplacent les paramètres obtenus par la configuration automatique.

Étape 3 (Facultatif) Réservez une adresse DHCP pour un client. L'ASA attribue une adresse spécifique de l'ensemble d'adresses configué à un client DHCP en fonction de l'adresse MAC du client.

dhcpd reserve-address *ip_address mac_address if_name*

Exemple :

```
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

L'adresse réservée doit provenir de l'ensemble d'adresses configuré, et l'ensemble d'adresses doit se trouver sur le même sous-réseau que l'interface ASA. En mode transparent, spécifiez une interface de membres de groupe de ponts. En mode routé, spécifiez une interface routée ou un BVI; ne spécifiez pas l'interface des membres du groupe de ponts.

Étape 4 (Facultatif) Spécifiez la ou les adresses IP du ou des serveurs DNS.

dhcpd dns *dns1* [*dns2*]

Exemple :

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

Étape 5 (Facultatif) Spécifiez la ou les adresses IP du ou des serveurs WINS. Vous pouvez spécifier jusqu'à deux serveurs WINS.

dhcpd wins *wins1* [*wins2*]

Exemple :

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

Étape 6 (Facultatif) Modifiez la durée du bail locatif à accorder au client. La durée du bail locatif équivaut à la durée en secondes pendant laquelle le client peut utiliser l'adresse IP qui lui a été attribuée avant l'expiration du bail. Saisissez une valeur de 0 à 1 048 575. La valeur par défaut est de 3 600 secondes.

dhcpd lease *lease_length*

Exemple :

```
ciscoasa(config)# dhcpd lease 3000
```

Étape 7 (Facultatif) Configurez le nom de domaine.

dhcpd domain *domain_name*

Exemple :

```
ciscoasa(config)# dhcpd domain example.com
```

Étape 8 (Facultatif) Configurez la valeur du délai d'expiration de l'envoi d'un message Ping DHCP pour les paquets ICMP. Pour éviter les conflits d'adresses, l'ASA envoie deux paquets Ping ICMP à une adresse avant d'affecter cette adresse à un client DHCP. La valeur par défaut est de 50 millisecondes.

dhcpd ping timeout *milliseconds*

Exemple :

```
ciscoasa(config)# dhcpd ping timeout 20
```

Étape 9 Définissez une passerelle par défaut qui est envoyée aux clients DHCP. Pour le mode routé, si vous n'utilisez pas la commande **dhcpd option 3 ip**, l'ASA envoie l'adresse IP de l'interface activée pour le serveur DHCP comme passerelle par défaut. Pour le mode transparent, vous devez définir **dhcpd option 3 ip** si vous souhaitez définir une passerelle par défaut; l'ASA lui-même ne peut pas servir de passerelle par défaut.

dhcpd option 3 ip *gateway_ip*

Exemple :

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

Étape 10 Activez le démon DHCP dans l'ASA pour écouter les demandes des clients DHCP sur l'interface activée.

dhcpd enable *interface_name*

Exemple :

