Dépannage de l'intégrité de la base de données de surveillance DHCP due à NTP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Topologie

Rôle de l'accessibilité NTP et NTP dans le remplissage de la base de données de surveillance DHCP

- 1. Problème de délai d'expiration du bail
- 2. Impact sur la sauvegarde de la table de liaison
- 3. Sauvegarde de base de données non fiable

Configuration de base

Scénario 1 - Serveur NTP inaccessible

Scénario 2 - Serveur NTP accessible

Scénario 3 - Serveur NTP accessible par intermittence

Conclusion

Introduction

Ce document décrit la relation entre NTP et la base de données de surveillance DHCP, mettant en évidence la synchronisation temporelle lors de l'enregistrement et de la restauration des liaisons DHCP.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Compréhension de base de :

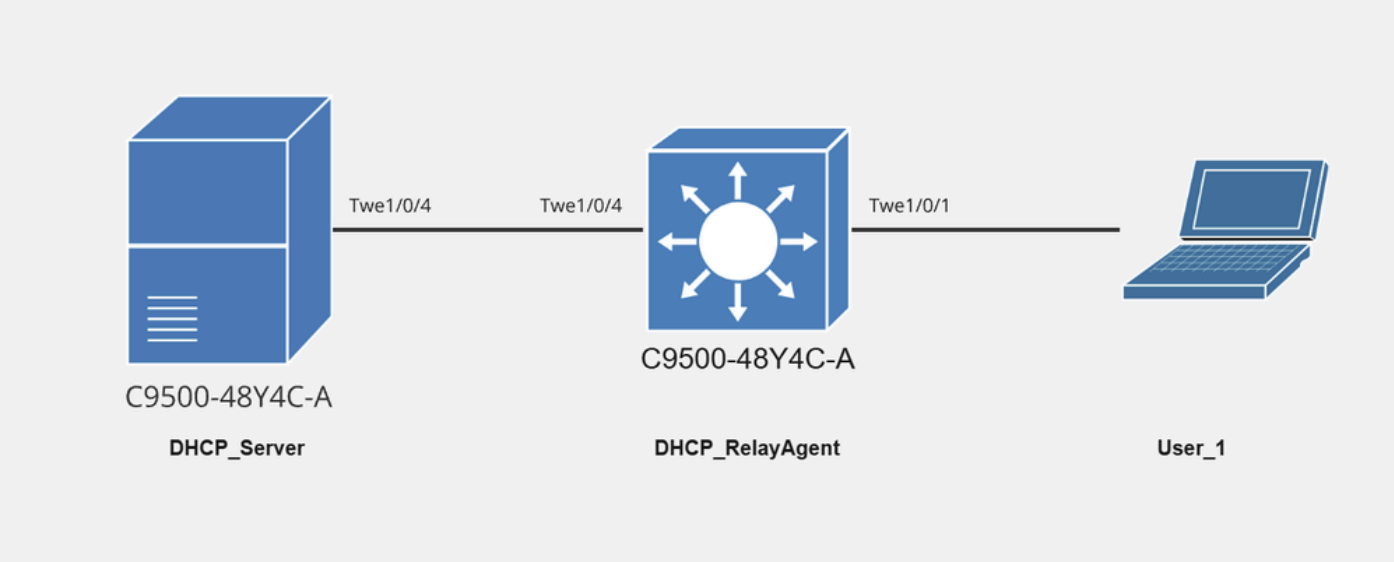
- Architecture de commutation Catalyst, série 9000
- Logiciel Cisco IOS® XE et ligne de commande
- DHCP (Dynamic Host Configuration Protocol), surveillance DHCP et fonctionnalités associées
- NTP (Network Time Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version 17.12.4 du logiciel Cisco Catalyst C9500 sur Cisco IOS®.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie



Diagramme_réseau avec User_1

Rôle de l'accessibilité NTP et NTP dans le remplissage de la base de données de surveillance DHCP

Dans un commutateur ou un périphérique réseau avec la surveillance DHCP activée, la table de liaison contient des informations dynamiques en temps réel sur les adresses IP, les adresses MAC, les VLAN et les délais d'expiration des baux. Ces informations sont essentielles pour vérifier les clients DHCP et protéger le réseau des serveurs DHCP non autorisés.

