Guide virtuel de déploiement de contrôleur sans-fil de Cisco

Contenu

Introduction

Avant la version 7.3, le logiciel contrôleur réseau local de radio (WLAN) a fonctionné sur le matériel dédié on s'est attendu à ce que que vous achetiez. Le contrôleur LAN Sans fil virtuel (vWLC) fonctionne sur le matériel général sous une infrastructure industriellement compatible de virtualisation. Le vWLC est idéal pour de petits et de taille moyenne déploiements avec une infrastructure virtuelle et exige un contrôleur de sur-sites. Les environnements distribués de branchement peuvent également bénéficier avec un contrôleur virtuel centralisé avec moins branchements exigés (jusqu'à 200).

les vWLCs ne sont pas un remplacement des contrôleurs de matériel d'expédition. La fonction et

les caractéristiques du vWLC offrent des avantages de déploiement et des avantages des services de contrôleur où les centres de traitement des données avec l'infrastructure de virtualisation existent ou sont considérés.

Avantages du vWLC :

- Flexibilité dans la sélection de matériel basée sur vos conditions requises.
- Coût réduit, d'espace requis, et d'autres temps système puisque de plusieurs cases peuvent être remplacées par des multiples instances courantes de matériel unique des contrôleurs, des périphériques de Gestion de réseau (NCS) et d'autres serveurs (ISE, MSE, VSG/Pare-feu).
- Indépendant et mutuellement - les exemples exclusifs permettent à des administrateurs pour utiliser de plusieurs contrôleurs virtuels pour gérer différents campus (ou même pour gérer des sites de plusieurs clients) utilisant le même matériel.
- Les caractéristiques d'enable ont fourni par le logiciel de virtualisation, y compris la Haute disponibilité, la protection de Basculement, et la facilité du transfert.

Avantages de VMware avec le vWLC :

- **vSphere** : Un module d'infrastructure de virtualisation du VMware, qui inclut le hypervisor ESX/ESXi, vMotion, jeu rouleau-tambour, ha, tolérance aux pannes, vSphere a distribué le commutateur, et plus.
- **serveur de vCenter** : Le serveur de vCenter de VMware (autrefois VMware VirtualCenter) fournit une plate-forme extensible et extensible qui forme la base pour la Gestion de virtualisation :Contrôle centralisé et visibilité à chaque niveau de l'infrastructure virtuelleGestion proactive avec le vSpherePlate-forme d'administration extensible et extensible avec un large écosystème partenaire

Conditions préalables

Support virtuel de contrôleur

- Plate-forme : AIR-CTVM-K9
- Matériel : Cisco UCS, UCS serveurs exprès, de HP et IBM
- SYSTÈME D'EXPLOITATION de VMware : ESX/ESXi 4.x/5.x
- Mode de FlexConnect : commutation centrale et locale
- Autorisation : Permis verrouillés de noeud à UDI (éval 60 jours)
- Nombre maximal de Points d'accès (aps) : 200
- Nombre maximal de clients : 3000
- Nombre maximal de sites jusqu'à 200
- Représentation de débit jusqu'à 500 Mbits/s par contrôleur virtuel
- Gestion avec l'infrastructure 1.2 de perfection de Cisco et en haut

Fonctions non prises en charge virtuelles de contrôleur WLAN

Cette liste inclut les fonctions non prises en charge de la version 7.3.112.0 WLC et de la release 7.4.100.60 :

- Transport Layer Security de datagramme de données (DTLS)

