Conseils de dépannage de l'outil de mise à niveau LWAPP

Contenu

Introduction

Ce document traite certains des problèmes clés qui pourraient se produire quand vous utilisez l'outil de mise à niveau afin de mettre à niveau les points d'accès (AP) autonomes au mode poids léger. Ce document fournit également des informations sur la façon de corriger ces problèmes.

Conditions préalables

Conditions requises

Les AP doivent exécuter le logiciel Cisco IOS® Version 12.3(7)JA ou ultérieure avant que vous puissiez exécuter la mise à niveau.

Les contrôleurs Cisco doivent exécuter au minimum la version 3.1 du logiciel.

Le système de contrôle sans fil (WCS) Cisco (si utilisé) doit utiliser au moins la version 3.1.

L'utilitaire de mise à niveau est pris en charge sur les plates-formes Windows 2000 et Windows XP. L'une ou l'autre de ces versions du système d'exploitation Windows doit être utilisée.

Composants utilisés

Les informations de ce document sont basées sur ces Points d'accès et Contrôleurs de LAN sans fil.

Les AP qui supportent ce transfert sont :

- Tous les Points d'accès 1121G
- Tous les points d'accès 1130AG
- Tous les points d'accès 1240AG
- Tous les points d'accès de la gamme 1250
- Pour toutes les plates-formes de points d'accès modulaires de la gamme 1200 basés sur IOS (AP de mise à niveau du logiciel Cisco IOS 1200/1220, 1210 et 1230), cela dépend de la radio :si 802.11G, MP21G et MP31G sont pris en chargesi 802.11A, RM21A et RM22A sont pris en chargeLes points d'accès de la gamme 1200 peuvent être mis à niveau avec n'importe quelle combinaison des radios prises en charge : G seul, A seul, ou G et A. Pour un point d'accès qui contient des doubles radios, si l'une des deux radios est une radio prise en charge LWAPP, l'outil de mise à niveau exécute toujours la mise à niveau. L'outil ajoute un message d'avertissement au journal détaillé qui indique quelle radio n'est pas prise en charge.
- Tous les points d'accès 1310 AG
- Carte d'interface Cisco C3201 mobile sans fil (WMIC)**Remarque:** Les radios 802.11a de seconde génération contiennent deux numéros de pièce.

Les points d'accès doivent exécuter Cisco IOS Version 12.3(7)JA ou ultérieure avant que vous puissiez exécuter la mise à niveau.

Pour Cisco C3201WMIC, les points d'accès doivent exécuter Cisco IOS Version 12.3(8)JK ou ultérieure avant que vous puissiez exécuter la mise à niveau.

Ces contrôleurs de LAN sans fil Cisco supportent les points d'accès autonomes mis au niveau du mode poids léger :

- contrôleurs de la gamme 2000
- contrôleurs de la gamme 2100
- contrôleurs de la gamme 4400
- Modules des services sans fil Cisco (WiSMs) pour les commutateurs de la gamme Cisco Catalyst 6500
- Modules de réseau de contrôleur dans les routeurs à services intégrés Cisco de la gamme 28/37/38xx
- Commutateurs des contrôleurs LAN sans fil intégrés Catalyst 3750G

Les contrôleurs Cisco doivent exécuter au minimum la version 3.1 du logiciel.

Le système de contrôle sans fil (WCS) Cisco doit exécuter au moins la version 3.1. L'utilitaire de mise à niveau est pris en charge sur les plates-formes Windows 2000 et Windows XP.

Vous pouvez télécharger la plus récente version de l'utilitaire de mise à niveau de la page Cisco Software Downloads.

Conventions

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

Processus de mise à niveau - Aperçu

L'utilisateur exécute un utilitaire de mise à niveau qui accepte un fichier d'entrée avec une liste des points d'accès et leurs qualifications. L'utilitaire envoie par Telnet aux points d'accès dans le fichier d'entrée une série de commandes Cisco IOS afin de préparer le point d'accès pour la mise à niveau, qui inclut les commandes pour créer des certificats auto-signés. En outre, l'utilitaire envoie par Telnet au contrôleur de programmer le périphérique pour permettre l'autorisation de points d'accès spécifiques de certificat auto-signé. Il charge alors le logiciel Cisco IOS version 12.3(11)JX1 sur le point d'accès de sorte qu'il puisse joindre le contrôleur. Après que le point d'accès aie joint le contrôleur, il télécharge une version complète de Cisco IOS. L'utilitaire de mise à niveau produit un fichier de sortie qui inclut la liste des points d'accès et les valeurs de hachage de la clé de certificat auto-signé correspondant, qui peuvent être importés dans le logiciel de gestion WCS. Le WCS peut alors envoyer cette information à d'autres contrôleurs sur le réseau.

