Contenu

Introduction

Le point d'accès distant Hybrid Remote Edge (H-REAP) est une solution pour les déploiements de succursale et de bureau distant. Il permet à des clients de configurer et contrôler deux ou trois Points d'accès (aps) dans un bureau de branchement ou de distant de l'entreprise par un lien de réseau d'étendu (WAN) sans nécessité de déployer un contrôleur dans chaque bureau. Ce document discute certains des problèmes courants qui peuvent se produire dans un environnement H-REAP. Ce document fournit également des informations sur la façon dont dépanner ces questions. Référez-vous à la conception H-REAP et au guide de déploiement pour des considérations de conception H-REAP quand vous déployez H-REAP et l'hybride REAP de configurer pour les étapes de configuration.

Conditions préalables

Conditions requises

- La connaissance fonctionnelle de H-REAP et de ses modes de fonctionnement
- La connaissance de la procédure d'enregistrement de point d'accès léger (LAP) à un contrôleur
- La connaissance du point d'accès léger Protocol (LWAPP)

Composants utilisés

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

- Contrôleurs LAN Sans fil de gammes Cisco 4400 et 2100 (WLCs) cette version 5.1 de

passage
- AG 1130AG aps, 1240 aps de Cisco, et 1250 aps
- Routeurs de gammes Cisco 2800 et 3800 qui exécutent la version 12.4

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.

Conventions

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

Informations générales

Ce sont les restrictions à se souvenir tandis que vous utilisez H-REAP.

- L'hybride REAP est pris en charge seulement sur le 1130AG, les 1140, les 1240, les 1250, les 1260, l'AP801, l'AP 802, 1040, et l'AP3550 aps et sur Cisco WiSM, Cisco 5500, 4400, 2100, 2500, les contrôleurs de gamme 7500 de flexible, le commutateur de contrôleur sans fil LAN intégré du Catalyst 3750G, et le module réseau de contrôleur pour des Integrated Services Router.
- N'importe quel type de Sécurité qui exige le contrôle du chemin de données, tel que le VPN, ne fonctionne pas avec le trafic sur des WLAN localement commutés parce que le contrôleur ne peut pas exercer le contrôle des données qui ne sont pas percées un tunnel de nouveau à lui. Tous autres travaux de type de Sécurité sur WLAN centralement ou localement commutés, à condition que le chemin entre le H-REAP et le contrôleur soit. Quand ce conduit est vers le bas, seulement un sous-ensemble de ces options de Sécurité permet à de nouveaux clients pour se connecter aux WLAN localement commutés.
- Quand un Point d'accès H-REAP entre le mode autonome, l'authentification WLAN qui sont configurés pour ouvert, partagé, de WPA-PSK, ou WPA2-PSK entrent dans « authentification locale, l'état de commutation locale » et continuent de nouvelles authentifications client.Dans la version 4.2 de logiciel contrôleur ou plus tard, cela vaut également pour les WLAN qui sont configurés pour le 802.1X, le WPA-802.1X, le WPA2-802.1X, ou le Cisco Centralized Key Management (CCKM). Cependant, ces types d'authentification exigent qu'un serveur RADIUS externe soit configuré. D'autres WLAN entrent dans « authentification vers le bas, commutant en bas » de l'état (si le WLAN était configuré pour la commutation centrale) ou « authentification vers le bas, l'état de commutation locale » (si le WLAN était configuré pour la commutation locale).
- Avec H-REAP en mode connecté, le contrôleur est libre d'imposer l'exclusion de client/mettre pour empêcher quelques clients d'associer avec ses aps. Cette fonction peut se produire de mode automatisée ou manuelle. En vue de global et les configurations par-WLAN, des clients peuvent être exclus pour une foule de raisons, qui s'étendent des tentatives répétées d'authentification défaillante au vol IP, aussi bien que pour n'importe quel temps donné. Des clients peuvent également être présentés dans cette liste d'exclusion manuellement. L'utilisation de cette caractéristique est seulement possible tandis qu'AP est en mode connecté. Les clients qui ont été placés sur cette liste d'exclusion restent incapables de se

connecter à AP, même tandis qu'il est en mode autonome
- Les WLAN qui utilisent l'authentification MAC (des gens du pays ou en amont) ne permettent plus des authentifications client supplémentaires quand AP est en mode autonome, qui est identique à la manière par WLAN pareillement configuré avec le 802.1X ou WebAuth fonctionne en même mode.
- Itinérance sécurisée rapide de support de versions 4.2.61.0 et ultérieures WLC utilisant CCKM. Itinérance sécurisée rapide de la couche 2 de supports de mode H-REAP utilisant CCKM. Cette caractéristique empêche le besoin de pleine authentification EAP de RAYON pendant que le client erre d'un AP à l'autre. Afin d'utiliser CCKM jeûnez itinérance avec des Points d'accès H-REAP, vous doivent configurer des groupes H-REAP.