- Point d'accès d'OfficeExtend (OEAP) (aucune données DTLS)
- Limitation de débit
- Limitation de taux de transmission sans fil (contrat de bande passante)
- Serveur DHCP interne
- Mobilité/ancre d'invité
- Mode Multicast**Remarque:** Le trafic de multidiffusion commuté par gens du pays de FlexConnect pont d'une manière transparente pour de câble et radio sur le même VLAN. Les Points d'accès de FlexConnect ne limitent pas le trafic qui est basé sur piller de Protocole IGMP (Internet Group Management Protocol) ou de Multicast Listener Discovery (MLD).
- Mode Unicast
- PMIPv6
- IPv6
- Points d'accès en mode local
- Points d'accès d'intérieur de maille
- Points d'accès extérieurs de maille (AP extérieur avec le mode de FlexConnect fonctionnera)**Remarque:** Des aps extérieurs tels qu'AP1552 sont pris en charge en mode de FlexConnect si les aps ne sont pas utilisés dans un déploiement de maille.
- Gamme Cisco 600 OEAPs
- Protocole d'échange de TrustSec SGT (SXP)
- Passerelle de groupe de travail (WGB)
- VideoStream
- Haute disponibilité
- Mobilité hiérarchique
- 802.11w
- Visibilité d'application et contrôle (AVC)**Remarque:** Voir les fonctions non prises en charge virtuelles de version 7.5 de contrôleur WLAN du guide Sans fil virtuel de déploiement de contrôleur de Cisco, version 7.5 pour la liste mise à jour.

Les besoins en matière de ressources virtuels simples de contrôleur

- CPU : CPU de 1virtual
- Mémoire : 2 Go
- Espace disque : 8 Go
- Interface réseau : le vWLC prend en charge un port pour la communication de données

Recommandations suggérées de matériel pour accueillir les contrôleurs virtuels de Cisco

- Serveur de montage sur bâti UCS R210-2121605W (2RU) :2 * CPU X5670 d'Intel Xeon @ 2.93 gigahertzMémoire de 16 G
- Serveur IBM x3550 M3 :2 * Les processeurs de gamme 5600 d'Intel Xeon avec 4 creuse chaque et chaque noyau capable de faire le filetage hyper qui te donne 16 CPU dans gigahertz @3.6 totalmémoire 12G
- Services Ready Engine d'ISR G2 (SRE) utilisant l'UCS exprès (but de bande) :SRE 700 : Intel Core Duo à un noyau 1.86 gigahertz avec la mémoire du Go 4SRE 900 : Dual core Intel Core Duo 1.86 gigahertz avec la mémoire du Go 4 (évolutive à 8 Go)

Condition requise AP

- Tous les 802.11n aps avec la version de logiciel exigée 7.3 sont pris en charge.
- Les aps fonctionneront en mode de FlexConnect seulement.
- L'autoconvert AP à FlexConnect est pris en charge sur le contrôleur.
- Les nouveaux aps commandés se transporteront avec le logiciel 7.3 de la fabrication.
- Des aps existants doivent être mis à jour au logiciel 7.3 avant de joindre un contrôleur virtuel.**Remarque:** Le contrôleur virtuel dans la version 7.3 utilise les Certificats signés d'individu (SSC) par comparaison avec les Certificats installés par fabrication (MIC) dans le contrôleur traditionnel. AP pourra valider le certificat de SSC fourni par le contrôleur virtuel avant de se joindre. Voir les considérations AP dans la section dépannage pour plus de détails.

Composants utilisés

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

- Commutateur Cisco Catalyst
- Appliance virtuelle de contrôleurs LAN Sans fil
- Logiciel Sans fil du contrôleur LAN 7.3
- Infrastructure 1.2 de perfection de Cisco
- Points d'accès 802.11n en mode de FlexConnect
- Serveur DHCP
- Serveur DNS
- NTP
- Ordinateur portable, Smartphone, et tablettes de client sans fil (IOS d'Apple, Android, Windows, et MAC)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Topologie

Afin de correctement implémenter et tester le vWLC de Cisco, une configuration réseau minimale est exigée, semblable au diagramme affiché dans cette section. Vous devez simuler un emplacement avec un FlexConnect AP dans un déploiement centralement commuté, et/ou en plus des sites locaux et distants avec le DHCP de gens du pays (mieux s'il y a également des DN et accès local à l'Internet).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Notes de mise à jour

Le réseau sans fil unifié Cisco (CUWN) 7.3 notes de mise à jour contiennent les informations importantes au sujet de cette release. Ouvrez une session à Cisco.com pour les dernières notes de mise à jour avant de charger et tester le logiciel.