Référez-vous à la section Procédure de mise à niveau de Mise à niveau au mode léger des points d'accès autonomes Cisco Aironet pour plus d'informations.

Outil de mise à niveau - Opération de base

Cet outil de mise à niveau est utilisé pour la mise à niveau au mode poids léger d'un AP autonome, à condition qu'AP soit compatible pour cette mise à niveau. L'outil de mise à niveau effectue les tâches de base nécessaires à la mise à niveau d'autonome au mode poids léger. Ces tâches incluent :

- Vérification de la condition de base - Vérifie si AP est pris en charge, s'il exécute un minimum de révision du logiciel et si les types de radio sont pris en charge.
- Assurez-vous qu'AP est configuré comme racine.
- Préparation de l'AP autonome pour la conversion - Ajoute la configuration et la hiérarchie de certificat de l'Infrastructure à clés publiques (PKI) de sorte que l'authentification AP aux contrôleurs Cisco puisse se produire, et que des certificats auto-signés (SSC) puissent être produits pour l'AP. Si AP a un certificat installé en usine (MIC), alors les SSC ne sont pas utilisés.
- Télécharge une image de la mise à niveau d'un autonome au mode léger, telle que 12.3(11)JX1 ou 12.3(7)JX, qui permet à AP de joindre un contrôleur. Sur un téléchargement réussi, ceci redémarre l'AP.
- Produit un fichier de sortie qui se compose d'adresses MAC AP, du type de certificat et d'un hachage de clé sécurisé, et qui met à niveau automatiquement le contrôleur. Le fichier de sortie peut être importé dans WCS et exporté vers d'autres contrôleurs.

Remarques importantes

Avant que vous utilisiez cet utilitaire, considérez ces remarques importantes :

- Les points d'accès convertis avec cet outil ne se connectent pas aux contrôleurs 40xx, 41xx ou 3500.
- Vous ne pouvez pas mettre à niveau les Points d'accès avec 802.11b seul ou des radios 802.11a de première génération.
- Si vous voulez retenir l'adresse ip statique, le masque de réseau, le nom de l'hôte et la passerelle par défaut des points d'accès après conversion et redémarrage, vous devez charger l'une de ces images autonomes sur les points d'accès avant que vous convertissiez les points d'accès à LWAPP :12.3(7)JA12.3(7)JA112.3(7)JA212.3(7)JA312.3(7)JA412.3(8)JA12.3(8)JA112.3(8)JA212.3(8)JEA12.3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g) JA12.4(3g) JA1
- Si vous mettez à niveau les points d'accès à LWAPP de l'une de ces images autonomes, les points d'accès convertis ne conservent pas leur adresse statique IP, le masque de réseau, le nom de l'hôte et la passerelle par défaut :12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- L'outil de mise à niveau LWAPP ne libère pas les ressources de mémoire du système d'exploitation Windows quand le processus de mise à niveau est terminé. Les ressources mémoire sont libérées seulement après que vous ayez quitté l'outil de mise à niveau. Si vous mettez à niveau plusieurs lots de points d'accès, vous devez quitter l'outil entre les lots afin de libérer les ressources mémoire. Si vous ne quittez pas l'outil entre les lots, la performance de la station de mise à niveau se dégrade rapidement en raison d'une consommation mémoire excessive.

Types de Certificats

Il y a deux genres différents d'AP :

- AP avec MIC
- AP qui requièrent SSC

Les certificats d'origine sont référencés par le terme « MIC » (Manufacturing Installed Certificate). Les points d'accès Cisco Aironet expédiés avant le 18 juillet 2005 n'ont pas de MIC, ainsi ces points d'accès créent un certificat auto-signé une fois mis à niveau pour fonctionner en mode léger. Les contrôleurs sont programmés pour accepter les certificats auto-signés pour l'authentification de points d'accès spécifiques.