Dépannage H-REAP

Il y a quelques scénarios et situations courants qui surgissent et empêchent la configuration H-REAP et la Connectivité douces de client. Ce sont juste quelques telles situations avec leurs étapes de dépannage suggérées.

H-REAP ne joint pas le WLC

Ce sont les raisons de base pour un H-REAP de ne pas joindre le WLC :

- H-REAP ne peut pas obtenir une adresse IP à lui-même, ou il a été assigné avec une adresse IP incorrecte.
- Il n'y a pas aucune Connectivité layer-3 entre H-REAP et le WLC.
- Il n'y a pas une Connectivité de Protocol de point d'accès léger (LWAPP) entre le H-REAP et le WLC.
- D'autres raisons sont les H-REAP se joignant à un contrôleur différent, à la non-concordance de certificat, au problème avec WLC ou H-REAP lui-même, etc.

Exécutez ces étapes pour dépanner ces problèmes :

1. Vérifiez que H-REAP AP est assigné une adresse IP.Si le DHCP est utilisé par la console d'AP, vérifiez qu'AP obtient une adresse avec cette commande :.`AP_CLI#show dhcp leaseSi` la sortie de cette commande n'en est aucune, elle implique que l'adressage DHCP n'est pas utilisé pour cet AP.Maintenant, assurez-vous que l'adresse IP statique est assignée à AP d'une manière appropriée. Ceci peut être vérifié avec cette commande :`AP_CLI#show lwapp ip configLWAPP Static IP ConfigurationIP Address 10.77.244.222IP netmask 255.255.0.0Default Gateway 10.77.244.220`La sortie affiche une adresse IP statique de 10.77.244.222 a assigné à AP. Si ce n'est pas l'adresse IP destinée à assigner, corrigez l'adresse IP.
2. Vérifiez la connectivité IP entre AP et l'interface de gestion du contrôleur.Une fois que l'adresse IP a été vérifiée, cinglez l'adresse IP de Gestion du contrôleur pour s'assurer qu'AP peut communiquer avec le contrôleur. Utilisez la commande ping par la console d'AP avec cette syntaxe :`AP_CLI#ping 10.77.244.210!--- 10.77.244.210/27 is the example management interface IP address of the controller.`Si le ping n'est pas réussi, il indique qu'il y a un problème dans la connectivité IP entre AP et le contrôleur. Assurez-vous que le réseau en amont est correctement configuré et que l'accès WAN de nouveau au réseau d'entreprise est en hausse. Vérifiez que le contrôleur est opérationnel et n'est pas derrière aucune borne **NAT/PAT**. Cinglez du contrôleur à AP avec la même syntaxe. Assurez-vous que le **MTU** pour

le chemin entre le contrôleur et le H-REAP est à un minimum de **1500**. Ceci peut être vérifié avec le **ping - l 1500** *Gestion <WLC IP >* commande à partir d'un ordinateur du côté H-REAP du WAN.Voici un résultat témoin de la **commande ping** réussie :**ping -l 1500 10.77.244.210**Pinging 10.77.244.204 with 1500 bytes of data:Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Ping statistics for 10.77.244.204: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds: Minimum = 6ms, Maximum = 6ms, Average = 6ms