Installation virtuelle de contrôleur

Pour le déploiement et la Gestion du vWLC, vous devrez télécharger l'un de ces suites de VMware au poste de travail :

- Administration de serveurs simple d'ESXi - Client de vSphere de VMware d'utilisation.
- Les plusieurs serveurs d'ESXi a besoin du vCenter - Des caractéristiques anticipées sont également attachées avec le vCenter qui a besoin de licences indépendantes (vMotion, et ainsi de suite).

Commencez le **client de vSphere de VMware**, et la procédure de connexion au serveur d'ESXi.

Interfaces virtuelles virtuelles de contrôleur

- Interface de gestion
- interface virtuelle
- Interface dynamique
- Interface de gestionnaire AP

Configuration d'interface commutateur connectée au serveur UCS

Cette section fournit une configuration d'échantillon de la connexion d'interface de Cisco Catalyst au serveur d'ESXi pour le commutateur virtuel comme interface de joncteur réseau. L'interface de gestion peut être connectée à un port d'accès sur le commutateur.

```
interface GigabitEthernet1/1/2
 description ESXi Management
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/1/3
 description ESXi Trunk
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

Procédez comme suit :

1. Créez deux Commutateurs virtuels distincts afin de tracer au service virtuel de contrôleur et les données mettent en communication. Allez à **ESX > configuration > réseau**, et cliquez sur Add le **réseau**.
2. **Le virtual machine** choisi, et cliquent sur Next.
3. Créez un vSwitch et assignez un NIC physique afin de connecter le port de service de vWLC. Le port de service ne doit pas être connecté à toute partie du réseau (typiquement déconnecté/inutilisé). En conséquence, n'importe quel NIC (même déconnecté) peut être utilisé pour ce vSwitch.

4. Cliquez sur **Next** (Suivant).
5. Fournissez une étiquette (dans ces exemple, **port de service de vWLC**).
6. Choisi **aucun (0)** pour l'ID DE VLAN comme port de service n'est typiquement un port d'accès.
7. Cliquez sur **Next** (Suivant).
8. Ici, vous voyez que vSwitch1 est créé pour le port de service de vWLC. Cliquez sur Add le **réseau** afin de répéter pour le port de données.
9. Pour le nouveau vSwitch, sélectionnez le NIC physique connecté sur un port de joncteur réseau s'il y a plusieurs NIC/portgroup assigné à un EtherChannel sur le commutateur.
10. Ajoutez le NIC.
11. Cliquez sur **Next** (Suivant).
12. Fournissez une étiquette (dans ces exemple, **port de données de vWLC**).
13. Pour l'ID DE VLAN, sélectionnez **ALL(4095)** puisque ceci est connecté à un port de joncteur réseau de commutateur.
14. Cliquez sur Next jusqu'à ce que vous vous terminiez les étapes pour ajouter le vSwitch.

Définition promiscueuse de mode de VMware

Le mode promiscueux est une stratégie de sécurité qui peut être définie au niveau virtuel de commutateur ou de portgroup dans le vSphere ESX/ESXi. Une interface réseau de virtual machine, de console de service, ou de VMkernel dans un portgroup qui permet l'utilisation du mode promiscueux peut voir tout le trafic réseau traverser le commutateur virtuel.

Par défaut, l'adaptateur réseau virtuel d'un système d'exploitation client reçoit seulement les trames qui sont signifiées pour lui. Le placement de l'adaptateur réseau de l'invité dans le mode promiscueux le fait recevoir toutes les trames passées sur le commutateur virtuel qui sont permises dans le cadre de la stratégie VLAN pour le portgroup associé. Ceci peut être utile pour la surveillance de détection d'intrusion ou si un renifleur doit analyser tout le trafic sur le segment de réseau.

Le port de données de vWLC exige du vSwitch assigné de recevoir le mode promiscueux pour des bons fonctionnements.

Procédez comme suit :

1. Localisez vSwitch2 (assigné pour le port de données de vWLC), et cliquez sur **Properties**.