Cependant, la base de données de surveillance est généralement destinée à fournir une persistance pour ces informations, de sorte qu'elle peut être restaurée après un redémarrage. La base de données peut être sauvegardée régulièrement et les informations sont stockées dans un fichier persistant (par exemple, flash:backup.text).Pour que cette procédure de sauvegarde fonctionne correctement, une heure système exacte est nécessaire, en particulier pour les horodatages d'expiration de bail et d'autres données sensibles au temps.

Le protocole NTP est essentiel pour garantir une synchronisation précise de l'horloge système. Le système s'appuie sur le temps précis pour :

- Calculez l'expiration du bail pour les liaisons DHCP.
- Assurez-vous que les horodatages corrects sont écrits dans la base de données de surveillance lors de l'enregistrement de la table de liaison.

Si le serveur NTP est inaccessible ou si le système ne peut pas synchroniser son horloge, le système ne peut pas disposer d'une référence d'heure précise pour gérer correctement les horodatages d'expiration des baux DHCP. Cela entraîne les problèmes suivants :

1. Problème de délai d'expiration du bail

Un horodatage incorrect peut entraîner des problèmes tels que :

- Expiration ou renouvellement incorrects des baux.
- Informations de liaison DHCP obsolètes ou obsolètes dans la base de données de surveillance.

2. Impact sur la sauvegarde de la table de liaison

Lorsque le serveur NTP est accessible, le système peut générer des horodatages précis pour chaque bail DHCP et sauvegarder correctement la table de liaison dans la base de données de surveillance.

Si le serveur NTP n'est pas accessible, le périphérique ne parvient pas à déterminer l'heure actuelle correcte, ce qui entraîne 0 tentative d'écriture d'informations de liaison valides dans la base de données.

3. Sauvegarde de base de données non fiable

La base de données de surveillance stocke en permanence des informations de liaison, y compris le délai d'expiration de chaque bail.

Sans heure système précise du protocole NTP , le périphérique ne parvient pas à écrire des horodatages précis pour les expirations de bail lors de l'enregistrement dans la base de données.

Si le serveur NTP est accessible par intermittence, il en résulte un problème d'intégrité entre la table de liaison DHCP et la table de base de données de surveillance DHCP.Par conséquent, les données de la base de données de surveillance sont considérées comme incomplètes ou incorrectes.

Configuration de base

Étape 1 : activation de la surveillance DHCP globalement et sous les VLAN, sur l’agent de relais Dans ce cas, l'agent de relais et le commutateur d'accès sont identiques.

```
DHCP_RelayAgent#configure terminal
DHCP_RelayAgent(config)#ip dhcp snooping
DHCP_RelayAgent(config)#ip dhcp snooping vlan 10
```

Étape 2 : configuration de l’approbation de surveillance DHCP sur toutes les interfaces du

commutateur qui reçoivent des offres DHCP de serveurs DHCP authentiques Le nombre de ces interfaces dépend de la conception du réseau et de l'emplacement des serveurs DHCP. Ce sont les interfaces qui vont vers le serveur DHCP authentique.

<#root>

DHCP_RelayAgent# show running-configuration interface TwentyFiveGigE1/0/4

```
Building configuration...
Current configuration : 84 bytes
!
interface TwentyFiveGigE1/0/4
 switchport mode trunk
 ip dhcp snooping trust
end
```

Étape 3 : configuration de la base de données de surveillance DHCP à un emplacement pour surveiller la table de liaison de surveillance DHCP, suivi de l'état des opérations de base de données et vérification de la mise à jour et du transfert corrects de la base de données

<#root>

```
DHCP_RelayAgent#configure terminal
DHCP_RelayAgent(config)#ip dhcp snooping database bootflash:dhcpsnoopingdatabase.txt
DHCP_RelayAgent(config)#ip dhcp snooping database timeout 300
DHCP_RelayAgent(config)#ip dhcp snooping database write-delay 15
```

DHCP_RelayAgent#show running-configuration | include database

```
ip dhcp snooping database bootflash:dhcpsnoopingdatabase.txt
ip dhcp snooping database write-delay 15
```

