Configurer les contrôleurs sans fil Catalyst 9800 du client en mode haute disponibilité du basculement dynamique (SSO, pour Stateful Switch Over) dans IOS-XE 16.12

Table des matières

Introduction Informations générales Restrictions Conditions préalables Exigences Composants utilisés Configurer la haute disponibilité sur un contrôleur LAN sans fil 9800 matériel Diagramme du réseau Configurations Configuration de la haute disponibilité sur les WLC 9800 virtuels Diagramme du réseau Configurations Configurer le réseau de redondance virtuel Définir la configuration à haute disponibilité Activer lâ€[™]accès à la console du contrôleur LAN sans fil 9800 de secours Forcer le basculement Rompre la haute disponibilité Effacer la configuration à haute disponibilité des deux contrôleurs LAN sans fil 9800 Configurer le délai dâ€[™]expiration des pairs Mise à niveau Vérifier Dépannage

Introduction

Ce document décrit comment configurer les contrôleurs sans fil Catalyst 9800 en haute disponibilité (HA) SSO dans Cisco IOS® XE 16.10 à 16.12.

Informations générales

Dans Cisco IOS XE® 17.x et versions ultérieures pour le Catalyst 9800. Cet article de document se concentre sur HA SSO dans les versions 16.x.

Le concept d'interface de gestion de la redondance ajoute un certain nombre de différences qui sont couvertes par le guide dédié,

Guide de déploiement SSO haute disponibilité pour les contrôleurs sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE Amsterdam 17.

La redondance expliquée dans cet article est 1:1, ce qui signifie que l'une des unités fonctionne à l'état Actif tandis que l'autre fonctionne à l'état Hot Standby.

Si le boîtier actif est détecté comme inaccessible, l'unité de secours automatique devient active et tous les points d'accès et clients maintiennent leur service via la nouvelle unité active.

Une fois les deux unités synchronisées, le WLC 9800 en veille imite sa configuration avec l'unité principale.

Toute modification de configuration effectuée sur l'unité active est répliquée sur l'unité en veille via le port de redondance (RP).

Il nâ€[™]est plus permis dâ€[™]effectuer des modifications de la configuration sur le contrôleur LAN sans fil 9800 de secours.

Outre la synchronisation de la configuration entre les boîtes, elles synchronisent également :

- AP à l'état UP (pas AP à l'état download ou AP dans la connexion DTLS)
- Clients à l'état EXÉCUTÉ (si un client est à l'état requis pour l'authentification Web et qu'un basculement se produit, ce client doit redémarrer son processus d'association),
- configuration RRM
- (autres paramètres)

Restrictions

Avant d'activer la haute disponibilité entre deux WLC 9800, effectuez les validations suivantes :

- Les deux périphériques doivent avoir le même identifiant de produit (PID). Dans le cas du 9800-CL, assurez-vous que l'environnement hôte (ESXi, KVM ou ENCS) est le même pour les deux instances.
- Les deux périphériques doivent exécuter la même version du logiciel.
- Les deux périphériques doivent s'exécuter dans le même mode d'installation (Bundle ou Install). Nous recommandons le mode d'installation pour WLC.
- Les deux périphériques doivent avoir des adresses IP redondantes dans le même sous-réseau. Les adresses IP utilisées pour la redondance doivent être non routables sans passerelle présente dans le sous-réseau.
- Les deux périphériques doivent disposer d'une interface de gestion sans fil unique.
- Lâ€[™]interface de gestion sans fil des deux appareils doit se trouver sur le même réseau local virtuel (VLAN) ou sous-réseau.
- Dans le cas du 9800-CL,
 - Vérifiez que les mêmes ressources de processeur, de mémoire et de stockage sont allouées aux deux instances.
 - Vérifiez que lâ€[™]instantané de la machine virtuelle (VM) est désactivé pour les deux instances;
 - Les deux périphériques doivent utiliser le même numéro d'interface (par exemple : GigabitEthernet3) pour la haute disponibilité

Conditions préalables

Exigences

Cisco recommande de connaître le fonctionnement de base du WLC 9800.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Contrôleur LAN sans fil 9800-CL virtuel, versions 16.10 à 16.12

• Contrôleur LAN sans fil 9800-40, versions 16.10 à 16.12

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 lâ€TMincidence possible des commandes.

Configurer la haute disponibilité sur un contrôleur LAN sans fil 9800 matériel

Diagramme du réseau

Le présent document se fonde sur la topologie suivante :



Configurations

La redondance SSO est activée par défaut, mais la configuration de la communication entre les unités est toujours requise.

Avant de configurer une étape, assurez-vous que les deux boîtes exécutent la même version.

Étape 1. Connectez les WLC 9800 au réseau et assurez-vous qu'ils sont accessibles les uns par les autres.