3. Vérifiez la Connectivité LWAPP entre AP et le contrôleur.Une fois la connectivité IP entre le H-REAP et le contrôleur a été vérifiée, exécute LWAPP met au point sur le contrôleur pour confirmer que des messages LWAPP sont communiqués à travers le WAN et pour identifier des problèmes relatifs. Sur le contrôleur, créez d'abord un filtre d'adresses MAC pour limiter la portée de la sortie de débogage. Utilisez cette commande de limiter la sortie de la commande ultérieure à AP simple :AP_CLI#**debug mac addr** <AP?s wired MAC address>.Une fois que ceci est placé pour limiter la sortie de débogage, activez l'élimination des imperfections LWAPP avec cette commande :Controller_CLI#**debug lwapp events enable**Vous voyez des messages de débogage semblables à ces derniers :----------
-------- ---------- ----------
---------- Thu Mar 15 15:07:56 2007: 00:12:44:b2:ae:d0 **Received LWAPP DISCOVERY REQUEST from AP 00:12:44:b2:ae:d0** to ff:ff:ff:ff:ff:ff on port '1'
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Received LWAPP JOIN REQUEST from AP 00:12:44:b2:ae:d0** to 00:0b:85:33:84:a0 on port '1' Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 AP AP0012.d92b.3a5e: txNonce 00:0B:85:33:84:A0 rxNonce 00:12:44:B2:AE:D0 Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **LWAPP Join-Request MTU path from AP 00:12:44:b2:ae:d0** is 1500, remote debug mode is 0 Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Successfully added NPU Entry for AP 00:12:44:b2:ae:d0 (index 50)Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.10, AP Port: 45989, next hop MAC: 0 0:12:d9:2b:3a:5e Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Successfully transmission of LWAPP Join-Reply to AP 00:12:44:b2:ae:d0**
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 0** Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 1 Thu Mar 15 15:08:08 2007: 00:12:44:b2:ae:d0 Received LWAPP CONFIGURE REQUEST from AP 00:12:44:b2:ae:d0 to 00:0b:85:33:84:a0 ----------
---------- ----------
--- ----------Cette sortie de débogage indique une transmission réussie des messages LWAPP entre le contrôleur et l'AP, suivi d'une demande de jonction réussie d'AP et le parallèle joignez la réponse du contrôleur. Plus tard AP obtient inscrit au contrôleur.Si aucun tel message de débogage LWAPP n'est vu, assurez-vous que le H-REAP a au moins une méthode par laquelle un contrôleur peut être découvert. Si de telles méthodes sont en place (comme la diffusion de sous-réseau locale, l'option 43 DHCP, ou les DN), vérifiez qu'ils sont correctement configurés. Si aucune autre méthode heuristique n'est en place, assurez-vous que l'adresse IP du contrôleur est manuellement écrite dans AP par la console CLI.AP_CLI#**lwapp ap controller ip address** <management interface Ip address of controller>
4. Si vous avez manuellement configuré le H-REAP, assurez-vous vous les informations précédemment associées claires de contrôleur quand vous déplacez votre AP à un endroit différent dans votre réseau. Ceci permet à votre AP pour s'associer avec le contrôleur dans le nouveau emplacement. Afin d'effacer la configuration précédente, émettez la commande de privé-**config de lwapp** AP CLI#clear. Puis, vérifiez si AP joint le contrôleur correct.Afin de vérifier avec quels contrôleurs AP communique, fournissez la commande de **debug ip udp à** AP CLI. De la sortie de cette commande, visualisez la source et les adresses de destination de chaque paquet qui traverse la pile IP d'AP.Voici un exemple :**UDP d'IP d'**AP_CLI#debug*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989),

dst=10.77.244.211(12223), length=60***Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223), length=75*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22 *Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989), length=49 *Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=76***Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22**De cette sortie, vous pouvez voir que les paquets UDP sont originaires d'AP et qu'ils atteignent l'interface d'interface de gestion (10.77.244.210) et de gestionnaire AP (10.77.244.211) du contrôleur.

5. Dépannez les questions de certificat si les tentatives AP de joindre le contrôleur mais échoue.Si des messages LWAPP sont vus sur le contrôleur, mais AP ne se joint pas, c'est probable une question de certificat. Pour plus de conseils de dépannage LWAPP, qui incluent des questions de certificat de dépannage, référez-vous à l'outil de mise à jour LWAPP dépannent des conseils.
6. Une autre raison pour laquelle H-REAP aps ne joignent pas WLCs est si le proxy ARP est désactivé sur la passerelle pour le H-REAP aps. De la console AP, ce message est enregistré :*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=60***Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223), length=75*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22 *Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989), length=49 *Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=76***Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22**Ceci peut sont provoqué par par l'ID de bogue Cisco CSCse92856. Ce problème s'applique seulement à AP1130 et à AP1240. Ce problème ne s'applique pas à AP1000s, à AP1100, ou à AP1200.Ce problème se pose quand ces conditions sont remplies :Le mode HREAP est utilisé dans le WLAN. Le mode local n'est pas affecté par cette question. Le mappage indigène VLAN est exigé.Les aps doivent être sur un différent IP de sous-réseau que le gestionnaire AP du WLCs.Le proxy ARP est désactivé sur la passerelle par défaut pour AP.Le H-REAP AP obtient la passerelle par défaut d'un serveur DHCP.Afin de résoudre ce problème, proxy ARP d'enable sur le routeur de passerelle par défaut d'AP.