Scénario 1 - Serveur NTP inaccessible

<#root>

DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
……
```

Success rate is 0 percent (0/0)

Maintenant, nous pouvons voir que l'utilisateur 1 a reçu l'adresse IP 10.10.10.1 dans le VLAN 10.

Voici la table de liaison de surveillance DHCP, qui indique l'adresse IP, l'adresse MAC et l'interface de User_1 sur TwentyFiveGigE1/0/1

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress        Lease(sec)    Type           VLAN   Interface
------------------  ---------------  ----------   --------------  ----   --------------------
78:BC:1A:0B:D5:1F   10.10.10.1       86372        dhcp-snooping   10     TwentyFiveGigE1/0/1

Total number of bindings: 1
```

En général, une fois que l'utilisateur reçoit une adresse IP, la table de liaison de surveillance est créée dynamiquement, et les informations correspondantes sont ensuite ajoutées à la base de données de surveillance. Mais, dans ce cas, comme le serveur NTP est inaccessible, il y a eu 0 tentatives totales de mise à jour ou de transfert des informations de liaison vers la base de données.

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

```
Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : 18:37:38 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.
```

Total Attempts : 0

```
         Startup Failures : 0
```

Successful Transfers : 0

```
   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0
```

Successful Writes : 0

```
      Failed Writes : 0
Media Failures : 0
```

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

```
%Error opening bootflash:dhcpsnoopingdatabase.txt (No such file or directory)
```

<#root>

```
*Mar 18 11:12:21.264: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Vl
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of option 82, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x1 0x2 0x8 0x0 0x6 0x78 0xBC 0x1A 0xB 0xC2 0x60
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x1
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x78 0xBC 0x1A 0xB 0xC2 0x60
*Mar 18 11:12:21.264: actual_fmt_cid OPT82_FMT_CID_VLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_RID
*Mar 18 11:12:21.264: DHCP_SNOOPING: opt82 data indicates local packet
*Mar 18 11:12:21.264: DHCP_SNOOPING: opt82 data indicates local packet
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: add binding on port TwentyFiveGigE1/0/1 ckt_id 0 TwentyFiveGigE1/0/
*Mar 18 11:12:21.264: DHCP_SNOOPING: dhcp binding entry already exists, update binding lease time to (86

*Mar 18 11:12:21.264: ipaddr: 10.10.10.1, hwidb: TwentyFiveGigE1/0/1, type: 1, phyidb: TwentyFiveGigE1/0

*Mar 18 11:12:21.264: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Mar 18 11:12:21.264: DHCP_SNOOPING: remove relay information option.
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: calling forward_dhcp_reply
*Mar 18 11:12:21.264: platform lookup dest vlan for input_if: Vlan10, is NOT tunnel, if_output: Vlan10,
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan 10 after pvlan check
*Mar 18 11:12:21.264: DHCP Memory dump is printed for direct forward reply

765DFA772750: FFFF FFFFFFFF 78BC1A0B C2FF0800
765DFA772760: 4500015E 00230000 FF11A64E 0A0A0A14
765DFA772770: FFFFFFFF 00430044 014A36A8 02010600
765DFA772780: BAF1E48A 00008000 00000000 0A0A0A01
765DFA772790: 00000000 0A0A0A14 78BC1A0B D51F0000
765DFA7727A0: 00000000 00000000 00000000 00000000
765DFA7727B0: 00000000 00000000 00000000 00000000
765DFA7727C0: 00000000 00000000 00000000 00000000
765DFA7727D0: 00000000 00000000 00000000 00000000
765DFA7727E0: 00000000 00000000 00000000 00000000
765DFA7727F0: 00000000 00000000 00000000 00000000
765DFA772800: 00000000 00000000 00000000 00000000
```

```
765DFA772810: 00000000 00000000 00000000 00000000
765DFA772820: 00000000 00000000 00000000 00000000
765DFA772830: 00000000 00000000 00000000 00000000
765DFA772840: 00000000 00000000 00000000 00000000
765DFA772850: 00000000 00000000 00000000 00000000
765DFA772860: 00000000 00000000 63825363 3501053D
765DFA772870: 1A006369 73636F2D 37386263 2E316130
765DFA772880: 622E6435 31662D56 6C313036 040A0A0A
765DFA772890: 0A330400 0151803A 040000A8 C03B0400
765DFA7728A0: 01275001 04FFFFFF 00FF0000 00000000
765DFA7728B0: 00000000 00000000 00000000 00FF
*Mar 18 11:12:21.273: DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/1.
```