L'interface de gestion sans fil des deux boîtiers doit se trouver sur le même VLAN et le même sousréseau.

Étape 2. Connectez le port RP en respectant la topologie du réseau. Il y a deux options pour connecter 9800 WLC RP :

- RP Port Ethernet de redondance RJ45 10/100/1000
- RP Port SFP 10-GE



Remarque : dans Cisco IOS® XE 16.10 à 16.12, il est recommandé de connecter le port de redondance 9800s au même commutateur où la connexion de gestion du 9800 est connectée (voir topologie du réseau). Cela est dû au fait qu'il n'y a aucune vérification de l'accessibilité de la passerelle dans ces versions. Une connexion dos à dos fonctionne mais augmente les chances des contrôleurs 9800 de devenir actifs-actifs lorsqu'ils sont connectés de cette manière. Notez que le port RP n'utilise pas l'étiquetage vlan.

Étape 3. Attribuez lâ€[™]adresse IP de redondance aux deux contrôleurs LAN sans fil 9800.

IUG:

Naviguez jusqu'à Administration > Device > Redundancy. Décocher Clear Redundancy Config et saisissez l'adresse IP souhaitée.

Les deux unités doivent avoir des adresses IP uniques et appartenir au même sous-réseau.

Ce sous-réseau ne peut être routé nulle part sur le réseau.

Contrôleur LAN sans fil 9800 1

Q. Search Menu Items	Device		
🔜 Dashboard	General	Clear Redundancy Config	
Monitoring	FTP/TFTP	Local IP*	203.0.113.1
🔧 Configuration 🛛 🔿	Wireless	Netmask*	255.255.255.0
() Administration >	Redundancy	Remote IP*	203.0.113.2
		Peer Timeout State*	Default 🔻
* Troubleshooting		Redundancy Mode	○ None O SSO
		Active Chassis Priority*	1
			Apply to Device

Contrôleur LAN sans fil 9800 2

Q Search Menu Items	Device			
Dashboard	General	Clear Redundancy Config		
Monitoring >	FTP/TFTP	Local IP*	203.0.113.2	
🖏 Configuration 💦 🔸	Wireless	Netmask*	255.255.255.0	
🏠 Administration 🛛 →	Redundancy	Remote IP*	203.0.113.1	
		Peer Timeout State*	Default +	
Troubleshooting		Redundancy Mode	None SSO	
		Active Chassis Priority*	1	
				Apply to Device



16.10

9800 WLC-1# chassis ha-interface local-ip <!--IP address--> remote-ip <!--IP address-->
9800 WLC-2# chassis ha-interface local-ip <!--IP address--> remote-ip <!--IP address-->
16.11
9800 WLC-1# chassis redundancy ha-interface local-ip <!--IP address--> remote-ip <!--IP address-->
9800 WLC-2# chassis redundancy ha-interface local-ip <!--IP address--> remote-ip <!--IP address-->

Pour spécifier l'unité qui doit être le WLC 9800 actif, définissez la priorité du châssis par GUI ou CLI. L'unité ayant la priorité la plus élevée est sélectionnée comme unité principale.

IUG:

Q. Search Menu Items	Device		
Dashboard	General	Clear Redundancy Config	
Monitoring >	FTP/TFTP	Local IP*	203.0.113.2
🔧 Configuration 💦 👌	Wireless	Netmask*	255.255.255.0
Administration	Redundancy	Remote IP*	203.0.113.1
All Tranklashashas		Peer Timeout State*	Default v
		Redundancy Mode	O None O SSO
		Active Chassis Priority*	1

CLI:

```
# chassis 1 priority <1-15>
16.11
# chassis 1 priority <1-2>
```

Si une unité spécifique n'est pas sélectionnée pour être active, les unités sélectionnent Active en fonction de l'adresse MAC la plus basse

Vérifiez la configuration actuelle à l'aide de cette commande :

```
# show chassis ha-status local
              My state = ACTIVE
            Peer state = DISABLED
     Last switchover reason = none
      Last switchover time = none
           Image Version = ...
Chassis-HA Local-IP Remote-IP MASK HA-Interface
_____
This Boot:
Next Boot: 203.0.113.2 <!--IP address--> <!--IP address-->
Chassis-HA Chassis# Priority
                         IFMac Address Peer Timeout
_____
        1
This Boot:
                                           0
Next Boot: 1
                                           0
```

Étape 4. Enregistrez les configurations sur les deux contrôleurs LAN sans fil 9800.