```
ciscoasa(config)# dhcpd enable inside
```

Spécifiez la même interface que la plage **dhcpd address**.

Configurer les options DHCPv4 avancées

L'ASA prend en charge les options DHCP répertoriées dans RFC 2132, RFC 2562 et RFC 5510 pour l'envoi de renseignements. Toutes les options DHCP (1 à 255) sont prises en charge, à l'exception des 1, 12, 50 à 54,58 à 59, 61, 67 et 82.

Procédure

Étape 1 Configurez une option DHCP qui renvoie une ou deux adresses IP :

dhcpd option *code* **ip** *addr_1* [*addr_2*]

Exemple :

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

L'option 150 fournit l'adresse IP ou les noms d'un ou de deux serveurs TFTP à utiliser avec les téléphones IP Cisco. L'option 3 définit le routage par défaut pour les téléphones IP Cisco.

Étape 2 Configurez une option DHCP qui renvoie une chaîne de texte :

dhcpd option *code* **ascii** *text*

Exemple :

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

L'option 66 fournit l'adresse IP ou le nom d'un serveur TFTP à utiliser avec les téléphones IP Cisco.

Étape 3 Configurez une option DHCP qui renvoie une valeur hexadécimale.

dhcpd option code hex *value*

Exemple :

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

Remarque
L'ASA ne vérifie pas que le type et la valeur d'option que vous fournissez correspondent au type et à la valeur attendus pour le code d'option, comme défini dans la RFC 2132. Par exemple, vous pouvez saisir la commande **dhcpd option 46 ascii hello** et l'ASA accepte la configuration, bien que l'option 46 soit définie dans la RFC 2132 pour s'attendre à une valeur hexadécimale à un seul chiffre. Pour en savoir plus sur les codes d'option, les types associés et les valeurs attendues, consultez la RFC 2132.

Le tableau suivant présente les options DHCP qui ne sont pas prises en charge par la commande **dhcpd option** .

Tableau 1 : Options DHCP non prises en charge

Code d'option	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS

Code d'option	Description
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Configurer le serveur sans état DHCPv6

Pour les clients qui utilisent SLAAC (StateLess Address Auto Configuration) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6), vous pouvez configurer l'ASA pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que l'ASA a reçu à l'aide de la délégation de préfixe.

Avant de commencer

Cette fonctionnalité n'est prise en charge qu'en mode routé simple. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.

Procédure

Étape 1 Configurez l'ensemble d'adresses DHCP IPv6 qui contient les informations que vous souhaitez que le serveur DHCPv6 fournisse :

ipv6 dhcp pool *pool_name*

Exemple :

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

Vous pouvez configurer des ensembles distincts pour chaque interface si vous le souhaitez, ou utiliser le même ensemble sur plusieurs interfaces.

Étape 2 Configurez un ou plusieurs des paramètres suivants à fournir aux clients dans les réponses aux messages IR :

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

import {[**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**]}

Exemple :

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

La commande **import** utilise un ou plusieurs paramètres que l'ASA a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et dans la commande **import**.

Étape 3 Passez en mode de configuration d'interface pour l'interface sur laquelle vous souhaitez que l'ASA écoute les messages IP :

interface *ID*

Exemple :

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

Étape 4 Activer le serveur DHCPv6 :

ipv6 dhcp server *pool_name*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

Étape 5 Configurez l'annonce de routeur pour informer les clients du SLAAC du serveur DHCPv6 :

ipv6 nd other-config-flag

Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS.

Exemple

Dans l'exemple suivant, deux groupes DHCP IPv6 sont créés et le serveur DHCPv6 est activé sur deux interfaces :

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

Configurer les agents de relais DHCP.

Lorsqu'une requête DHCP entre dans une interface, les serveurs DHCP auxquels l'ASA relaye la requête dépendent de votre configuration. Vous pouvez configurer les types de serveurs suivants :

- Serveurs DHCP spécifiques à l'interface : lorsqu'une requête DHCP entre dans une interface particulière, l'ASA ne relaye la requête qu'aux serveurs spécifiques à l'interface.
- Serveurs DHCP globaux : lorsqu'une requête DHCP entre dans une interface qui n'a pas de serveurs spécifiques à l'interface configurés, l'ASA relaye la requête à tous les serveurs globaux. Si l'interface comporte des serveurs propres à une interface, les serveurs globaux ne sont pas utilisés.

Configurer l'agent de relais DHCPv4

Lorsqu'une requête DHCP entre dans une interface, l'ASA la relaye au serveur DHCP.

Procédure

Étape 1 Effectuez l'une des opérations suivantes ou les deux :

- Spécifiez une adresse IP globale de serveur DHCP et l'interface par laquelle il est accessible.

  dhcprelay server *ip_address if_name*

Exemple :

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- Spécifiez l'ID de l'interface connectée au réseau client DHCP et l'adresse IP du serveur DHCP à utiliser pour les requêtes DHCP qui accèdent à cette interface.