***Mar 18 11:12:38.546: Write delay timer expired**

***Mar 18 11:12:38.546: Restarting write delay timer.**

***Mar 18 11:13:38.546: Write delay timer expired**

***Mar 18 11:13:38.546: Restarting write delay timer.**

***Mar 18 11:14:08.547: Write delay timer expired**

***Mar 18 11:14:08.547: Restarting write delay timer.**

```
*Mar 18 11:14:14.266: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.110.129.206)
```

Scénario 2 - Serveur NTP accessible

<#root>

DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 175/175/176 ms

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress        Lease(sec)    Type          VLAN   Interface
------------------  ---------------  ----------   -------------  ----   --------------------
```

```
78:BC:1A:0B:D5:1F   10.10.10.1      86372       dhcp-snooping  10     TwentyFiveGigE1/0/1

Total number of bindings: 1
```

Une fois que l'utilisateur a reçu une adresse IP, la table de liaison de surveillance est créée dynamiquement et les informations correspondantes sont ensuite ajoutées à la base de données de surveillance. Par conséquent, il y a eu 1 tentative totale de mise à jour ou de transfert de la base de données, toutes ayant réussi. Il n'y a eu aucun échec d'écriture, de lecture ou de transfert.

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping database


Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:39:27 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.


Total Attempts : 1

         Startup Failures : 0

Successful Transfers : 1

   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0

Successful Writes : 1

      Failed Writes : 0
Media Failures : 0
```

<#root>

```
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt


67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
```

```
10.10.10.1    10    78bc.1a0b.d51f    67D9BBCA    Twe1/0/1    8b21f6ef

END
```

Scénario 3 - Serveur NTP accessible par intermittence

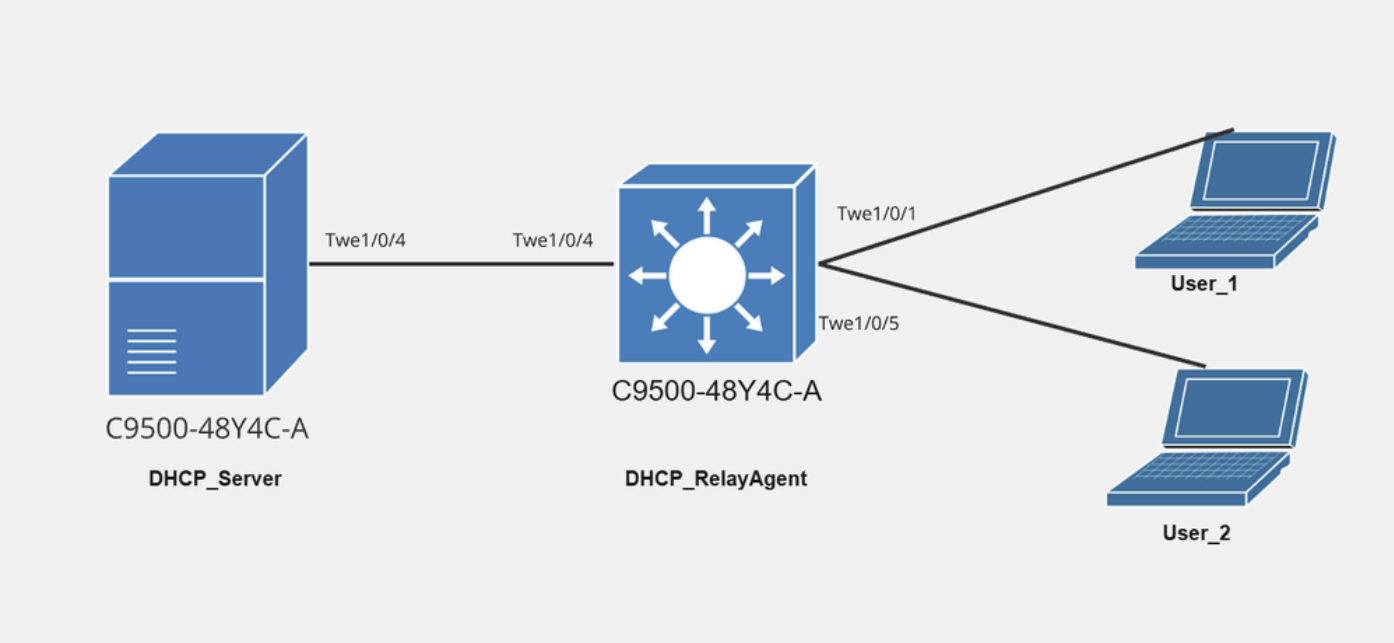


Schéma de réseau avec User_1 et User_2

<#root>

```
DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 175/175/176 ms
```

Maintenant, nous pouvons voir que l'utilisateur 1 a reçu l'adresse IP 10.10.10.1 dans le VLAN 10.