IUG:



CLI:

write

Étape 5. Redémarrez les deux unités en même temps

IUG:

Naviguez jusqu'à Administration > Management > Backup & Restore > Reload

Q. Search Menu Items	Backup & Restore
Dashboard	Config File Management Reload
Monitoring >	 Save Configuration and Reload.
\sim Configuration \rightarrow	 Reload without Saving Configuration.
Administration	 Reset to Factory Default and Reload.
X Troubleshooting	 Apply to Device

CLI:

reload

Configurer la haute disponibilité sur un contrôleur LAN sans fil 9800 virtuel

Diagramme du réseau

Le présent document se fonde sur la topologie suivante :



Configurations

Configurer le réseau de redondance virtuel

Étape 1. Ouvrez votre client vCenter et accédez à Host > Configuration > Networking > Add Networking...

🖉 vCenter - vSphere Client		- 0
File Edit View Inventory Administration Plug-ins Help Image: State of the state of	sters	Search Inventory
Center DIGITAL-TOOL MEX-Wireless	10.88.173.65 VHware ESXI, 5.5.0, 2068 Getting Started Summary Virtual Macl Hardware Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings	190 hines Resource Allocation Performance Configuration Tasks 8 View: vSphere Standard Switch vSphere Distributed Switch Networking Refresh Add Networking Prope Group (Group) (s) VLAN ID: 2601

Étape 2. Sélectionner Virtual Machine et cliquez sur Next.

Add Network Wizard		-		×
Connection Type Networking hardware	can be partitioned to accommodate each service that requires connectivity.			
Connection Type Network Access Connection Settings Summary	Connection Types • Virtual Machine Add a labeled network to handle virtual machine network traffic. • VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iS and host management.	CSI, NF	s,	
Help	< Back Next >		Cano	el

Étape 3. Sélectionner Create a vSphere standard switch et cliquez sur Next.

Create a vSphere standard switch Speed Corporation 82599EB 10-Gigabit SFI/S Wmnic3 10000 Wmnic2 10000	d Networks d Networks SFP+ Network Connection
Use vSwitch0 Speed Intel Corporation 82599EB 10-Gigabit SFI/S wmnic3 10000 Wmnic2 10000	d Networks SFP+ Network Connection
Intel Corporation 82599EB 10-Gigabit SFI/S Image: Second secon	SFP+ Network Connection
vmnic3 10000	
🗌 🖷 vmnic2 10000	0 Full
	0 Full
C Use vSwitch1 Speed	d Networks
Intel Corporation I350 Gigabit Network Con	nnection
🗌 📟 vmnic1 1000 F	Full None
1 🔽 🛤 vmnic0 1000 F	Full 0.0.0.1-255.255.255.254 (VI AN 210)
Preview:	
Virtual Machine Port Group Physical Ad	dapters
	oters

Étape 4. Vous pouvez également personnaliser le Network Label paramètre. Après cela, cliquez sur Next.

Add Network Wizard Virtual Machines - Conne Use network labels to id	ection Settings lentify migration compatible connect	ions common to two or more hosts.		-		×
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional):	Redundancy Network	•			
	Preview: Virtual Machine Port Group Redundancy Network	Physical Adapters				
Help			< Back	Next >	Can	ncel

Étape 5. Cliquez sur Finish (terminer) pour fermer l'assistant.

Add Network Wizard Ready to Complete Verify that all new and	modified vSphere standard switches are configured appropriately.	-		×
Connection Type Network Access Connection Settings Summary	Host networking will include the following new and modified standard switches: Preview: Virtual Machine Port Group Physical Adapters Redundancy Network No adapters			
Help	< Back	Finish	Cano	el

Étape 6. Reliez une interface de chacun des deux contrôleurs LAN sans fil 9800 virtuels au réseau de redondance.

Cliquez avec le bouton droit sur le WLC virtuel 9800 et cliquez sur Edit Settings...



Sélectionnez l'une des cartes réseau disponibles et attribuez-la à la Redundancy Network, puis cliquez sur OK.

🚱 eWLC-2 - Virtual Machine Prope	rties	– 🗆 ×
Hardware Options Resources		Virtual Machine Version: vmx-10
Show All Devices	Add Remove	Device Status
Hardware	Summary	✓ Connect at power on
 Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 CD/DVD drive 2 Hard disk 1 Network adapter 1 Network adapter 2 Network adapter 3 	8192 MB 4 Video card Restricted Paravirtual [datastore1] eWLC-karlc [datastore1] eWLC-karlc Virtual Disk Trunk vlan2601 Redundancy Network	Adapter Type Current adapter: VMXNET 3 MAC Address 00:0c:29:41:1c:9c Automatic C Manual DirectPath I/O Status: Inactive 1 To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory. Network Connection Network label: Redundancy Network Port: N/A Switch to advanced settings

Faites de même pour les deux machines.