```
interface interface_id
  dhcprelay server ip_address
```

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

Notez que vous ne spécifiez pas l'interface de sortie pour les requêtes, comme dans la commande globale **dhcprelay server**; au lieu de cela, l'ASA utilise la table de routage pour déterminer l'interface de sortie.

Étape 2 Activez le service de relais DHCP sur l'interface connectée aux clients DHCP. Vous pouvez activer le relais DHCP sur plusieurs interfaces.

dhcprelay enable *interface*

Exemple :

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

Étape 3 (Facultatif) Définissez le nombre de secondes autorisées pour le traitement de l'adresse de relais DHCP.

dhcprelay timeout *seconds*

Exemple :

```
ciscoasa(config)# dhcprelay timeout 25
```

Étape 4 (Facultatif) Modifiez la première adresse de routeur par défaut dans le paquet envoyé par le serveur DHCP pour qu'elle corresponde à l'adresse de l'interface ASA.

dhcprelay setroute *interface_name*

Exemple :

```
ciscoasa(config)# dhcprelay setroute inside
```

Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers l'ASA, même si le serveur DHCP spécifie un routeur différent.

S'il n'y a pas d'option de routeur par défaut dans le paquet, l'ASA en ajoute une contenant l'adresse de l'interface.

Étape 5 (Facultatif) Configurez les interfaces en tant qu'interfaces de confiance. Effectuez l'une des opérations suivantes :

- Spécifiez une interface client DHCP en laquelle vous souhaitez avoir confiance :

```
interface interface_id
  dhcprelay information trusted
```

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

Vous pouvez configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance.

- Configurez toutes les interfaces client comme de confiance :

dhcprelay information trust-all

Exemple :

```
ciscoasa(config)# dhcprelay information trust-all
```

Configurer l'agent de relais DHCPv6

Lorsqu'une requête DHCPv6 entre dans une interface, l'ASA la relaye à tous les serveurs globaux DHCPv6.

Procédure

Étape 1 Spécifiez l'adresse de destination du serveur DHCP IPv6 à laquelle les messages des clients sont transférés.

ipv6 dhcprelay server *ipv6_address* [*interface*]

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

L'argument *ipv6-address* peut être une adresse de monodiffusion à portée de liaison, une adresse de multidiffusion, une adresse de monodiffusion à portée de site ou une adresse IPv6 globale. Les adresses de multidiffusion non spécifiées, de boucle avec retour et locales au nœud ne sont pas autorisées comme destination de relais. L'argument *interface* facultatif spécifie l'interface de sortie d'une destination. Les messages des clients sont acheminés à l'adresse de destination par la liaison à laquelle l'interface de sortie est connectée. Si l'adresse spécifiée est une adresse à portée de liaison, vous devez indiquer l'interface.

Étape 2 Activez le service de relais DHCPv6 sur une interface.

ipv6 dhcprelay enable *interface*

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Étape 3 (Facultatif) Précisez la durée en secondes autorisée pour les réponses du serveur DHCPv6 à transmettre au client DHCPv6 via la liaison de relais pour la gestion des adresses de relais.

ipv6 dhcprelay timeout *seconds*

Exemple :

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

Les valeurs valides pour l'argument *seconds* sont comprises entre 1 et 3600. La valeur par défaut est de 60 secondes.

Configuration du DNS dynamique

Lorsqu'une interface utilise l'adressage IP DHCP, l'adresse IP attribuée peut changer lors du renouvellement du bail DHCP. Lorsque l'interface doit être accessible à l'aide d'un nom de domaine complet (FQDN), le changement d'adresse IP peut rendre périmés les enregistrements de ressources du serveur DNS. Le DNS dynamique (DDNS) fournit un mécanisme pour mettre à jour les programmes de routage du DNS chaque fois que l'adresse IP ou le nom d'hôte change. Vous pouvez également utiliser DDNS pour les adresses IP statiques ou PPPoE.

DDNS met à jour les réflecteurs de routage suivants sur le serveur DNS : le RR A comprend le mappage nom-adresse IP, tandis que le RR PTR mappe les adresses aux noms.

L'ASA prend en charge les méthodes de mise à jour DDNS suivantes :

- DDNS standard : la méthode de mise à jour DDNS standard est définie par la RFC 2136.

  Avec cette méthode, l'ASA et le serveur DHCP utilisent les requêtes DNS pour mettre à jour les taux de renouvellement (RR) DNS. L'ASA ou le serveur DHCP envoie une requête DNS à son serveur DNS local pour obtenir des renseignements sur le nom d'hôte et, en fonction de la réponse, détermine le serveur DNS principal qui possède les RR. L'ASA ou le serveur DHCP envoie ensuite une demande de mise à jour directement au serveur DNS principal. Consultez les scénarios typiques suivants.

  - L'ASA met à jour le RR de A et le serveur DHCP met à jour le RR des PTR.

En règle générale, l'ASA « possède » le RR de A, tandis que le serveur DHCP « possède » le taux de renouvellement (RR) PTR, de sorte que les deux entités doivent demander les mises à jour séparément. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR du PTR.

- Le serveur DHCP met à jour les taux de renouvellement A et PTR.

  Utilisez ce scénario si l'ASA n'a pas l'autorité pour mettre à jour le RR de A. Lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR A et PTR.

Vous pouvez configurer différentes propriétés en fonction de vos besoins en matière de sécurité et des exigences du serveur DNS principal. Par exemple, pour une adresse statique, l'ASA doit être propriétaire des mises à jour pour les deux enregistrements.

- Web : la méthode de mise à jour Web utilise la spécification de l'API distante DynDNS. (https://help.dyn.com/remote-access-api/).

  Avec cette méthode, lorsque l'adresse IP ou le nom d'hôte change, l'ASA envoie une requête HTTP directement à un fournisseur DNS auprès duquel vous avez un compte.

Remarque DDNS n'est pas pris en charge sur les interfaces BVI ou de membre du groupe de ponts.

Avant de commencer

- Configurez un serveur DNS sur **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**. Consultez Configurer des serveurs DNS.
- Configurez le nom d'hôte et le nom de domaine du périphérique dans **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**. Consultez Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet. Si vous ne spécifiez pas de nom d'hôte par interface, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, pour l'adressage IP statique ou PPPoE, le nom de domaine du système ou le nom de domaine du serveur DNS est ajouté au nom d'hôte.

Procédure

Étape 1 Méthode standard DDNS : configurez une méthode de mise à jour DDNS pour activer les requêtes DNS de l'ASA.

Vous n'avez pas besoin de configurer une méthode de mise à jour DDNS si le serveur DHCP effectue toutes les demandes.

a) Créez une méthode de mise à jour.

ddns update method *name*

Exemple :

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

b) Spécifiez la méthode DDNS standard.

ddns [**both**]

Par défaut, l'ASA met uniquement à jour le RR A. Utilisez ce paramètre si vous souhaitez que le serveur DHCP mette à jour le RR des PTR. Si vous souhaitez que l'ASA mette à jour le RR A et PTR, spécifiez **both**. Utilisez le mot clé **both** pour les adresses IP statiques ou PPPoE.

Exemple :