2. Sélectionnez le VMNet assigné au port de données de vWLC (note que le mode promiscueux de Sécurité par défaut est placé pour rejeter), et cliquez sur Edit.
3. Dans la fenêtre de Properties, sélectionnez l'**onglet Sécurité**.
4. Cochez la case pour le **mode promiscueux**, choisissez **reçoivent de la** liste déroulante, et cliquent sur OK. Il est important de noter que l'**adresse MAC change** et **a modifié des transmissions que des** champs sont placés **pour recevoir** par défaut. Vous devez retourner ces valeurs **pour recevoir** si vous les changiez des valeurs par défaut.
5. Confirmez la modification, et cliquez sur **étroitement**.Le logiciel contrôleur virtuel est signalé comme un module .ovf au centre logiciel Cisco. Vous pouvez télécharger le module .ova/.ovf et l'installer sur n'importe quelle autre application virtuelle. Le logiciel est livré avec un permis libre d'évaluation de 60-jour. Après que la VM soit commencée, le permis d'évaluation peut être lancé et un permis acheté peut être automatiquement installé et lancé plus tard.
6. Téléchargez l'image virtuelle d'OVULES de contrôleur au disque local.

7. Allez à **ESX > fichier > déploient le modèle OVF** afin de mettre sur pied l'installation.
8. Parcourez à l'emplacement des OVULES classent (téléchargé du site de Cisco), et cliquent sur Next.
9. Cliquez sur **Next** (Suivant).
10. Fournissez un nom pour le vWLC ou recevez le par défaut, et cliquez sur Next.
11. Recevez la configuration **mise à zéro paresseuse de disposition épaisse** par défaut, et cliquez sur Next.
12. Recevez le par défaut de mappage de réseau, et cliquez sur Next.
13. Confirmez les configurations de déploiement, et cliquez sur Finish afin de commencer l'installation.
14. **Fin de** clic quand le déploiement est complet.

Deux choses importantes à noter concernant améliorer les contrôleurs virtuels :

- L'image d'OVULES est nécessaire seulement pour l'installation de première fois.
- L'image .AES peut être ultérieurement utilisée pour améliorer/déclassifiant.

Configurations virtuelles de contrôleur

Après création du contrôleur virtuel, configurez les configurations de virtual machine pour tracer le réseau et pour ajouter une console série virtuelle.

Procédez comme suit :

1. Sélectionnez le vWLC, et cliquez sur Edit les **configurations de virtual machine**.
2. **Adaptateur réseau** choisi **1 au port de service de vWLC** (vSwitch créé dans le réseau ESX).
3. **Adaptateur réseau 2 de** carte au **port de données de vWLC**.
4. Confirmez le mappage correct.

Port de console virtuel de contrôleur

Le port de console donne l'accès à l'invite de console du WLC. En conséquence, la VM peut provisioned avec des ports série afin de se connecter à ces derniers. Faute de ports série, la console de client de vSphere est connectée à la console sur le vWLC.

Le VMware ESXi prend en charge un port de console série virtuel qui peut être ajouté à la VM de vWLC. Le port série peut être accédé à dans une de ces deux manières :

- **Port série physique sur l'hôte** : Le port série virtuel des vWLC est tracé au port série de matériel sur le serveur. Cette option est limitée au nombre de port série physique sur l'hôte. Si dans un scénario de vWLC de multi-locataire, ceci peut ne pas être idéal.
- **Connectez par l'intermédiaire du réseau** : Le port série virtuel des vWLC peut être accédé à utilisant la session de telnet d'un ordinateur distant à un port spécifique alloué pour la VM sur le hypervisor. Par exemple, si l'adresse IP des hypervisor est 10.10.10.10 et le port alloué pour une VM de vWLC est 9090, utilisant le « telnet 10.10.10.10 9090", juste comme accéder à la console d'un WLC physique utilisant un serveur de terminaux de Cisco, la console série des vWLC peut être accédée à.

Procédez comme suit :

1. Sur l'**onglet Matériel de** vWLC, cliquez sur Add.