Définir la configuration à haute disponibilité

Avant d'effectuer une autre configuration, assurez-vous que l'interface de gestion sans fil des deux unités appartient au même VLAN et au même sous-réseau et qu'elle est accessible l'une à l'autre.

Vérifiez que les deux boîtes exécutent la même version.

Étape 1. Attribuez lâ€[™]adresse IP de redondance aux deux contrôleurs LAN sans fil 9800.

IUG:

Naviguez jusqu'à Administration > Device > Redundancy. Décocher Clear Redundancy Config et saisissez l'adresse IP souhaitée.

Vérifiez que les deux ont une adresse IP unique et que les deux unités appartiennent au même sous-réseau.

Contrôleur LAN sans fil 9800 1

Q. Search Menu Items	Device		
📰 Dashboard	General	Clear Redundancy Config	
Monitoring >	FTP/TFTP	Local IP*	203.0.113.1
🔧 Configuration 💦 👌	Wireless	Netmask*	255.255.255.0
Administration >	Redundancy	HA Interface	GigabitE v GigabitEthernet1
X Troubleshooting		Remote IP* Peer Timeout State* Redundancy Mode Active Chassis Priority*	GigabitEthernet2 GigabitEthernet3 None SSO 1 1

Contrôleur LAN sans fil 9800 2

Dashboard	General	Clear Redundancy Config	
Monitoring >	FTP/TFTP	Local IP*	203.0.113.2
🔾 Configuration >	Wireless	Netmask*	255.255.255.0
(Ô) Administration →	Redundancy	HA Interface	GigabitE •
¥ Troubleshooting		Remote IP*	203.0.113.1
		Peer Timeout State*	Default
		Redundancy Mode	None OSSO
		Active Chassis Priority*	1
			Apply to Device

Remarque : Notez que **GigabitEthernet3 a été sélectionné pour l'interface HA.** C'est parce que la troisième interface de la machine virtuelle est celle associée au réseau de redondance. Cette interface est utilisée pour activer la communication entre les deux boîtiers avant le démarrage de Cisco IOS, le transport des messages de contrôle haute disponibilité (tels que la sélection des rôles, les messages de maintien de la connexion, etc.) et fournir le transport pour la communication interprocessus (IPC) entre les deux boîtiers.

CLI 16.10 :

9800 WLC-1# chassis ha-interface gigabitEthernet 3 local-ip <!--IP address--> remote-ip <!--IP address--> 9800 WLC-2# chassis ha-interface gigabitEthernet 3 local-ip <!--IP address--> remote-ip <!--IP address-->

CLI 16.12 :

```
9800WLC1# chassis redundancy ha-interface g3 local-ip <!--IP address--> remote-ip <!--IP address-->
9800WLC2# chassis redundancy ha-interface g3 local-ip <!--IP address--> remote-ip <!--IP address-->
```

Remarque : une fois que l'interface GigabitEthernet 3 est sélectionnée pour être utilisée comme HA et que l'unité est redémarrée (même si HA n'est pas construit entre deux WLC 9800), vous ne voyez plus cette interface répertoriée dans le résultat de **show ip interface brief** or any other command that shows the 9800 WLC's interfaces, this is because that interface is now marked for HA only.

Étape 2. (Facultatif) Pour spécifier manuellement la case qui doit être le WLC 9800 actif, définissez la Active Chassis Prioritysoit par interface graphique utilisateur, soit par CLI.

Le châssis ayant la priorité la plus élevée est sélectionné comme châssis principal.

IUG:



CLI:

chassis 1 priority <1-15>

Si une unité spécifique à activer n'est pas spécifiée, les cases choisissent laquelle est le WLC 9800 actif principal.

Étape 3. Enregistrez les configurations sur les deux contrôleurs LAN sans fil 9800.

IUG:



Étape 4. Redémarrez les deux boîtes en même temps.

IUG:

Naviguez jusqu'à Administration > Management > Backup & Restore > Reload

Q. Search Menu Items	Backup & Restore
Dashboard	Config File Management Reload
Monitoring >	Save Configuration and Reload.
🔾 Configuration 🛛 🔸	Reload without Saving Configuration.
🕥 Administration 🛛 🔸	 Reset to Factory Default and Reload.
X Troubleshooting	✓ Apply to Device

CLI:

reload

Activer lâ€[™]accès à la console du contrôleur LAN sans fil 9800 de secours

Une fois que la haute disponibilité est activée et que l'une des zones est attribuée comme active et l'autre comme hôte de secours, par défaut, il n'est pas permis d'atteindre le mode d'exécution (enable) sur la zone de secours.