Vous devez traiter les AP de Cisco Aironet MIC qui utilisent le protocole de point d'accès léger (LWAPP), tel que les AP Aironet 1000, et dépanner en conséquence. En d'autres termes, contrôlez la connectivité IP, déboguez la machine d'état LWAPP et contrôlez ensuite le cryptage.

Les journaux de l'outil de mise à niveau vous montrent si AP est une MIC AP ou SSC AP. Ceci est un exemple d'un journal détaillé de l'outil de mise à niveau :

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO  172.16.1.60  MIC is already configured in the AP
2006/08/21 16:59:07 INFO  172.16.1.60      Hardware is PowerPC405GP Ethernet,
```

```
                                        address is 0015.63e5.0c7e (bia 0015.63e5.0c7e)
2006/08/21 16:59:08 INFO  172.16.1.60  Inside Shutdown function
2006/08/21 16:59:10 INFO  172.16.1.60  Shutdown the Dot11Radio1
2006/08/21 16:59:11 INFO  172.16.1.60  Shutdown the Dot11Radio0
2006/08/21 16:59:12 INFO  172.16.1.60  Updating the AP with Current System Time
2006/08/21 16:59:13 INFO  172.16.1.60  Saving the configuration into memory
2006/08/21 16:59:13 INFO  172.16.1.60  Getting  AP Name
2006/08/21 16:59:58 INFO  172.16.1.60  Successfully Loaded the LWAPP Recovery
                                         Image on to the AP
2006/08/21 16:59:58 INFO  172.16.1.60  Executing Write Erase Command
2006/08/21 17:00:04 INFO  172.16.1.60  Flash contents are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Environmental Variables are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Reloading the AP
2006/08/21 17:00:08 INFO  172.16.1.60  Successfully executed the Reload command
```

Dans ce journal, la ligne mise en valeur spécifie que l'AP a un MIC installé avec lui. Référez-vous à la section Aperçu du processus de mise à niveau de Mise à niveau des points d'accès autonomes Cisco Aironet au mode léger pour plus d'informations sur les certificats et le processus de mise à niveau.

Dans le cas des AP SSC, aucun certificat n'est créé sur le contrôleur. L'outil de mise à niveau fait produire par AP une paire de clés Rivest, Shamir et Adelman (RSA) qui est utilisée pour signer un certificat auto-généré (le SSC). L'outil de mise à niveau ajoute une entrée à la liste d'authentification du contrôleur avec l'adresse MAC d'AP et le hachage de la clé publique. Le contrôleur a besoin de la clé publique afin de valider la signature SSC.

Si l'entrée n'a pas été ajoutée au contrôleur, contrôlez le fichier de sortie CSV. Il devrait y avoir des entrées pour chaque AP. Si vous trouvez l'entrée, importez ce fichier dans le contrôleur. Si vous utilisez l'interface de ligne de commande du contrôleur (CLI) (avec l'utilisation de la commande **config auth-list**) ou le Web du commutateur, vous devez importer un fichier à la fois. Avec un WCS, vous pouvez importer le fichier CSV en entier comme modèle.

En outre, contrôlez le domaine réglementaire.

Remarque: Si vous avez un AP LAP mais vous voulez la fonctionnalité Cisco IOS, vous avez besoin de charger une image autonome de Cisco IOS. Réciproquement, si vous avez un AP autonome et voulez le convertir en LWAPP, vous pouvez installer une image de reprise LWAPP au-dessus de l'autonome IOS.

Vous pouvez compléter les étapes pour changer l'image AP avec le bouton MODE ou les commandes CLI **archive download**. Référez-vous au Dépannage pour plus d'informations sur la façon d'utiliser la recharge de l'image du bouton MODE, qui fonctionne avec l'autonome IOS ou l'image de reprise nommée au nom de fichier par défaut du modèle AP.

La section suivante discute certains des problèmes généralement rencontrés dans les opérations de mise à niveau et les étapes pour résoudre ces problèmes.

Problème

Symptôme

AP ne joint pas le contrôleur. La section Solutions de ce document fournit les causes par ordre de probabilité.

Solutions

Employez cette section pour résoudre ce problème.

Cause 1

AP ne peut pas trouver le contrôleur par l'intermédiaire de la détection LWAPP, ou AP ne peut pas atteindre le contrôleur.

Dépanner

Procédez comme suit :

1. Émettez la commande **debug lwapp events enable** au contrôleur CLI.Recherchez LWAPP discovery > discovery response > join request > join response sequence. Si vous ne voyez pas la demande LWAPP discovery, il signifie qu'AP ne peut pas trouver le contrôleur.Voici un exemple de RÉPONSE JOINTE réussie du contrôleur LAN sans fil (WLC) à l'AP léger converti (LAP). C'est la sortie de la commande **debug lwapp events enable** :