2. Sur l'**onglet Matériel de** vWLC, cliquez sur Add.
3. Dans cet exemple, choisissez **se connectent par l'intermédiaire du réseau**, et cliquent sur Next.
4. Allez au **soutien choisi de réseau** :Pour le soutien de réseau, choisissez le **serveur (la VM écoute la connexion)**.Pour l'URI de port, écrivez le **<host> de telnet:// : <port>** (par exemple, telnet://10.10.10.10:9090).
5. Cliquez sur Next afin de passer en revue les options, et cliquez sur Finish.
6. Cliquez sur OK afin de se terminer les configurations configurées.Afin d'activer pour l'interface série par l'intermédiaire du réseau, ESX doit être configuré pour tenir compte de telles demandes.
7. Naviguez vers l'ESX, cliquez sur l'onglet de **configuration**, allez au **logiciel** > au **profil de Sécurité**, et cliquez sur en fonction **Properties**.
8. Dans la fenêtre de **Properties de Pare-feu**, le **port série** choisi **VM connecté au vSPC**, et cliquent sur OK.

Commencez le vWLC

Procédez comme suit :

1. Commencez le vWLC, et sélectionnez la console afin d'observer la première fois le processus d'installation.
2. Surveillez la progression jusqu'à la console VM prouve que le vWLC a redémarré (c'est automatique).
3. Ouvrez une session de telnet au vWLC comme affiché ici :
4. La session de telnet gèrera maintenant la console au vWLC.**Remarque:** Seulement un mode de console peut être opérationnel à tout moment, comme une console VM (par clé-interruption au startup) ou la console série (examen médical/réseau). Il n'est pas possible de mettre à jour chacun des deux en même temps.
5. Continuez à attendre jusqu'à ce que le vWLC ait été livré en ligne entièrement et vous incite à commencer l'assistant d'outil de configuration.
6. Configurez l'adresse/masque/passerelle d'interface de gestion. Configurez l'ID DE VLAN d'interface de gestion si étiqueté. Continuez le reste.
7. Semblable à tous les dispositifs de réseau, configurer le NTP est crucial. Le contrôleur virtuel doit avoir l'horloge correcte car il est possible d'avoir une horloge incorrecte sur l'hôte ESX, ou de la configuration manuelle, qui peut avoir comme conséquence les aps ne se joignant pas dans le processus.
8. Terminez-vous la configuration et permettez au vWLC pour remettre à l'état initial.
9. On lui suggère que vous cingliez l'interface de gestion de vWLC afin de s'assurer qu'elle a été livré en ligne. Procédure de connexion au vWLC.
10. Vous pouvez émettre la commande **récapitulative d'interface d'exposition** et cingler la passerelle du vWLC.
11. Connectez à la Gestion de vWLC utilisant un navigateur Web
12. Au commencement, il y a 0 Points d'accès (zéro) pris en charge. Permettez au permis d'évaluation afin de permettre à AP pour se joindre.
13. Allez à la **Gestion** > au **lancement** > aux **permis de logiciel**. **Le base-ap-compte** choisi, et a fixé la priorité à la **haute**.
14. Cliquez sur OK, et **recevez le** CLUF afin de continuer.

15. Cliquez sur OK, et remettez à l'état initial le vWLC pour que le permis d'évaluation le prenne effet.
16. Redémarrez le vWLC.
17. Connectez-vous de retour dedans au vWLC, et notez que les 200 aps sont maintenant pris en charge avec le permis d'évaluation activé.
18. Connectez AP, et le surveillez pour que le message de joindre se produise.
19. Du navigateur, allez à la **RADIO** et confirmez qu'AP s'est joint.
20. Cliquez sur AP, et changez le mode AP à **FlexConnect**. Seulement FlexConnect est pris en charge (commutation centrale et locale) dans la release 7.3.
21. Il peut être utile d'envisager d'utiliser la fonction d'autoconvert du contrôleur (par exemple, n'importe quel mode AP joignant le vWLC sera converti automatiquement en FlexConnect). Émettez cette commande afin d'implémenter :`(Cisco Controller) >` **`config ap autoconvert flexconnect enable`**

Gestion virtuelle de contrôleur avec la perfection 1.2 de Cisco

