Exemple de configuration de certificats importants localement sur les contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document explique comment configurer le contrôleur LAN Sans fil (WLC) et le Point d'accès léger (recouvrements) pour utiliser localement - la caractéristique significative de certificat. Cette fonction a été introduite dans la version 5.2 du contrôleur de réseau local sans fil. Avec cette configuration, si vous choisissez de contrôler l'Infrastructure à clés publiques (PKI), vous pouvez générer localement - les Certificats significatifs (LSC) sur les Points d'accès et les contrôleurs. Ces Certificats peuvent alors être utilisés pour authentifier mutuellement le WLC et POUR ENROULER.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer le WLC, le RECOUVREMENT, et la carte de client

sans fil pour le fonctionnement de base
- La connaissance de la façon configurer et utiliser le serveur du Microsoft Windows 2003 CA
- La connaissance de l'infrastructure de clé publique et des Certificats numériques

Composants utilisés

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

- Gamme Cisco 4400 WLC qui exécute les micrologiciels 5.2
- Point d'accès léger (LAP) de Gamme Cisco Aironet 1130 AG
- Serveur de Microsoft Windows 2003 configuré comme contrôleur de domaine, et en tant que serveur d'autorité de certification.
- Adaptateur de client du 802.11 a/b/g de Cisco Aironet qui exécute la version de microprogramme 4.2
- Cisco Aironet Desktop Utility (ADU) ce exécute la version 4.2 de micrologiciels

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.

Localement - Certificats significatifs

Dans des versions de logiciel de logiciel contrôleur plus tôt que 5.2.157.0, le contrôleur peut employer les Certificats auto-signés (SSCs) pour authentifier des Points d'accès ou pour envoyer les informations d'autorisation à un serveur de RAYON, si les Points d'accès fabrication-ont installé des Certificats (MICs). Dans la version de logiciel de logiciel contrôleur 5.2.157.0, vous pouvez configurer le contrôleur pour utiliser un certificat significatif local (LSC). Vous pouvez utiliser un LSC si vous voulez que votre propre Infrastructure à clés publiques (PKI) fournisse une meilleure Sécurité ; pour avoir le contrôle de votre Autorité de certification (CA), et définir des stratégies, des restrictions, et des utilisations sur les Certificats générés.

Le nouveau LSC délivre un certificat les besoins d'abord et puis de provisioned sur le contrôleur le RECOUVREMENT du serveur d'Autorité de certification (CA).

Le RECOUVREMENT communique avec le contrôleur (WLC) avec le protocole CAPWAP. Toutes les demandes de signer le certificat et de délivrer les Certificats CA pour le RECOUVREMENT et pour le WLC lui-même, doivent être initiées du WLC. Le RECOUVREMENT ne communique pas directement avec le serveur CA. Le WLC se comporte comme Ca-proxy à AP du LWAPP. Les petits groupes de serveur CA doivent être configurés sur le WLC, et il doit être accessible.

Le contrôleur se sert de l'inscription de certificat simple Protocol (SCEP) pour expédier les certReqs générés sur les périphériques au CA et se sert de SCEP de nouveau pour obtenir les Certificats signés du CA.

SCEP est un protocole de gestion de certificat que les clients d'Infrastructure à clés publiques (PKI) et les serveurs d'autorité de certification les utilisent pour prendre en charge l'inscription de certificat et la révocation. Il est très utilisé à Cisco et est pris en charge par beaucoup de Ca-serveurs. Dans le protocole SCEP, le HTTP est utilisé comme protocole de transport pour les messages de PKI. L'objectif principal de SCEP est l'émission sécurisée des Certificats aux périphériques de réseau. SCEP est capable de beaucoup d'exécutions, mais pour ces projet et release, SCEP est utilisé pour ces exécutions.

- La distribution de clé de public CA et de RA
- Inscription de certificat

Toutes les transactions SCEP se produisent en mode automatique. La révocation de certificat n'est pas prise en charge.

Remarque: Des LSC ne sont pas pris en charge sur les Points d'accès qui sont configurés pour le mode de passerelle.

Ravitaillement de certificat sur les contrôleurs LAN Sans fil (WLCs)

Les nouveaux Certificats LSC, le CA et les Certificats de périphérique doivent être installés sur le contrôleur.

Avec le protocole SCEP, les Certificats CA sont reçus du serveur CA. Depuis en ce moment, il n'y a aucun Certificats actuel sur le contrôleur, cette exécution est un clair obtiennent l'exécution. Ceux-ci sont installés sur le contrôleur. Ces mêmes Certificats CA sont également poussés aux aps quand les aps provisioned avec des LSC.