```
ciscoasa(DDNS-update-method)# ddns
```

c) (Facultatif) Configurez l'intervalle de mise à jour entre les requêtes DNS.

interval maximum *days hours minutes seconds*

Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres *days* (jours) (0-364), *hours* (heures), *minutes* et *seconds* (secondes).

Exemple :

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

d) Associez cette méthode à une interface. Consultez Étape 3, à la page 17.

Étape 2 Méthode Web : configurez une méthode de mise à jour DDNS pour activer les demandes de mise à jour HTTP à partir de l'ASA.

a) Créez une méthode de mise à jour.

ddns update method *name*

Exemple :

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) Spécifiez le nom d'identité de référence pour valider l'identité du certificat du serveur DDNS. L'ASA tente de trouver une correspondance de nom d'hôte. Si l'hôte ne peut être résolu ou si aucune correspondance n'est trouvée, la connexion est interrompue.

Exemple :

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) Spécifiez la méthode Web et l'URL de mise à jour.

web update-url https://*username (nom d'utilisateur)***:***password (mot de passe)***@***provider-domain (domaine du fournisseur)*/*path (chemin)***?hostname=<h>&myip=<a>**

Avant de saisir le point d'interrogation (?), appuyez simultanément sur les touches Ctrl et v de votre clavier. Cela vous permettra de saisir le caractère ? sans que le logiciel l'interprète comme une requête d'aide.

Exemple :

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) (Facultatif) Spécifiez les types d'adresses (IPv4 ou IPv6) que vous souhaitez mettre à jour.

Par défaut, l'ASA met à jour toutes les adresses IPv4 et IPv6. Si vous souhaitez limiter les adresses, saisissez la commande suivante.

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all** : (par défaut) met à jour toutes les adresses IPv4 et IPv6.
- **both** : met à jour l'adresse IPv4 et la dernière adresse IPv6.
- **ipv4** : met à jour uniquement l'adresse IPv4.
- **ipv6** : met à jour uniquement la dernière adresse IPv6.
- **ipv6 all** : met à jour toutes les adresses IPv6.

Exemple :

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) (Facultatif) Configurez l'intervalle de mise à jour entre les requêtes DNS.

interval maximum *days hours minutes seconds*

Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres *days* (jours) (0-364), *hours* (heures), *minutes* et *seconds* (secondes).

Exemple :

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

f) Associez cette méthode à une interface. Consultez Étape 3, à la page 17.

g) La méthode de type Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Voir l'étape Étape 4, à la page 19.

Étape 3 Configurez les paramètres d'interface pour DDNS, y compris la définition de la méthode de mise à jour, les paramètres du client DHCP et le nom d'hôte pour cette interface.

a) Entrez en mode de configuration d'interface.

interface *ID*

Exemple :

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

b) Attribuez une méthode de mise à jour.

ddns update *name*

Méthode DDNS standard : vous n'avez pas besoin d'attribuer de méthode si vous souhaitez que le serveur DHCP effectue toutes les mises à jour. Cette commande est requise pour la méthode de mise à jour Web.

Exemple :