Pour lâ€[™]activer, connectez-vous par SSH/console au contrôleur LAN sans fil 9800 actif et saisissez les commandes suivantes :

config t
redundancy
main-cpu
standby console enable
end

Forcer le basculement

Pour forcer un basculement entre les boîtiers, redémarrez manuellement le WLC 9800 actif ou exécutez cette commande :

Rompre la haute disponibilité

Effacer la configuration à haute disponibilité des deux contrôleurs LAN sans fil 9800

Afin de rompre la haute disponibilité sur les deux boîtiers, vous pouvez effectuer les étapes suivantes :

Étape 1. Effacer la configuration HA du WLC 9800 actif actuel et forcer un basculement par redondance (il redémarre le WLC 9800 actif actuel, il redémarre avec la configuration HA effacée)

```
16.10:
Active-9800 WLC# chassis clear
WARNING: Clearing the chassis HA configuration results in the chassis coming up in Stand Alone mode afte
Active-9800 WLC# redundancy force-switchover
16.11
Active-9800 WLC# clear chassis redundancy
```

Étape 2. Une fois que le WLC de secours 9800 est activé, connectez-vous et effacez la configuration de redondance.

```
new-Acitve-9800 WLC# chassis clear
WARNING: Clearing the chassis HA configuration will resultin the chassis coming up in Stand Alone mode a
```

Étape 3. Mettez à jour lâ€[™]adresse IP du nouveau contrôleur LAN sans fil 9800 actif. Mettez éventuellement à jour son nom d'hôte.

```
new-Acitve-9800 WLC# config t
new-Acitve-9800 WLC# hostname <new-hostname>
new-Acitve-9800 WLC# interface <wireless-mgmt-int-id>
new-Acitve-9800 WLC# ip address <a.b.c.d> <a.b.c.d>
new-Acitve-9800 WLC# exit
```

Étape 4. Enregistrez la configuration et rechargez le nouveau contrôleur LAN sans fil 9800 actif.

new-Acitve-9800 WLC# write
new-Acitve-9800 WLC# reload

Ensuite, le deuxième boîtier redémarre et revient avec une nouvelle configuration d'adresse IP (pour éviter la

duplication d'adresse IP avec l'ancien WLC HA 9800) et avec la configuration HA effacée. Le contrôleur LAN sans fil 9800 actif d'origine conserve son adresse IP initiale.

Configurer le délai dâ€[™]expiration des pairs

Les châssis actif et de secours s'envoient mutuellement des messages de maintien de la connexion pour s'assurer que les deux sont toujours disponibles.

Le délai d'expiration de l'homologue est utilisé pour déterminer si le châssis homologue est perdu s'il ne reçoit aucun message de maintien de la connexion du châssis homologue dans le délai d'expiration de l'homologue configuré.

Le délai dâ€TMexpiration par défaut est de 500 ms, mais il peut être configuré par la CLI. La valeur du délai dâ€TMattente configuré est synchronisée avec celle du contrôleur LAN sans fil 9800 de secours.

Utilisez la commande suivante pour personnaliser ce minuteur :

```
# chassis timer peer-timeout <500-16000 msec>
```

Utilisez cette commande pour effacer le minuteur configuré (si nécessaire) :

```
# chassis timer peer-timeout default
```

Mise à niveau

La mise à niveau standard (pas AP ou ISSU) peut être effectuée à partir de l'interface utilisateur Web. Une fois les contrôleurs LAN sans fil dans une paire à haute disponibilité, ils exécutent la même version dans le même mode (de préférence INSTALL [installation]).

La page de mise à niveau de l'interface Web prend en charge la distribution du logiciel aux deux contrôleurs de la paire et installe et redémarre les deux unités en même temps.

Cela entraîne des temps d'arrêt identiques sur les deux unités. Pour d'autres techniques qui entraînent moins de temps d'arrêt, veuillez consulter le <u>guide d'installation et d'application de correctifs</u>.

Vérifier

Une fois que les deux unités WLC 9800 ont redémarré et sont synchronisées l'une avec l'autre, vous pouvez y accéder via la console et vérifier leur état actuel avec ces commandes :

<#root>

9800 WLC-1# show chassis

Chassis/Stack Mac Address : <!--IP address--> - Local Mac Address Mac persistency wait time: Indefinite Local Redundancy Port Type: Twisted Pair

```
H/W Current
Chassis# Role Mac Address Priority Version State IP
_____
*1 Active 00a3.8e23.a240 1 V02 Ready <!--IP address-->
2 Standby 00a3.8e23.a280 1 V02 Ready <!--IP address-->
<#root>
9800 WLC-1-stby# show chassis
Chassis/Stack Mac Address : <!--IP address--> - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair
                                H/W Current
Chassis# Role Mac Address Priority Version State
                                                     IΡ
_____
    Active <!--address--> 1 V02 Ready <!--IP address-->
1
*2
     Standby <!--address-->
                         1
                              V02
                                    Ready
                                               <!--IP address-->
```