Cisco amorcent la version 1.2 d'infrastructure est la version minimum exigée pour gérer centralement un ou plusieurs contrôleurs virtuels de Cisco. La Gestion pour le contrôleur virtuel de Cisco n'est pas différente que les contrôleurs physiques existants par rapport au Cisco WCS ou au NCS. Cisco amorcent l'infrastructure 1.2 fournit la configuration, la gestion de logiciel, la surveillance, l'enregistrement, et le dépannage des contrôleurs virtuels. Référez-vous à la documentation principale d'infrastructure de Cisco de la manière prescrite pour administratif et la prise en charge de la gestion.

1. Procédure de connexion au serveur d'infrastructure de perfection de Cisco comme **racine**. Par défaut, la sélection de vue de Gestion est le thème de cycle de vie, qui est nouveau début avec la version 1.2. Le thème classique (affiché plus tard) sera plus familier aux administrateurs qui avaient fonctionné dans le Cisco WCS et le NCS.
2. Allez **fonctionner > centre de travail de périphérique**.
3. Au centre de travail de périphérique, cliquez sur Add le **périphérique**.
4. Écrivez l'adresse IP et la chaîne de caractères de la communauté SNMP (lecture/écriture). Par défaut, le SNMP RW pour le contrôleur est privé. Cliquez sur **Add**.
5. Cisco amorcent l'infrastructure le découvrira et synchronisera avec le contrôleur virtuel. Le clic régénèrent afin de mettre à jour l'écran.
6. Quand le contrôleur virtuel est découvert, il est répertorié comme géré et accessible (affiché dans le vert). Ajoutez n'importe quels autres contrôleurs virtuels en ce moment, si disponible.
7. Le nouveau contrôleur sera répertorié dans le **type de périphérique >** le **contrôleur LAN VIRTUEL de radio de gamme de Cisco**.
8. Naviguez pour autoguider pour une vue récapitulative (dans le thème de cycle de vie) des périphériques étant gérés.
9. Pour le reste de ce guide, le thème classique est utilisé pour effectuer la tâche semblable d'ajouter le contrôleur virtuel, aussi bien que de mettre à jour l'image de système. Allez à et **commutateur** choisi au **thème classique**.
10. Allez au **Configure > Controllers**.
11. Afin d'ajouter un nouveau contrôleur virtuel, choisi **ajoutent des contrôleurs… du** choisi une liste déroulante de commande.
12. Écrivez l'adresse IP, chaîne de caractères de la communauté SNMP lecture/écriture, et cliquez sur Add.

13. L'infrastructure de perfection de Cisco affichera cette notification :
14. Allez au **Configure > Controllers**. Le contrôleur virtuel sera répertorié en tant qu'accessible une fois qu'il a été avec succès découvert et ajouté. Autrement, et comme affiché ci-dessus, le périphérique apparaîtra dans la page inconnue de périphérique s'il n'était pas découvert avec succès.

Améliorez le contrôleur virtuel

Dans les étapes tôt de l'installation, le contrôleur virtuel de Cisco a au commencement exigé un fichier d'OVULES pour la nouvelle création virtuelle d'appareils. Cependant, les caractéristiques de contrôleur et les mises à niveau de logiciel virtuelles de mise à jour exigent un fichier commun AES téléchargeable du site Web Cisco.

Procédez comme suit :

1. Téléchargez le fichier AS*7_3*aes à un hôte de cible (par exemple, le serveur TFTP/FTP).
2. Juste comme pour les contrôleurs existants, allez au GUI de Web du contrôleur > du **Commands > Download File**. Sélectionnez le type de fichier, le Transfer Mode, l'adresse IP, le chemin de fichier, et le nom du fichier (fichier .aes). Cliquez sur Download afin de commencer le processus.
3. Quand le processus s'est terminé avec succès, vous êtes incité à redémarrer pour que la nouvelle image logicielle la prenne effet. Cliquez sur le lien à la page de réinitialisation afin de continuer.
4. **Sauvegarde et réinitialisation de** clic.