Voici la table de liaison de surveillance DHCP, qui indique l'adresse IP, l'adresse MAC et l'interface de User_1 sur TwentyFiveGigE1/0/1

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
```

78:BC:1A:0B:D5:1F 10.10.10.1 86372 dhcp-snooping 10 TwentyFiveGigE1/0/1

Total number of bindings: 1

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:40:20 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 1

Startup Failures : 0

Successful Transfers : 1

Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0

Successful Writes : 1

Failed Writes : 0
Media Failures : 0

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1 10 78bc.1a0b.d51f 67D9BBCA Twe1/0/1 8b21f6ef

END

Au bout d'un moment, le NTP est devenu inaccessible, mais User_2 a obtenu son adresse IP

10.10.10.2 dans le VLAN 10 et il a été mis à jour dans la table de liaison, mais pas dans la table de base de données de surveillance.

<#root>

DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
……
```

Success rate is 0 percent (0/0)

Voici la table de liaison de surveillance DHCP, qui indique l'adresse IP, l'adresse MAC et l'interface pour User_2 sur TwentyFiveGigE1/0/5

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress        Lease(sec)   Type           VLAN   Interface
------------------  ---------------  ----------   -------------  ----   --------------------
```

78:BC:1A:0B:D5:1F   10.10.10.1   86217   dhcp-snooping 10   TwentyFiveGigE1/0/1

F8:E5:7E:75:04:46   10.10.10.2   85336   dhcp-snooping 10   TwentyFiveGigE1/0/5

```
Total number of bindings: 2
```

L'entrée de la base de données de surveillance n'est pas incrémentée et le nombre total d'écritures réussies reste égal à 1.

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

```
Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running
```

```
Last Succeded Time : 18:41:38 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.


Total Attempts : 1

         Startup Failures : 0


Successful Transfers : 1

   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0


Successful Writes : 1

      Failed Writes : 0
Media Failures : 0
```

<#root>

```
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt


67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1  10  78bc.1a0b.d51f  67D9BBCA  Twe1/0/1  8b21f6ef