Vérification du mode de fonctionnement H-REAP

Une fois que le H-REAP a joint le contrôleur correct, vous pouvez vérifier si le H-REAP AP est connecté au contrôleur à tout moment. En d'autres termes, vous pouvez vérifier en quel mode le H-REAP AP fonctionne. Ceci peut être vérifié avec la commande de **show lwapp reap status d'**AP CLI.

Le lwapp d'AP_CLI#show **récoltent l'état**

AP Mode: REAP, Connected Radar detected on:

Cette sortie indique que le H-REAP AP est en mode H-REAP et mode connecté. En d'autres termes, le lien WAN entre AP et le contrôleur est EN HAUSSE (connecté), et le mode de fonctionnement est H-REAP.

Le lwapp d'AP_CLI#show **récoltent l'état**

AP Mode: REAP, Standalone Radar detected on:

Cette sortie indique qu'AP est en mode autonome, ainsi il signifie que le lien WAN entre AP et le contrôleur est en baisse. Le mode de fonctionnement AP est REAP. Ceci signifie que les WLAN qui sont configurés pour la commutation locale avec l'authentification locale sont fonctionnels et

permettent de nouveaux clients à ce WLAN. Référez-vous à l'exemple de configuration de modes de fonctionnement H-REAP afin de comprendre les différents modes de fonctionnement de H-REAP.

Consolez les commandes de H-REAP ne sont pas opérationnels et renvoient une erreur

Toutes commandes de configuration (configuration ou effacement de la configuration) exécutées par le retour H-REAP CLI l'**ERREUR ! ! ! La commande est** message **désactivé**. Ceci peut se produire pour une de deux raisons :

- H-REAP aps qui sont en mode connecté (enregistré au contrôleur) ne permettent aucune configuration à placer ou être effacée par la console. Quand AP est dans cet état, des configurations doivent être faites par l'interface de contrôleur. Si l'accès aux commandes de configuration à AP est exigé, assurez-vous qu'AP est en mode autonome avant que vous tentiez de sélectionner toutes les commandes de configuration.
- Une fois qu'AP s'est connecté ou s'est enregistré à un contrôleur à un point quelconque, assurez-vous que le mot de passe par défaut d'enable de H-REAP, **Cisco**, est changé. Si ce mot de passe par défaut n'est pas changé, vous ne pouvez pas accéder à la console CLI du H-REAP est déplacé au mode autonome. Le mot de passe d'enable peut seulement être placé par le CLI du contrôleur auquel AP est connecté. Cette syntaxe de commande peut être utilisée au contrôleur pour placer le mot de passe de console d'AP individuel ou le mot de passe à tous les aps du contrôleur : *<passwd> de* **mot de passe de** *<user-id> de* **nom d'utilisateur du** >config (WLC_CLI) **AP {tout | name> <AP}**.Voici un exemple :`WLC-1>config ap username hreap password hreap all`**Remarque:** Si vous exécutez la version 5.0 et ultérieures WLC, utilisez cette commande : **le config ap mgmtuser ajoutent le** *secret* **secret de password password de nom d'utilisateur nom d'utilisateur {tout | Nom AP}Remarque:** Pour AP qui n'a pas eu ses mots de passe de console réglés, rendez-vous compte que cette configuration est seulement envoyée à AP quand la commande est sélectionnée au contrôleur. Tous les aps qui joignent ultérieurement le WLC exigent la commande d'être entré de nouveau.**Remarque:** Travail de ces commandes en fonction **hors de - Enfermez dans une boîte les H-**REAP même lorsque le mot de passe par défaut n'est pas changé :*<name> d'*adresse Internet du lwapp AP*adresse IP de l'*IP address *<AP du* lwapp AP *> < masque de sous-réseau >l'adresse IP des <Gateway d'*ip default-gateway du lwapp AP *>adresse IP du* lwapp ap controller ip address *<WLC >*clear lwapp private-config
- **Remarque:** Afin de renvoyer complètement AP aux par défaut d'usine, sur le démarrage AP, appuyez sur le **bouton mode** jusqu'à ce que la lumière d'Ethernets tourne l'ambre. Sur les 1131, cette lumière est près du bouton mode et est clairement identifiée par des Ethernets. Sur les 1242, c'est sous la façade en plastique blanche et notated avec E. Release le bouton mode et a permis le démarrage AP. AP est retourné à l'interface, qui est disponible par l'image de reprise IOS d'AP. Rendez-vous compte que si les nouvelles commandes de configuration sont désirées, AP doit exécuter la version de logiciel 12.3(11)JX1 ou ultérieures de Cisco IOS®. Ceci peut être vérifié par la console d'AP en écrivant la commande de **show version**.**Remarque:** Tous **affichent** et les commandes de **débogage** continuent à fonctionner sans mot de passe par défaut étant placé et tandis qu'AP est en mode connecté.Seulement en ce moment peuvent toutes les configurations LWAPP être faites.