5. Cisco amorcent l'infrastructure peut également être utile pour promouvoir un contrôleur virtuel ou beaucoup de contrôleurs virtuels en même temps. Allez au **Configure > Controllers**. Sélectionnez (case) un ou plusieurs contrôleurs virtuels. Sélectionnez le **logiciel de téléchargement (TFTP) de la** liste déroulante de commande. Cet exemple utilise le mode TFTP pour la mise à niveau d'image.
6. Fournissez le type de téléchargement, le serveur TFTP (nouveau si utilisation externe), l'adresse IP, le chemin de fichier, et le nom du fichier de serveur (qui est le type de fichier .aes). Cliquez sur **Download**.
7. Cet écran est un exemple de l'image AES étant transférée vers les contrôleurs virtuels :
8. Cisco amorcent l'infrastructure mettra à jour l'état jusqu'à ce que le logiciel ait transféré avec succès.
9. Semblable à l'expérience directement du contrôleur, une réinitialisation est exigée quand le transfert est complet. En infrastructure de perfection de Cisco, allez au **Configure > Controllers**, et sélectionnez les contrôleurs virtuels. Sélectionnez les **contrôleurs de réinitialisation du** choisi une liste déroulante de commande….
10. Cisco amorcent l'infrastructure incitera pour des paramètres de réinitialisation tels que la save configuration, et ainsi de suite. Cliquez sur **OK**.
11. Cisco amorcent l'infrastructure informera l'administrateur que les contrôleurs virtuels sont redémarrés.
12. Quand complète, l'infrastructure principale de Cisco fournira les résultats du processus.

Dépannage

Considérations AP

Problème connu : AP ne joignant pas le vWLC - AP doit obtenir l'entrée d'informations parasites d'un contrôleur existant avant qu'il joigne un vWLC.

- AP doit être à la version de logiciel 7.3.1.35 et en haut avec succès joindre un contrôleur virtuel. Les contrôleurs virtuels emploient SSC afin de valider AP avant de se joindre.
- AP à la version 7.3 peut valider le certificat SSC fourni par le contrôleur virtuel.
- Après que réussi délivrez un certificat la validation, AP vérifiera la clé d'informations parasites du contrôleur virtuel dans la liste de clés enregistrées dans l'éclair. S'il apparie les informations parasites enregistrées, la validation est passée et les mouvements AP à l'état de PASSAGE. Si la validation d'informations parasites échoue, elle démontera du contrôleur et redémarrera le processus de découverte.
- La validation d'informations parasites, qui est une étape supplémentaire d'autorisation, sera exécutée seulement si AP joint un contrôleur virtuel. Il y aura une molette pour activer/désactiver la validation principale d'informations parasites.
- Par défaut, la validation d'informations parasites est activée, ainsi il signifie qu'AP doit avoir la clé virtuelle d'informations parasites de contrôleur dans son éclair avant qu'il puisse avec succès se terminer l'association avec le contrôleur virtuel. Si la molette est arrêtée, AP sautera la validation et le mouvement d'informations parasites directement à l'état de PASSAGE.
- La clé d'informations parasites peut être configurée dans les configurations de mobilité de contrôleur, qui obtient poussé à tous les aps qui sont joints. AP sauvegardera cette configuration jusqu'à ce qu'il s'associe avec succès à un autre contrôleur. Après quoi, il hérite de la configuration de clé d'informations parasites du nouveau contrôleur.
- Typiquement, les aps peuvent joindre un contrôleur traditionnel, téléchargent les clés d'informations parasites, et puis joignent un contrôleur virtuel. Cependant, si elle est jointe à un contrôleur traditionnel, la molette de validation d'informations parasites peut être arrêtée et elle peut joindre n'importe quel contrôleur virtuel. L'administrateur peut décider de maintenir la molette "Marche/Arrêt"

Ces informations sont capturées dans l'ID de bogue Cisco CSCua55382.

Exceptions :