END
```

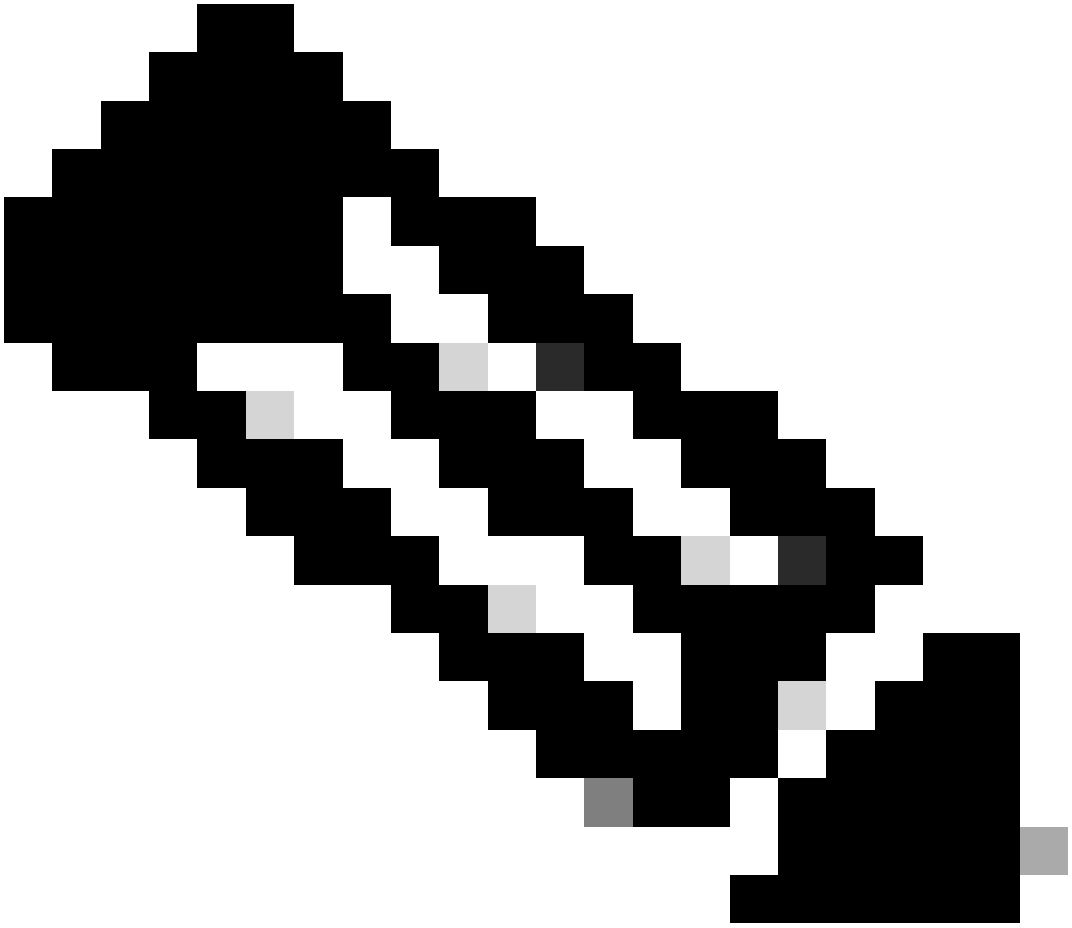
Lorsque le serveur NTP devient accessible, le système synchronise la table de liaison de surveillance DHCP et la base de données de surveillance DHCP. Ce scénario n'est pas illustré ici. Cependant, des résultats similaires peuvent être obtenus en supprimant la configuration du serveur NTP.

Une fois la configuration NTP supprimée, l'entrée pour User_2 est ajoutée à la table de base de données de surveillance.
Dans ce cas, le commutateur utilise l'heure d'horloge du système.

<#root>

```
DHCP_RelayAgent#configure terminal

DHCP_RelayAgent(config)# no ntp server 10.81.254.131
```



Remarque : À des fins de démonstration, nous avons supprimé la configuration du serveur NTP.Techniquement, le résultat du serveur NTP accessible et du serveur NTP non configuré est similaire.

```
*Mar 17 17:26:26.475: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expir
*Mar 17 17:26:26.486: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Write succeeded
```

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress           IpAddress        Lease(sec)   Type            VLAN   Interface
------------------   ---------------  ----------   -------------   ----   --------------------
```

78:BC:1A:0B:D5:1F   10.10.10.1   86217   dhcp-snooping   10   TwentyFiveGigE1/0/1

F8:E5:7E:75:04:46 10.10.10.2 85336 dhcp-snooping 10 TwentyFiveGigE1/0/5

Total number of bindings: 2

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:42:16 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 2

Startup Failures : 0

Successful Transfers : 2

Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0

Successful Writes : 2

Failed Writes : 0
Media Failures : 0

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1 10 78bc.1a0b.d51f 67D9BBCA Twe1/0/1 8b21f6ef