Exécution d'inscription de certificat de périphérique

Pour le RECOUVREMENT et le contrôleur qui demande un CA certificat signé, le certRequest est envoyé comme message PKCS#10. Le certRequest contient le nom du sujet, PublicKey et d'autres attributs à inclure dans le certificat X.509, et digitalement signés par le PrivateKey du demandeur. Ceux-ci doivent être envoyés au CA, qui transforme le certRequest en certificat X.509.

Le CA qui reçoit un PKCS#10 certRequest exige des informations complémentaires d'authentifier l'identité de demandeur et de la vérifier que la demande est inchangée. Beaucoup de fois PKCS#10 ont combiné avec d'autres approches, telles que PKCS#7, pour envoyer et recevoir le CERT Reqs/Resps.

Ici, le le PKCS#10 est enveloppé dans un type de message PKCS#7 SignedData. Ceci est pris en charge en tant qu'élément de la fonctionnalité de client SCEP, alors que le message de PKCSReq est envoyé au contrôleur.

Sur l'exécution réussie d'inscription, le CA et le certificat de périphérique sont maintenant présents sur le contrôleur.

Ravitaillement de certificat sur LWAPP AP

Pour qu'un nouveau certificat provisioned sur le RECOUVREMENT, alors qu'en mode CAPWAP le RECOUVREMENT doit pouvoir obtenir le nouveau certificat X.509 signé. Afin de faire ceci, il envoie un certRequest au contrôleur, qui agit en tant que Ca-proxy et les aides obtiennent le certRequest signé par le CA pour le RECOUVREMENT.

Le certReq et les certResponses sont envoyés au RECOUVREMENT avec les charges utiles LWAPP. Ce diagramme affiche que l'écoulement pour le RECOUVREMENT provision un LSC.

Voici les étapes en détail :

1. Le ravitaillement du RECOUVREMENT avec de plus nouveaux LSC se produit une fois que le RECOUVREMENT est dans l'état HAUT, après qu'il AIT JOINT le WLC avec son courant MIC/SSC. Dans la phase de ravitaillement LSC, quoiqu'AP soit dans l'état HAUT, les radios sont de force arrêtées.
2. La fourniture d'utiliser-et du LSC doit être activée sur le WLC. Ce processus inclut pour activer le LSC, pour ajouter le serveur CA, et pour configurer d'autres paramètres. Les paramètres d'un certificat LSC commandent la demande est envoyés du contrôleur POUR ENROULER, avec le subject-name, le temps de validité et Keysize réglé dans la charge utile. Ces champs sont utilisés par le RECOUVREMENT quand le certRequest est créé. La charge utile indique également que le RECOUVREMENT doit créer un certRequest et l'envoyer de nouveau au contrôleur.
3. Le RECOUVREMENT génère configuré keysize paire de clés RSA publique/privée. Après la génération du keypair, un certRequest est généré après le SubjectName reçu du contrôleur est configuré. La NC autogenerated avec le format existant SSC/MIC, « Cxxxx-EtherMacAddr ». Le RECOUVREMENT génère un PKCS#10 CertReq et l'envoie comme charge utile, demande de certificat LSC, au contrôleur.
4. Le contrôleur crée alors un message SSCEP PKCSReq, un message PKCS#7 formaté, et l'envoie au CA au nom du : ENROULEZ, afin d'obtenir la demande de certificat signée par le CA configuré. Les CERT installés CA/RA sont utilisés pour chiffrer le certReq.
5. Si le CA peut approuver la demande de certificat, un message de CertRep avec Status=SUCCESS est renvoyé au client SSCEP (contrôleur) dans un format PKCS#7. La réponse de CERT est écrite localement dans un fichier comme certificat de format PEM.
6. Puisque ce CertResp est pour le RECOUVREMENT, WLC envoie le certificat au RECOUVREMENT avec une charge utile « réponse de certificat ». Le CERT CA est envoyé d'abord avec la même charge utile, puis le certificat de périphérique est introduit une charge utile distincte.

Le LSC CA et les Certificats de périphérique de RECOUVREMENT sont installés dans le RECOUVREMENT, et les auto-réinitialisations de système. La prochaine fois qu'il monte, puisqu'il est configuré pour utiliser des LSC, AP envoie le certificat de périphérique LSC au contrôleur en tant qu'élément de la demande de jonction. En tant qu'élément de la réponse de jonction, le contrôleur envoie son nouveau certificat de périphérique et valide également le certificat d'arrivée de RECOUVREMENT avec le nouveau certificat racine CA.