```
ciscoasa(config-if)# ddns update ddns1
```

c) Attribuez un nom d'hôte à cette interface.

ddns update hostname *hostname*

Si vous ne définissez pas de nom d'hôte, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de FQDN, le nom de domaine système ou le domaine par défaut du groupe de serveurs DNS est ajouté (pour les adresses IP statiques ou PPPoE) ou le nom de domaine du serveur DHCP est ajouté (pour les adresses IP DHCP).

Exemple :

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

d) Méthode DDNS standard : déterminez les enregistrements que vous souhaitez que le serveur DHCP mette à jour.

dhcp client update dns [**server** {**both** | **none**}]

L'ASA envoie les requêtes des clients DHCP au serveur DHCP. Notez que le serveur DHCP doit également être configuré pour prendre en charge DDNS. Le serveur peut être configuré pour répondre aux demandes du client ou il peut remplacer les commandes du client (auquel cas, il répondra au client pour que le client n'essaye pas également d'effectuer les mises à jour effectuées par le serveur). Même si le client ne demande pas de mises à jour DDNS, le serveur DHCP peut être configuré pour envoyer quand même des mises à jour.

Pour les adresses IP statiques ou PPPoE, ces paramètres sont ignorés.

Remarque
Vous pouvez également définir ces valeurs globalement pour toutes les interfaces à l'aide de la commande **dhcp-client update dns**. Les paramètres par interface prévalent sur les paramètres globaux.

- Par défaut (sans mot clé) : demande au serveur DHCP d'effectuer la mise à jour des RR PTR. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les enregistrements **ddns** A activés.
- **server both** : demande au serveur DHCP d'effectuer les mises à jour des enregistrements A et RR PTR. Ce paramètre ne nécessite pas l'association d'une méthode de mise à jour DDNS à l'interface.
- **server none** : demande au serveur DHCP de ne pas effectuer de mises à jour. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les enregistrements **ddns both** A et PTR activés.

Exemple :

```
ciscoasa(config-if)# ddns client update dns
```

Étape 4 La méthode Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Consultez Configurer les points de confiance.

Exemple :

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

Méthode DDNS standard pour une adresse IP statique

L'exemple suivant montre comment configurer la méthode DDNS standard pour une utilisation avec une adresse IP statique. Notez que vous ne configurez pas les paramètres du client DHCP pour ce scénario.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
 ddns both
interface gigabitethernet1/1
 ip address 209.165.200.225
! Associate the method with the interface:
 ddns update ddns-2
 ddns update hostname asa1.example.com
```

Exemple : méthode DDNS standard; mises à jour RR A de l'ASA et mises à jour RR PTR du serveur DHCP

L'exemple suivant configure l'ASA pour mettre à jour le RR A et le serveur DHCP pour mettre à jour le RR PTR.