10.10.10.2 10 f8e5.7e75.0446 67D9B6DC Twe1/0/5 bef43442

END

<#root>

```
*Mar 18 11:36:38.283: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Mar 18 11:36:38.283: DHCP_SNOOPING: remove relay information option.
*Mar 18 11:36:38.283: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:36:38.283: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/5 found for f8e5.7e75.0446
*Mar 18 11:36:38.283: DHCP_SNOOPING: calling forward_dhcp_reply
*Mar 18 11:36:38.283: platform lookup dest vlan for input_if: Vlan10, is NOT tunnel, if_output: Vlan10,
*Mar 18 11:36:38.283: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:36:38.283: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/5 found for f8e5.7e75.0446
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan 10 after pvlan check
*Mar 18 11:36:38.283: DHCP Memory dump is printed for direct forward reply
765DFA80B990: FFFF FFFFFFFF 78BC1A0B C2FF0800
765DFA80B9A0: 4500015E 002B0000 FF11A646 0A0A0A14
765DFA80B9B0: FFFFFFFF 00430044 014A51AD 02010600
765DFA80B9C0: ED9296E4 00008000 00000000 0A0A0A01
765DFA80B9D0: 00000000 0A0A0A14 78BC1A0B D51F0000
765DFA80B9E0: 00000000 00000000 00000000 00000000
765DFA80B9F0: 00000000 00000000 00000000 00000000
765DFA80BA00: 00000000 00000000 00000000 00000000
765DFA80BA10: 00000000 00000000 00000000 00000000
765DFA80BA20: 00000000 00000000 00000000 00000000
765DFA80BA30: 00000000 00000000 00000000 00000000
765DFA80BA40: 00000000 00000000 00000000 00000000
765DFA80BA50: 00000000 00000000 00000000 00000000
765DFA80BA60: 00000000 00000000 00000000 00000000
765DFA80BA70: 00000000 00000000 00000000 00000000
765DFA80BA80: 00000000 00000000 00000000 00000000
765DFA80BA90: 00000000 00000000 00000000 00000000
765DFA80BAA0: 00000000 00000000 63825363 3501053D
765DFA80BAB0: 1A006369 73636F2D 37386263 2E316130
765DFA80BAC0: 622E6435 31662D56 6C313036 040A0A0A
765DFA80BAD0: 0A330400 0151803A 040000A8 C03B0400
765DFA80BAE0: 01275001 04FFFFFF 00FF0000 00000000
765DFA80BAF0: 00000000 00000000 00000000 00FF
*Mar 18 11:36:38.291: DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/5.
*Mar 18 11:37:25.795: DHCP_SNOOPING: checking expired snoop binding entries
*Mar 18 11:37:36.694: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.110.129.206)
*Mar 18 11:37:38.956: DHCPD: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:38.956: DHCPD: Sending notification of DISCOVER:
*Mar 18 11:37:38.956: DHCPD: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:38.956: DHCPD: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:38.956: DHCPD: interface = GigabitEthernet0/0
*Mar 18 11:37:38.956: DHCPD: class id 436973636f204e394b2d433933333243
*Mar 18 11:37:38.956: DHCPD: FSM state change INVALID
*Mar 18 11:37:38.956: DHCPD: Workspace state changed from INIT to INVALID
*Mar 18 11:37:39.957: DHCPD: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:39.957: DHCPD: Sending notification of DISCOVER:
*Mar 18 11:37:39.957: DHCPD: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:39.957: DHCPD: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:39.957: DHCPD: interface = GigabitEthernet0/0
*Mar 18 11:37:39.957: DHCPD: class id 436973636f204e394b2d433933333243
```

```
*Mar 18 11:37:39.957: DHCPD: FSM state change INVALID
*Mar 18 11:37:39.957: DHCPD: Workspace state changed from INIT to INVALID
*Mar 18 11:37:50.819: Write delay timer expired
*Mar 18 11:37:50.819: Restarting write delay timer.
*Mar 18 11:37:50.819: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expir
*Mar 18 11:37:50.827: to string : 10.10.10.1 10 78bc.1a0b.d51f 67DAAC45 Twe1/0/1
*Mar 18 11:37:50.827: to string : 10.10.10.2 10 f8e5.7e75.0446 67D9B6DC Twe1/0/5
*Mar 18 11:37:50.832: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Write succeeded
*Mar 18 11:37:50.832: Resetting fail log parameters.
```

Conclusion

- Si l'adresse IP du serveur NTP est présente et accessible, la table de liaison de surveillance DHCP et la base de données de surveillance sont renseignées. Les entrées doivent être horodatées avec précision à l'aide de l'heure synchronisée du serveur NTP.
- Si l'adresse IP du serveur NTP est présente mais inaccessible, la table de liaison de surveillance DHCP est toujours renseignée, mais les entrées ne peuvent pas être renseignées dans la base de données de surveillance, car le système ne peut pas synchroniser l'heure pour une gestion précise des baux.
- Si l'adresse IP du serveur NTP n'est pas configurée ou n'existe pas, la table de liaison de surveillance DHCP et la base de données de surveillance contiennent toujours des entrées, mais les horodatages de la base de données de surveillance ne sont pas fiables, car ils peuvent être basés sur l'heure du système local.
- En résumé, pour une gestion précise et fiable de la base de données de surveillance DHCP, le protocole NTP est essentiel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.