Remarque : la veille affiche également les adresses IP, suivez 'Cisco bug ID CSCvm64484' pour fix

Le signe * indique le châssis à partir duquel vous exécutez la commande.

```
<#root>
```

```
9800 WLC-1# show redundancy
Redundant System Information :
-----
      Available system uptime = 1 hour, 35 minutes
Switchovers system experienced = 0
            Standby failures = 0
       Last switchover reason = none
               Hardware Mode = Duplex
   Configured Redundancy Mode = sso
    Operating Redundancy Mode = sso
            Maintenance Mode = Disabled
              Communications = Up
Current Processor Information :
Active Location = slot 1
       Current Software state = ACTIVE
      Uptime in current state = 1 hour, 35 minutes
               Image Version = Cisco IOS Software [Fuji], WLC9500 Software (WLC9500_IOSXE), Experiment
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 20-Sep-18 03:07 by mcpre
                       BOOT = bootflash:packages.conf,12;
                 CONFIG FILE =
       Configuration register = 0x2102
Peer Processor Information :
```

```
Standby Location = slot 2
Current Software state = STANDBY HOT
Uptime in current state = 1 hour, 33 minutes
Image Version = Cisco IOS Software [Fuji], WLC9500 Software (WLC9500_IOSXE), Experiment
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 20-Sep-18 03:07 by mcpre
BOOT = bootflash:packages.conf,12;
CONFIG_FILE =
Configuration register = 0x2102
```

Vous pouvez vérifier les données actuelles des contrôleurs LAN sans fil 9800 actif et de secours pour confirmer quâ€[™]elles sont identiques sur les deux périphériques.

Exemples:

<#root> 9800 WLC-1# show ap summary chassis active r0								
AP Name	Slots	AP Model	Ethernet MAC	Radio MAC	Location			
AP Name	2	3702I	MAC	MAC	CALO	-		
AP Name	2	37021	MAC	MAC	abcde123456789012345			
9800 WLC-1# show ap summary cha	assis standb	y rO						
Number of APs: 2								
AP Name	Slots	AP Model	Ethernet MAC	Radio MAC	Location			
AP Name	2	37021	MAC .</td <td>MAC> (</td> <td>CALO</td> <td>I</td>	MAC> (CALO	I		
AP Name	2	3702I	MAC .</td <td>MAC> a</td> <td>abcde123456789012345</td> <td>I</td>	MAC> a	abcde123456789012345	I		

Dépannage

Exemple de résultat de console dâ€[™]une synchronisation de paire à haute disponibilité réussie entre deux contrôleurs LAN sans fil 9800 matériels :

Contrôleur LAN sans fil 9800 1

<#root>

9800 WLC-1# chassis ha-interface local-ip

remote-ip

9800 WLC-1# show chassis Chassis/Stack Mac Address : <!--MAC address--> - Local Mac Address Mac persistency wait time: Indefinite Local Redundancy Port Type: Twisted Pair H/W Current Chassis# Role Mac Address Priority Version State ΙP _____ *1 Active <!--MAC address--> 1 Ready V02 9800 WLC-1# wr Building configuration... [OK] 9800 WLC-1# reload Reload command is issued on Active unit, this will reload the whole stack Proceed with reload? [confirm] MMM DD HH:MM:SS.XXX: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command. Chassis 1 reloading, reason - Reload command *MMM DD HH:MM:SS.XXX: %IOSXE_REDUNDANCY-6-PEER: Active detected chassis 2 as standby. *MMM DD HH:MM:SS.XXX: %STACKMGR-6-STANDBY_ELECTED: Chassis 1 R0/0: stack_mgr: Chassis 2 has been elected *MMM DD HH:MM:SS.XXX: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for proce *MMM DD HH:MM:SS.XXX: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for proce *MMM DD HH:MM:SS.XXX: %CMRP-5-PRERELEASE_HARDWARE: Chassis 2 R0/0: cmand: 0 is pre-release hardware *MMM DD HH:MM:SS.XXX: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=1 *MMM DD HH:MM:SS.XXX: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion (raw-event=1 *MMM DD HH:MM:SS.XXX: %IOSXE_PEM-6-INSPEM_FM: PEM/FM Chassis 2 slot P0 inserted *MMM DD HH:MM:SS.XXX: %IOSXE_PEM-6-INSPEM_FM: PEM/FM Chassis 2 slot P2 inserted *MMM DD HH:MM:SS.XXX: % Redundancy mode change to SSO *MMM DD HH:MM:SS.XXX: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will not take effect until after a platfor *MMM DD HH:MM:SS.XXX: Syncing vlan database *MMM DD HH:MM:SS.XXX: Vlan Database sync done from bootflash:vlan.dat to stby-bootflash:vlan.dat (616 by MMM DD HH:MM:SS.XXX: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set. MMM DD HH:MM:SS.XXX: %PKI-6-CS_ENABLED: Certificate server now enabled. MMM DD HH:MM:SS.XXX: %HA CONFIG SYNC-6-BULK CFGSYNC SUCCEED: Bulk Sync succeeded MMM DD HH:MM:SS.XXX: %VOICE_HA-7-STATUS: VOICE HA bulk sync done. MMM DD HH:MM:SS.XXX: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)