Remarque: Des LSC ne sont pas pris en charge sur les Points d'accès qui sont configurés pour le mode de passerelle.

Support LSC sur les contrôleurs LAN Sans fil (WLCs) et le Point d'accès léger (recouvrements)

Le LSC est pris en charge sur ces Plateformes WLC :

- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Contrôleurs de réseau local sans fil de la gamme Cisco 2100
- Module de services sans fil (WiSM) des gammes Cisco Catalyst 6500/7600

- Contrôleur de réseau local sans fil intégré Cisco Catalyst 3750G
- Module contrôleur de réseau local sans fil Cisco

Le LSC est pris en charge sur les Points d'accès C1130, C1140, C1240, C1252 de Cisco Aironet et tous les nouveaux Points d'accès.

Le LSC n'est pas pris en charge sur la MAILLE AP (1510, 1522), le mode AP de passerelle.

Ce document explique avec un exemple de configuration, comment activer et authentifier des recouvrements avec localement - les Certificats significatifs.

Configurez

Remarque: Localement - la caractéristique significative de certificat peut être activée par le GUI ou le CLI sur le contrôleur.

Remarque: La caractéristique LSC sur un contrôleur ne prend pas le défi de mot de passe. Par conséquent, pour que le LSC fonctionne, vous devez désactiver le défi de mot de passe sur le serveur CA. En outre, vous ne pouvez pas utiliser la Microsoft Windows Server 2008 en tant que serveur CA parce qu'il n'est pas possible de désactiver le défi de mot de passe là-dessus.

Configuration du réseau

Dans cet exemple, vous configurez un contrôleur LAN de 4400 radios et un point d'accès léger de gamme 1130 pour utiliser localement - les Certificats significatifs (LSC). Afin d'accomplir ceci, vous devez provision le contrôleur LAN Sans fil et le RECOUVREMENT avec des LSC du serveur d'Autorité de certification (CA).

Ce document utilise le serveur de Microsoft Windows 2003 en tant que serveur CA.

Procédure d'installation CA et SCEP

Le document suppose que la configuration du serveur CA sur le serveur de Microsoft Windows 2003 est en place. Voici le résumé des étapes pour la procédure d'installation CA et SCEP :

1. L'installation Windows 2003 et le serveur CA, s'assurent le travail de *http://ca-server/certsrv*
2. Téléchargement *cepsetup.exe de* site Web de Microsoft
3. Installez cepsetup.exe, décochez « l'*expression de défi de* RequireSCEP *»,* puisque WLC ne pourrait pas prendre en charge le défi s'inscrit le mode maintenant.
4. Fournissez le nom, l'email, le pays, ville et les autres petits groupes.
5. Assurez les travaux de *http://ca-server/certsrv/mscep/mscep.dll* comme prévus.

Remarque: Vous devrez créer un compte utilisateur, l'assigner lisez et inscrivez-vous les autorisations pour le modèle d'IPSec (demande hors ligne), et faites-lui un membre du groupe IIS_WPG. Pour les détails complets référez-vous au site Web de Microsoft pour installer et configurer SCEP

Configurez le contrôleur LAN Sans fil par le GUI

Procédez comme suit :

1. Du GUI Sans fil de contrôleur LAN, cliquez sur Security **> certificat > LSC** afin d'ouvrir la page significative locale des Certificats (LSC).
2. Cliquez sur l'**onglet Général**.
3. Afin d'activer le LSC sur le système, cochez l'**enable LSC sur la** case de **contrôleur**.
4. Dans le champ URL de serveur CA, écrivez l'URL au serveur CA. Vous pouvez écrire un nom de domaine ou une adresse IP.
5. Dans les domaines de params, entrez les paramètres pour le certificat de périphérique. La taille de clé est une valeur de 384 à 2048 (dans les bits), et la valeur par défaut est 2048.
6. Cliquez sur **Apply** pour valider les modifications.
7. Afin d'ajouter le certificat de CA dans la base de données de certificat de CA du contrôleur, planer votre curseur au-dessus de la flèche déroulante bleue pour le type de certificat, et choisir **ajoutent**. Voici un exemple.
8. Afin de provision le LSC sur le Point d'accès, cliquer sur l'**onglet Préconfiguration AP**, et cocher la case de **ravitaillement de l'enable AP**.
9. Afin d'ajouter des Points d'accès à la liste de disposition, écrivez l'adresse MAC de Point d'accès dans la zone adresse d'adresses MAC Ethernet AP et cliquez sur Add. Afin d'enlever un Point d'accès de la liste de disposition, planer votre curseur au-dessus de la flèche déroulante bleue pour le Point d'accès, et choisir **retirent**.Si vous configurez une liste de disposition de Point d'accès, seulement les Points d'accès dans la liste de disposition provisioned quand vous activez le ravitaillement AP. Si vous ne configurez pas une liste de disposition de Point d'accès, tous les Points d'accès avec un certificat MIC ou de SSC qui joignent le contrôleur sont LSC provisioned.
10. Cliquez sur **Apply** pour valider les modifications.