```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
                          00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
                          to ff:ff:ff:ff:ff:ff on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to
                          AP 00:15:63:e5:0c:7e on Port 1
Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e
                          is 1500, remote debug mode is 0
Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e
                          (index 51)Switch IP: 172.16.1.11, Switch Port: 12223,
                          intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679,
                          next hop MAC: 00:15:63:e5:0c:7e
Thu May 25 06:54:05 2006: Successfully transmission of LWAPP Join-Reply to AP
                          00:15:63:e5:0c:7e
.........................................
.........................................
......................................... // the debug output continues for
full registration process.
```

2. Vérifiez la connectivité IP entre le réseau AP et le contrôleur. Si le contrôleur et l'AP résident dans le même sous-réseau, assurez-vous qu'ils sont correctement interconnectés. S'ils résident dans différents sous-réseaux, assurez-vous qu'un routeur est utilisé entre eux et que le routage est correctement activé entre les deux sous-réseaux.
3. Vérifiez que le mécanisme de découverte est correctement configuré.Si l'option Système de noms de domaine (DNS) est utilisée pour découvrir le WLC, assurez-vous que le serveur DNS est correctement configuré pour mapper le CISCO-LWAPP-CONTROLLER.local-domain avec l'adresse IP WLC. Par conséquent, si AP peut résoudre le nom, il émet un message joint LWAPP à l'adresse IP résolue.Si l'option 43 est utilisée comme option de découverte, assurez-vous qu'elle est correctement configurée sur serveur DHCP.Référez-

vous à Enregistrer le LAP avec le WLC pour plus d'informations sur le processus et la séquence de découverte.Référez-vous à Exemple de DHCP OPTION 43 pour configuration de points d'accès Cisco Aironet légers pour plus d'informations sur la façon de configurer l'option 43 du DHCP.**Remarque:** Rappelez-vous que quand vous convertissez des AP à adressage statique, le seul mécanisme de découverte de couche 3 qui fonctionne est le DNS parce que l'adresse statique est préservée pendant la mise à niveau.Sur AP, vous pouvez émettre la commande **debug lwapp client events** et la commande **debug ip udp** afin de recevoir assez d'informations pour déterminer exactement ce qui se produit. Vous devriez voir une séquence de paquet du Protocole de datagramme utilisateur (UDP) de ce type :Originaire de l'AP IP avec l'interface IP de gestion du contrôleur.Originaire du contrôleur AP gestionnaire IP à l'AP IP.Les séries de paquets qui sont originaires de l'AP IP à l'IP du gestionnaire AP.**Remarque:** Dans quelques situations, il peut y avoir plus d'un contrôleur et AP pourrait essayer de joindre un contrôleur différent sur la base de la machine d'état et des algorithmes de découverte LWAPP. Cette situation pourrait se produire en raison de l'équilibrage de charge dynamique AP par défaut que le contrôleur exécute. Cette situation peut valoir l'examen.**Remarque:** C'est un exemple de sortie de la commande **debug ip udp** :