Contrôleur LAN sans fil 9800 2

<#root>

9800 WLC-2# chassis ha-interface local-ip

remote-ip

9800 WLC-2# show chassis

Chassis/Stack Mac Address : <!--MAC address--> - Local Mac Address Mac persistency wait time: Indefinite Local Redundancy Port Type: Twisted Pair H/W Current Chassis# Role Mac Address Priority Version State IP

*1 Active <!--MAC address--> 1 V02 Ready

9800 WLC-2# wr

Building configuration...
[OK]

9800 WLC-2# reload

Reload command is issued on Active unit, this will reload the whole stack Proceed with reload? [confirm]

MMM DD HH:MM:SS.XXX: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command. Chassis 1 reloading, reason - Reload command

Press RETURN to get started!

*MMM DD HH:MM:SS.XXX: %IOSXE_PLATFORM-3-WDC_NOT_FOUND: WDC returned length: 0Adding registry invocations

*MMM DD HH:MM:SS.XXX: %REDUNDANCY-3-PEER_MONITOR: PEER_FOUND event on standby

*MMM DD HH:MM:SS.XXX: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized *MMM DD HH:MM:SS.XXX: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled *MMM DD HH:MM:SS.XXX: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is not allowed *MMM DD HH:MM:SS.XXX: %SMART_LIC-6-HA_ROLE_CHANGED: Smart Agent HA role changed to Standby. *MMM DD HH:MM:SS.XXX: dev_pluggable_optics_selftest attribute table internally inconsistent @ 0x1ED *MMM DD HH:MM:SS.XXX: mcp_pm_subsys_init : Init done sucessfullySID Manager, starting initialization ... *MMM DD HH:MM:SS.XXX: Notifications initializedSID Manager, completed initialization ...

*MMM DD HH:MM:SS.XXX: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan

*MMM DD HH:MM:SS.XXX: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized *MMM DD HH:MM:SS.XXX: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled *MMM DD HH:MM:SS.XXX: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is not allowed *MMM DD HH:MM:SS.XXX: %CRYPTO-4-AUDITWARN: Encryption audit check could not be performed *MMM DD HH:MM:SS.XXX: %VOICE_HA-7-STATUS: CUBE HA-supported platform detected. *MMM DD HH:MM:SS.XXX: %IOSXE_VMAN-3-MSGINITFAIL: Failed to initialize required Virt-manager resource: In *MMM DD HH:MM:SS.XXX: mcp_pm_init_done : Called *MMM DD HH:MM:SS.XXX: %ONEP_BASE-6-SS_ENABLED: ONEP: Service set Base was enabled by Default *MMM DD HH:MM:SS.XXX: cwan_pseudo_oir_insert_one: [0/0] ctrlr[16506] already analyzed *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1598997203 has been gene *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named ca has been generated or imported by ca *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named ewlc-tp1 has been generated or imported *MMM DD HH:MM:SS.XXX: %AAA-5-USER_RESET: User admin failed attempts reset by console *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_REPLACE: A key named TP-self-signed-1598997203 has been repla *MMM DD HH:MM:SS.XXX: %SSH-5-DISABLED: SSH 1.99 has been disabled *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_REPLACE: A key named ca has been replaced by crypto config w *MMM DD HH:MM:SS.XXX: %CRYPTO_ENGINE-5-KEY_REPLACE: A key named ewlc-tp1 has been replaced by crypto con MMM DD HH:MM:SS.XXX: %SPA_OIR-6-OFFLINECARD: SPA (BUILT-IN-4X10G/1G) offline in subslot 0/0 MMM DD HH:MM:SS.XXX: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0 MMM DD HH:MM:SS.XXX: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0 MMM DD HH:MM:SS.XXX: %IOSXE OIR-6-INSCARD: Card (cc) inserted in slot 0 MMM DD HH:MM:SS.XXX: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 0 MMM DD HH:MM:SS.XXX: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0 MMM DD HH:MM:SS.XXX: %IOSXE_OIR-3-SPA_INTF_ID_ALLOC_FAILED: Failed to allocate interface identifiers for MMM DD HH:MM:SS.XXX: %SYS-5-RESTART: System restarted --Cisco IOS Software [Fuji], WLC9500 Software (WLC9500_IOSXE), Experimental Version 16.10.20180920:011848 Copyright (c) 1986-2018 by Cisco Systems, Inc. Compiled Thu 20-Sep-18 03:07 by mcpre MMM DD HH:MM:SS.XXX: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to MMM DD HH:MM:SS.XXX: %SSH-5-ENABLED: SSH 1.99 has been enabled MMM DD HH:MM:SS.XXX: %CRYPTO ENGINE-5-KEY ADDITION: A key named TP-self-signed-1598997203.server has bee MMM DD HH:MM:SS.XXX: %SYS-6-BOOTTIME: Time taken to reboot after reload = 328 seconds MMM DD HH:MM:SS.XXX: %SMART_LIC-3-HOT_STANDBY_OUT_OF_SYNC: Smart Licensing agent on hot standby is out of MMM DD HH:MM:SS.XXX: %SPA_OIR-6-ONLINECARD: SPA (BUILT-IN-4X10G/1G) online in subslot 0/0 MMM DD HH:MM:SS.XXX: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/2, link down due to local faul MMM DD HH:MM:SS.XXX: %IOSXE_SPA-6-UPDOWN: Interface TenGigabitEthernet0/0/3, link down due to local faul MMM DD HH:MM:SS.XXX: BUILT-IN-4X10G/1G[0/0] : Unsupported rate(0) for the XCVR inserted inport 0 xcvr_ty MMM DD HH:MM:SS.XXX: BUILT-IN-4X10G/1G[0/0] : Unsupported rate(0) for the XCVR inserted inport 1 xcvr_ty MMM DD HH:MM:SS.XXX: %PKI-3-KEY_CMP_MISMATCH: Key in the certificate and stored key does not match for MMM DD HH:MM:SS.XXX: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new ce MMM DD HH:MM:SS.XXX: %TRANSCEIVER-3-INIT_FAILURE: SIP0/0: Detected for transceiver module in TenGigabit MMM DD HH:MM:SS.XXX: %LINK-3-UPDOWN: SIP0/0: Interface TenGigabitEthernet0/0/0, changed state to up