- Si AP n'a aucune clé d'informations parasites dans son éclair, il sautera la validation d'informations parasites, supposant que c'est une installation de première fois.Dans ce cas, la validation d'informations parasites est sautée indépendamment de si la molette de validation d'informations parasites est "Marche/Arrêt".Une fois qu'il joint avec succès le contrôleur, il héritera de la configuration d'informations parasites de membre de groupe de mobilité (si configuré dans le contrôleur). Après quoi, il peut joindre un contrôleur virtuel seulement s'il a une entrée principale d'informations parasites dans sa base de données.
- Effacer la configuration AP du contrôleur ou sur la console AP aura comme conséquence s'effacer de toutes les clés d'informations parasites. Après quoi, AP joint le contrôleur virtuel comme si c'est une installation de première fois.`Effacement de capwap de test AP>Reprise de capwap de test AP>`

Le temps est incorrect

- À l'initiale installez, il est possible que le temps puisse être biaisé ou pas correctement synced. En conséquence, AP peut ne pas pouvoir se joindre correctement. Dans ce cas, vérifiez le groupe date/heure de validité de SSC afin de s'assurer qu'il est correct. Le NTP est toujours aller recommandé en avant.`(Cisco Controller) >`**`show certificate ssc`** `SSC Hash validation.............................. Enabled. SSC Device Certificate details: Subject Name : C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller, CN=DEVICE-vWLC-AIR-CTVM-K9-000C29085BB8, MAILTO=support@vwlc.com Validity :` **`Start : 2012 Jun 8th, 17:52:46 GMT End : 2022 Apr 17th, 17:52:46 GMT`** `Hash key :` **`bd7bb60436202e830802be1e8931d539b67b2537`**

Informations parasites de SSC

- AP est nouvel AP avec 7.3 et n'a pas des informations parasites peut joindre WLC virtuel aisément :`ap#`**`show capwap client config`**
- AP peut avoir des informations parasites plus anciennes de SSC, d'une vieille installation ou de joindre d'autres contrôleurs. Il est possible de configurer le WLC pour ne pas valider SSC, permettent à des aps de joindre le vWLC, réactivant alors la validation de nouveau.`(Cisco Controller) >`**`configure certificate ssc hash validation disable`**
- Exécutez la commande du **capwap** *<erase/restart> de* **test** afin d'effacer des configurations de capwap AP et initiez le processus de jonction.`APf866.f267.67af#`**`test capwap erase`** `APf866.f267.67af#`**`test capwap restart`** `restart capwap APf866.f267.67af# *Jun 9 12:27:22.469: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 10.10.11.20:5246 *Jun 9 12:27:22.525: %WIDS-6-DISABLED: IDS Signature is removed and disabled. *Jun 9 12:27:22.529: %LWAPP-3-CLIENTERRORLOG: LWAPP LED Init: incorrect led state 255 *Jun 9 12:27:22.897: Starting Ethernet promiscuous mode *Jun 9 12:27:32.903: %CAPWAP-3-ERRORLOG: Go join a capwap controller *Jun 9 12:27:23.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.10.11.20 peer_port: 5246 *Jun 9 12:27:23.276: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: 10.10.11.20 peer_port: 5246 *Jun 9 12:27:23.276: %CAPWAP-5-SENDJOIN: sending Join Request to 10.10.11.20`
- En tant qu'élément de la configuration de mobilité, s'il y a un contrôleur virtuel dans le réseau, l'administrateur doit ajouter une clé d'informations parasites du contrôleur virtuel dans tous les contrôleurs de pair. Si ajoutant un autre contrôleur de pair, la considération est d'ajouter les informations parasites (affichées dans SSC sorti ci-dessus) au membre de groupe de mobilité.`(Cisco Controller) >`**`config mobility group member add 10.10.11.30`** `(Cisco Controller) >`**`config mobility group member hash 10.10.11.30 bd7bb60436202e830802be1e8931d539b67b2537`**

Informations connexes

- Matrice de caractéristique de FlexConnect
- Cisco ENROULENT la documentation
- Guide de déploiement de contrôleur de branchement de radio du flexible 7500
- Support et documentation techniques - Cisco Systems