```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222),
                     length=78
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223),
                     length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679),
                     length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=89
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=222
```

Résolution

Procédez comme suit :

1. Passez en revue le manuel.
2. Configurez l'infrastructure de sorte qu'elle supporte correctement la découverte LWAPP.
3. Déplacez l'AP au même sous-réseau que le contrôleur afin de l'amorcer.
4. S'il y a lieu, émettez la commande A.B.C.D **lwapp ap controller ip address** afin de définir manuellement l'IP du contrôleur à AP CLI :La *pièce A.B.C.D* de cette commande est l'adresse IP d'interface de gestion du WLC.**Remarque:** Cette commande CLI peut être utilisée sur un AP qui ne s'est jamais enregistré à un contrôleur, ou sur un AP qui a eu son mot de passe d'activation par défaut changé alors qu'il était joint à un contrôleur précédent. Référez-vous à Réinitialiser la configuration LWAPP sur un AP léger (LAP) pour plus d'informations.

Cause 2

Le temps du contrôleur est en dehors de l'intervalle de validité du certificat.

Dépanner

Procédez comme suit :

1. Émettez les commandes **debug lwapp errors enable** et **debug pm pki enable**.Ces commandes **debug** montrent le débogage de messages du certificat qui sont passées entre l'AP et le WLC. Les commandes montrent clairement un message que le certificat est rejeté comme étant en dehors de l'intervalle de validité.**Remarque:** Veillez à prendre en compte le décalage du Coordinated Universal Time (UTC).C'est la sortie de la commande **debug pm pki enable** sur le contrôleur :

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
.........................
.........................
.........................
.........................
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
                          validity interval: make sure the controller time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

Dans cette sortie, notez l'information mise en valeur. Cette information montre clairement que le **temps du contrôleur est en dehors de l'intervalle de validité du certificat d'AP**. Par conséquent, AP ne peut pas enregistrer avec le contrôleur. Les certificats installés dans AP ont un intervalle de validité prédéfini. Le temps du contrôleur devrait être défini de telle

manière qu'il soit dans l'intervalle de validité du certificat de l'AP.

2. Émettez la commande **show crypto ca certificates** d'AP CLI afin de vérifier l'intervalle de validité du certificat défini dans l'AP.Voici un exemple :

```
AP0015.63e5.0c7e#show crypto ca certificates
.....................................
.....................................
.....................................
.....................................
Certificate
  Status: Available
  Certificate Serial Number: 4BC6DAB80000000517AF
  Certificate Usage: General Purpose
  Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  Subject:
    Name: C1200-001563e50c7e
    ea=support@cisco.com
    cn=C1200-001563e50c7e
    o=Cisco Systems
    l=San Jose
    st=California
    c=US
  CRL Distribution Point:
    http://www.cisco.com/security/pki/crl/cmca.crl
  Validity Date:
    start date: 17:22:04 UTC Nov 30 2005
    end   date: 17:32:04 UTC Nov 30 2015
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: Cisco_IOS_MIC_cert
.................................
.................................
.................................
```

La sortie entière n'est pas listée car il peut y avoir beaucoup d'intervalles de validité associés avec la sortie de cette commande. Vous devez considérer seulement l'intervalle de validité spécifié par le **point de confiance associé : Cisco_IOS_MIC_cert** avec le nom d'AP pertinent dans le champ de nom (**Here, Name : C1200-001563e50c7e**), comme mis en valeur dans cet exemple de sortie. **C'est l'intervalle réel de validité du certificat à considérer.**

3. Émettez la commande **show time** du contrôleur CLI afin de vérifier que la date et l'heure définis sur votre contrôleur tombent dans cet intervalle de validité.Si le temps du contrôleur est au-dessus ou au-dessous de cet intervalle de validité du certificat, alors changez le temps du contrôleur pour être dans cet intervalle.

Résolution

Complétez cette étape :

Choisissez **Commands > Set Time** dans le mode GUI du contrôleur ou émettez la commande **config time** dans le contrôleur CLI afin de définir le temps du contrôleur.

Cause 3

Avec SSC AP, la politique SSC AP est désactivée.

Dépanner

En pareil cas, vous voyez ce message d'erreur sur le contrôleur :

```
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                          :spamDecodeJoinReq failed
Wed Aug  9 17:20:21 2006  [ERROR] spam_crypto.c 1509: Unable to free public key for
                          AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                          valid certificate in CERTIFICATE_PAYLOAD from
                          AP 00:12:44:b3:e5:60.
Wed Aug  9 17:20:21 2006  [CRITICAL] sshpmPkiApi.c 1493: Not configured to accept
                          Self-signed AP cert
```

Procédez comme suit :

Exécutez l'une de ces deux actions :

- Émettez la commande **show auth-list** au contrôleur CLI afin de vérifier si le contrôleur est configuré pour accepter les AP avec SSC.C'est un exemple de sortie de la commande **show auth-list** :
  ```
  #show auth-list