Les clients ne peuvent pas se connecter à H-REAP

Si les clients sans fil ne peuvent pas se connecter à H-REAP, exécutez ces étapes :

1. Assurez-vous que le lien WAN entre le contrôleur et le H-REAP est en hausse.
2. Vérifiez qu'AP a correctement joint le contrôleur et que le contrôleur a au moins un (et activé) WLAN correctement configuré. Assurez-vous que le **H-REAP** est dans l'état activé pour des WLAN localement commutés
3. Au contrôleur, configurez le WLAN pour annoncer son SSID pour aider à dépanner ce processus. Sur l'extrémité client, vérifiez si le client peut trouver AP avec le SSID. Reflétez le nom SSID et la configuration de sécurité du WLAN sur le client. Les configurations de sécurité de côté client sont où l'immense majorité de problèmes de Connectivité résident.
4. Assurez-vous que les clients sur des WLAN localement commutés sont correctement IP adressé. Si le DHCP est utilisé, assurez-vous qu'un serveur DHCP en amont est correctement configuré et cela il fournit des adresses aux clients. Si l'adressage de charge statique est utilisé, assurez-vous que les clients sont correctement configurés pour le sous-réseau correct.
5. Assurez-vous que les ports UDP **12222** et **12223** sont ouverts sur tous les Pare-feu intermédiaires.
6. Afin de dépanner plus loin des problèmes de connectivité de client au port de console du H-REAP, émettez cette commande :`AP_CLI#show lwapp reap association`
7. Afin de mettre au point les problèmes de connectivité de 802.11 d'un client, émettez cette commande :`AP_CLI#debug dot11 state enable`
8. Afin de mettre au point la procédure d'authentification de 802.1X et les pannes d'un client, émettez cette commande :`AP_CLI#debug dot1x events enable`

Comptes incorrects de client d'états du système de contrôle sans fil (WCS) à AP en mode H-REAP

Si votre environnement sans fil est géré par le système de contrôle sans fil (WCS), parfois ce WCS peut signaler les clients incorrects au H-REAP AP, par opposition aux comptes corrects de client spécifiés par le contrôleur.

Ce problème est dû à l'ID de bogue Cisco CSCsg48059 (clients enregistrés seulement). WCS signale les comptes de client qui sont trop élevés quand H-REAP est activé sur le contrôleur. C'est le contournement.

1. Afin de découvrir combien de clients sont associés aux aps ou au contrôleur donné, utilisez la caractéristique de **Monitor > Clients WCS**.
2. Recherche par AP ou le contrôleur, qui sont limités par le type par radio, pour éviter des doublons.
3. Utilisez le nombre total d'éléments trouvés en tant que votre véritable nombre de population.Vous pouvez également employer le WLC pour trouver le compte correct de client.

Cette question est résolue dans la release Sans fil 4.0.206.0 de contrôleur LAN.

Informations connexes

- Dépanner un point d'accès léger ne pouvant pas se joindre à un contrôleur LAN sans fil
- Guide de conception et de déploiement d'un point d'accès H-Reap

- Configurer l'hybride REAP
- Exemple de configuration des modes d'opération des points d'accès H-REAP
- Configurer l'hybride REAP sur WCS
- Point d'accès léger - Forum Aux Questions
- Support et documentation techniques - Cisco Systems