MMM DD HH:MM:SS.XXX: %PLATFORM-6-RF_PROG_SUCCESS: RF state STANDBY HOT

Exécutez cette commande sur n'importe quelle unité et, par défaut, toutes les 5 secondes, vous voyez une mise à jour de la synchronisation haute disponibilité :

<#root>

show redundancy history monitor [interval <5-3600 seconds >]

```
Sep 21 15:24:24.727 RF_EVENT_CLIENT_PROGRESSION(503) RP Platform RF(1340) op=8 rc=0
Sep 21 15:24:24.727 RF_EVENT_CLIENT_PROGRESSION(503) RP Platform RF(1340) op=8 rc=11
Sep 21 15:24:24.740 RF_EVENT_CLIENT_PROGRESSION(503) CWAN Interface Events(1504) op=8 rc=0
Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) CWAN Interface Events(1504) op=8 rc=0
Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) CWAN Interface Events(1504) op=8 rc=11
```

Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT HA(401) op=8 rc=0 Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT HA(401) op=8 rc=0 Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT HA(401) op=8 rc=0 Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT64 HA(404) op=8 rc=0 Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT64 HA(404) op=8 rc=0 Sep 21 15:24:24.741 RF_EVENT_CLIENT_PROGRESSION(503) NAT64 HA(404) op=8 rc=0 Sep 21 15:24:24.743 RF_EVENT_CLIENT_PROGRESSION(503) DHCPv6 Relay(148) op=8 rc=0 Sep 21 15:24:24.782 RF_EVENT_CLIENT_PROGRESSION(503) DHCPv6 Server(149) op=8 rc=0 Sep 21 15:24:24.782 RF_EVENT_CLIENT_PROGRESSION(503) DHCPv6 Server(149) op=8 rc=0 Sep 21 15:24:24.782 RF_EVENT_CLIENT_PROGRESSION(503) DHCPv6 Server(149) op=8 rc=0 Sep 21 15:24:24.783 RF_EVENT_CLIENT_PROGRESSION(503) Last Slave(65000) op=8 rc=0 Sep 21 15:24:25.783 RF_PROG_STANDBY_HOT(105) Last Slave(65000) op=8 rc=0 Sep 21 15:24:25.783 RF_EVENT_CLIENT_PROGRESSION(503) Last Slave(65000) op=8 rc=0

End = e Freeze = f

Enter Command: e

Pour obtenir une vue plus détaillée du processus de synchronisation haute disponibilité, exécutez la commande suivante :

show logging process stack_mgr internal

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.