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
 ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
  ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
  dhcp client update dns
```

Exemple : méthode DDNS standard; aucune mise à jour des RR du serveur DHCP

L'exemple suivant configure l'ASA pour mettre à jour le RR A et PTR, tout en demandant au serveur DHCP de mettre à jour les RR.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
```

```
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
  dhcp client update dns server none
```

Exemple : méthode DDNS standard; le serveur DHCP met à jour tous les RR

L'exemple suivant configure le client DHCP pour demander au serveur DHCP de mettre à jour les RR A et PTR. Étant donné que le serveur effectue toutes les mises à jour, il n'est pas nécessaire d'associer une méthode de mise à jour à l'interface.

```
interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
  dhcp client update dns server both
```

Exemple : type Web

L'exemple suivant configure la méthode du type Web.

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

Supervision des services DHCP et DDNS

Cette section comprend les procédures pour superviser les services DHCP et DDNS.

Supervision des services DHCP

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  Cette commande affiche les statistiques, l'état et la liaison du client du serveur DHCP actuel.

- **show dhcprelay** {**state** | **statistics**}

  Cette commande affiche l'état et les statistiques du relais DHCP.

- **show ipv6 dhcprelay binding**

  Cette commande affiche les entrées de liaison de relais qui ont été créées par l'agent de relais.

- **show ipv6 dhcprelay statistics**

  Cette commande affiche les statistiques de l'agent de relais DHCP pour IPv6.

- **show ipv6 dhcp server statistics**

  Cette commande affiche les statistiques du serveur sans état DHCPv6. L'exemple suivant montre les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]
- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  La commande **show ipv6 dhcp interface** affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6, à la page 9), cette commande répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cette commande affiche l'état de chaque client et les valeurs reçues du serveur. Pour une interface en particulier, vous pouvez afficher les statistiques des messages pour le serveur ou le client DHCP. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD
```

```
Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                 preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

La commande **show ipv6 dhcp ha statistics** affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités. Les exemples suivants montrent les renseignements fournis par cette commande.

Sur une unité active :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

Sur une unité de secours :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

Dépannage du relais DHCP sur VTI

Si le client DHCP ne parvient pas à obtenir une adresse IP :

- Vérifiez la configuration de l'interface de tunnel/VTI dans les deux sites ASA.
- Vérifiez les paquets transférés entre les sites à l'aide de la commande **show crypto ipsec sa** :

  Exemple

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

Activer les commandes de débogage

L'activation des débogages de relais DHCP vous aide à savoir si les paquets DISOVER/REQUEST ont été transférés vers le serveur de relais DHCP :

- **debug dhcprelay event 255**
- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

Exemple

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at 04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

Supervision de l'état DDNS

Consultez la commande suivante pour superviser l'état du DDNS.

- **show ddns update** {**interface** *if_name* | **method** [*name*]}

  Cette commande affiche l'état de la mise à jour du DDNS.

  L'exemple suivant montre les détails de la méthode de mise à jour du DDNS :

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  L'exemple suivant montre les détails de la méthode de mise à jour Web :

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

  L'exemple suivant montre les renseignements relatifs à l'interface DDNS :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

  L'exemple suivant montre une mise à jour de type Web réussie :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
```