  Authorize APs against AAA ..... disabled

  Allow APs with Self-signed Certificate (SSC) .... enabled


  Mac Addr                  Cert Type    Key Hash

  ------------------------  ----------   ----------------------------------------

  00:09:12:2a:2b:2c         SSC          123456789012345678901234567890123456789O
  ```
- Choisissez **Security > AP Policies** dans le GUI.

1. Vérifiez si la case à cocher **Accept Self Signed Certificate** est activée. Sinon, activez-la.
2. Choisissez **SSC** en tant que type de certificat.
3. Ajoutez **AP** à la liste des autorisations avec adresse MAC et hachage de clé.Ce hachage de clé peut être obtenu à partir de la sortie de la commande **debug pm pki enable**. Voir la Cause 4 pour informations sur l'obtention de la valeur du hachage de clé.

Cause 4

Le hachage de clé publique SSC est erroné ou manquant.

Dépanner

Procédez comme suit :

1. Émettez la commande **debug lwapp events enable**.Vérifiez qu'AP essaye de se joindre.
2. Émettez la commande **show auth-list**.Cette commande montre le hachage de clé publique que le contrôleur a dans la mémoire.
3. Émettez la commande **debug pm pki enable**.Cette commande montre le hachage de clé

publique réel. Le hachage de clé publique réel doit correspondre au hachage de clé publique que le contrôleur a dans la mémoire. Une différence cause le problème. C'est un exemple de sortie de ce message de débogage :

```
(Cisco Controller) > debug pm pki enable

Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle...
Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert>
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
>bsnDefaultRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscoDefaultMfgCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert<
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
Data
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
2a864886 f70d0101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
3082010a 02820101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
43b95a34 49292e11
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
56f0ad91 2d61a389
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
b5cf7cef 06ba4375
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
774ce74e 9e2fde19
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
65d8639b d63aa0e3
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
9cd31041 b0734a55
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
c54e75f2 6d28fc6b
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
02d37140 7c9c865a
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
bc1acc13 0d334aa6
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
23311756 8302b8b8
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
280cbed1 49b2d50f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This is the actual SSC key-hash value. Mon May 22 06:34:14 2006: LWAPP Join-Request
```

```
MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14
2006: spamRadiusProcessResponse: AP Authorization failure for
00:0e:84:32:04:f0
```

Résolution

Procédez comme suit :

1. Copiez le hachage de la clé publique situé dans la sortie de la commande **debug pm pki enable** et employez-le pour substituer le hachage de la clé publique dans la liste d'authentification.
2. Émettez la commande **config auth-list add ssc AP_MAC AP_key** afin d'ajouter l'adresse MAC AP et le hachage de la clé à la liste d'autorisation :C'est un exemple de cette commande :
```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Cause 5

Il y a corruption d'un certificat ou d'une clé publique sur AP.

Dépanner

Complétez cette étape :

Émettez les commandes **debug lwapp errors enable** et **debug pm pki enable**.

Vous voyez des messages qui indiquent que des certificats ou des clés sont altérés.

Résolution

Employez l'une de ces deux options afin de résoudre le problème :

- MIC AP - Demander une autorisation de retour de matériel (RMA).
- SSC AP - Rétrograder au logiciel Cisco IOS Version 12.3(7)JA.Accomplissez ces étapes afin de rétrograder :

1. Utilisez le bouton de réinitialisation.
2. Effacez les paramètres du contrôleur.
3. Réexécutez la mise à niveau.

Cause 6

Le contrôleur pourrait fonctionner en mode couche 2.

Dépanner

Complétez cette étape :

Vérifiez le mode de fonctionnement du contrôleur.

Les AP convertis supportent seulement la découverte de la couche 3. Les AP convertis ne supportent pas la découverte de la couche 2.