```
IP addresses(s): 10.10.32.45,2001:DB8::1
```

L'exemple suivant montre une défaillance de type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

L'exemple suivant montre que le serveur DNS a renvoyé une erreur pour la mise à jour du type Web :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

L'exemple suivant montre qu'une mise à jour Web n'a pas encore été tentée en raison de l'adresse IP non configurée ou de l'échec de la requête DHCP, par exemple :

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

Historique des services DHCP et DDNS

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de DDNS pour la méthode de mise à jour Web	9.15(1)	Vous pouvez maintenant configurer une interface pour utiliser DDNS avec la méthode de mise à jour Web. Commandes nouvelles ou modifiées : **show ddns update interface**, **show ddns update method**, **web update-url**, **web update-type**
Prise en charge du serveur de relais DHCP sur les VTI	9.14(1)	Vous pouvez maintenant activer le relais DHCP sur les VTI. Commandes nouvelles ou modifiées : **dhcprelay server** .

Nom de la caractéristique	Versions de plateforme	Description
Réservation DHCP	9.13(1)	L'ASA prend en charge la réservation DHCP. Le serveur DHCP attribue une adresse IP statique à partir de l'ensemble d'adresses à un client DHCP en fonction de l'adresse MAC du client. Commandes nouvelles ou modifiées : **dhcpd reserve-address** .
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les commandes suivantes : **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address**
Supervision DHCPv6	9.4(1)	Vous pouvez maintenant superviser les statistiques DHCP pour IPv6 et les liaisons DHCP pour IPv6.
Le serveur de relais DHCP valide l'identifiant du serveur DHCP pour les réponses	9.2(4)9.3(3)	Si le serveur de relais DHCP ASA reçoit une réponse d'un serveur DHCP incorrect, il vérifie désormais que la réponse provient du bon serveur avant de donner suite à la réponse. Nous n'avons pas introduit ni modifié de commandes. Nous n'avons pas modifié d'écrans ASDM. Nous n'avons pas introduit ni modifié de commandes.
Fonction de liaison DHCP	9.1(4)	Pendant la phase de liaison DHCP, le client tente maintenant de se rétablir d'autres serveurs DHCP dans la liste des groupes du tunnel. Avant cette version, le client ne se reconnectait pas à un autre serveur lorsque le renouvellement du bail DHCP échouait. Nous n'avons pas introduit ni modifié de commandes.

Nom de la caractéristique	Versions de plateforme	Description
Interfaces de confiance DHCP	9.1(2)	Vous pouvez désormais configurer des interfaces en tant qu'interfaces de confiance pour conserver l'option 82 de DHCP. L'option 82 DHCP est utilisée par les commutateurs et les routeurs en aval pour la surveillance DHCP et la protection source IP. Normalement, si l'agent de relais DHCP ASA reçoit un paquet DHCP avec l'option 82 déjà définie, mais que le champ giaddr (qui spécifie l'adresse de l'agent de relais DHCP définie par ce dernier avant de transmettre le paquet au serveur) est réglé sur 0, l'ASA supprimera ce paquet par défaut. Vous pouvez désormais conserver l'option 82 et transférer le paquet en identifiant une interface comme interface de confiance. Nous avons introduit ou modifié les commandes suivantes : **dhcprelay information trusted**, **dhcprelay information trust-all**, **show running-config dhcprelay**.
Serveurs de relais DHCP par interface (IPv4 uniquement)	9.1(2)	Vous pouvez désormais configurer des serveurs de relais DHCP par interface, de sorte que les demandes qui entrent dans une interface donnée ne sont relayées que vers les serveurs spécifiés pour cette interface. IPv6 n'est pas pris en charge pour le relais DHCP par interface. Nous avons introduit ou modifié les commandes suivantes : **dhcprelay server** (mode de configuration d'interface), **clear configure dhcprelay**, **show running-config dhcprelay**.
Relais DHCP pour IPv6 (DHCPv6)	9.0(1)	La prise en charge des relais DHCP pour IPv6 a été ajoutée. Nous avons introduit les commandes suivantes : **ipv6 dhcprelay server**, **ipv6 dhcprelay enable**, **ipv6 dhcprelay timeout**, **clear config ipv6 dhcprelay**, **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**, **debug ipv6 dhcp**, **debug ipv6 dhcprelay**, **show ipv6 dhcprelay binding**, **clear ipv6 dhcprelay binding**, **show ipv6 dhcprelay statistics** et **clear ipv6 dhcprelay statistics**.
Système de nom de domaine dynamique (DDNS)	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **ddns**, **ddns update**, **dhcp client update dns**, **dhcpd update dns**, **show running-config ddns** et **show running-config dns server-group**.
DHCP (protocole de configuration dynamique des hôtes)	7.0(1)	L'ASA peut fournir un serveur DHCP ou des services de relais DHCP aux clients DHCP connectés aux interfaces ASA. Nous avons introduit les commandes suivantes : **dhcp client update dns**, **dhcpd address**, **dhcpd domain**, **dhcpd enable**, **dhcpd lease**, **dhcpd option**, **dhcpd ping timeout**, **dhcpd update dns**, **dhcpd wins**, **dhcp-network-scope**, **dhcprelay enable**, **dhcprelay server**, **dhcprelay setroute**, **dhcp-server**. **show running-config dhcpd** et **show running-config dhcprelay**.

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.