Résolution

Procédez comme suit :

1. Définissez le WLC pour être en mode couche 3.
2. Redémarrez et donnez à l'interface du gestionnaire AP une adresse IP dans le même sous-réseau que l'interface de gestion.Si vous avez un port de service, comme le service port sur 4402 ou 4404, vous devriez l'avoir dans un super-réseau différent du gestionnaire AP et des interfaces de gestion.

Cause 7

Vous voyez cette erreur pendant la mise à niveau :

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Dépanner

Quand vous voyez cette erreur, complétez ces étapes :

1. Vérifiez que votre serveur TFTP est correctement configuré.Si vous utilisez l'outil de mise à niveau incorporé dans le serveur TFTP, un coupable commun est le logiciel du pare-feu personnel, qui bloque l'entrant TFTP.
2. Vérifiez si vous utilisez l'image correcte pour la mise à niveau.La mise à niveau au mode léger exige une image spéciale et ne fonctionne pas avec les images normales de mise à niveau.

Cause 8

Vous recevez ce message d'erreur sur AP après la conversion :

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

L'AP se recharge après 30 secondes et recommence le processus.

Résolution

Complétez cette étape :

Vous avez un SSC AP. Une fois que vous convertissez au LWAPP AP, ajoutez le SSC et son adresse MAC sous la liste d'authentification AP dans le contrôleur.

Conseils de dépannage

Ces conseils peuvent être utilisés quand vous mettez à niveau de l'autonome vers le mode LWAPP :

- Si le NVRAM n'est pas effacé quand le contrôleur essaye d'écrire dessus après la conversion, des problèmes se produisent. Cisco recommande d'effacer la configuration avant que vous convertissiez AP en LWAPP. Afin d'effacer la configuration :Dans l'IOS GUI — Allez à **System Software > System Configuration > Reset to Defaults**, ou **Reset to Defaults Except IP**.Dans CLI - Émettez les commandes **write erase** et **reload** et ne permettez pas à la configuration d'être sauvegardée une fois invité de le faire.Ceci facilite également la création des fichiers texte des AP devant être convertis par l'outil de mise à niveau étant donné que les entrées deviennent <ip address>, Cisco, Cisco, Cisco.
- Cisco recommande que vous utilisiez le tftp32. Vous pouvez télécharger le dernier serveur TFTPD à http://tftpd32.jounin.net/.
- Si un pare-feu ou une liste de contrôle d'accès est activé pendant le processus de mise à niveau, l'outil de mise à niveau peut devenir incapable de copier le fichier qui contient les variables environnementales d'un poste de travail à un AP.Si un pare-feu ou une liste de contrôle d'accès bloque la copie et vous sélectionnez l'option Use Upgrade Tool TFTP Server, vous ne pouvez pas poursuivre la mise à niveau parce que l'outil ne peut pas mettre à niveau les variables environnementales, et le téléchargement de l'image à AP échoue.
- Vérifiez une deuxième fois l'image à laquelle vous essayez de mettre à niveau. La mise à niveau des images IOS vers LWAPP est différente des images IOS normales.Sous Mes documents/Mon ordinateur--> outils--> Options de dossier, veillez à décocher la case à cocher **Hide file extensions for known file types**.
- Veillez toujours à utiliser le plus récent outil de mise à niveau et image de rétablissement de mise à niveau. Les dernières versions sont disponibles au centre logiciel sans fil.
- Un AP ne peut pas démarrer un fichier image **.tar**. C'est une archive, semblable aux fichiers zip. Vous devez dégrouper le fichier **.tar** dans AP flash avec la commande **archive download**, ou bien sortez d'abord l'image amorçable du fichier tar, puis mettez l'image amorçable dans AP flash.

Informations connexes

- Passer les points d'accès autonomes de Cisco Aironet au mode léger
- Réinitialisation de la configuration LWAPP sur AP léger (LAP)
- Exemple de configuration de DHCP OPTION 43 basculement pour les points d'accès légers Cisco Aironet
- Comment récupérer la clé d'informations parasites outre du Point d'accès et l'importer sur le contrôleur
- Peut le point d'accès autonome de Cisco Aironet être converti en point d'accès léger Protocol (LWAPP) utilisant le CLI
- Support et documentation techniques - Cisco Systems