Configurez le contrôleur LAN Sans fil par le CLI

Référez-vous à **employer le CLI pour configurer la** section **LSC du** guide de configuration Sans fil de contrôleur LAN de Cisco, version 5.2 pour les informations sur la procédure activer localement - la caractéristique significative du certificat (LSC) du CLI sur le contrôleur.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Une fois que le contrôleur LAN Sans fil est configuré et le serveur CA est en place, le contrôleur LAN Sans fil emploie le protocole SCEP afin de communiquer avec le serveur CA et saisir le certificat LSC. Voici un tir d'écran du WLC une fois que le certificat est installé.

Quand le RECOUVREMENT est soulevé, le RECOUVREMENT découvre le WLC avec la couche des mécanismes de détection de 2 couches 3 et envoie des demandes de jonction au contrôleur avec le certificat MIC.

Le contrôleur LAN Sans fil envoie alors la demande de paramètre de certificat LSC au RECOUVREMENT.

Le SubjectName/CN étant envoyé du WLC, AP génère PKCS #10 CertReq et envoie « une

demande de certificat LWAPP LSC » au WLC.

Cette demande consécutivement est expédiée par le WLC au serveur CA. Le serveur CA envoie le certificat du RECOUVREMENT LSC au contrôleur. Le contrôleur envoie alors le LSC au RECOUVREMENT.

Ce message apparaît sur AP CLI.

```
The name for the keys will be: Cisco_IOS_LSC_Keys

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
LSC CA cert successfully imported
LSC device cert successfully imported
```

En conclusion, le RECOUVREMENT envoie une demande de jonction avec le LSC.

Émettez la commande d'**enable d'événements de capwap de débogage** afin de visualiser cette séquence d'opérations.

Une fois le RECOUVREMENT s'inscrit au WLC avec le LSC, vous peut confirmer ceci sur le GUI WLC.

Vous pouvez également employer ces commandes du WLC CLI afin de vérifier ceci. Voici un exemple :

```
show certificate lsc summary Information similar to the following appears: LSC
Enabled..................................... Yes LSC CA-
Server...................................... http://10.77.244.201:8080/caserver LSC AP-
Provisioning................................ Yes Provision-
List.............................. Not Configured LSC Revert Count in AP
reboots................... 3 LSC Params: Country..................................... 4
State....................................... ca
City........................................ ch
Orgn........................................ abc
Dept........................................ xyz
Email....................................... abc@abc.com
KeySize..................................... 2048 LSC Certs: CA
Cert.................................... Not Configured RA
Cert.................................. Not Configured
```

Afin de visualiser des détails au sujet des Points d'accès qui provisioned avec le LSC, sélectionnez cette commande :

```
show certificate lsc ap-provision Information similar to the following appears: LSC AP-
Provisioning.......................... Yes Provision-List.............................
Present Idx Mac Address --- ------------ 1 00:18:74:c7:c0:90
```

Dépannez

Cette section explique comment dépanner votre configuration. Vous pouvez employer la commande d'**enable de scep de PKI de debug pm** afin de visualiser la séquence d'opérations.

Voici un exemple d'un réussi mettent au point le log :

```
Success log:
```

WLC

```
(Cisco Controller) >

scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:21.455:
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 06:52:27.526:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 06:52:30 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 06:52:34.463:
```

AP

```
(Cisco Controller) >
scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:47.471:
scep: waiting for 10 secs 06:53:00.479:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:01.542:
scep: data payload size: 797 bytes:
scep: successfully encrypted payload
scep: envelope size: 1094 bytes545:
scep: Sender Nonce before send: 089AC8C4604FCEB10C1F30E045073B10
scep: creating outer PKCS#7:01.545:
scep: signature added successfully:
scep: adding signed attributes.545:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.565:
scep: base64 encoded payload size: 3401 bytes

scep: Sent 3646 bytesed: Operation now in progress*sshpmLscTask: Nov 23 06:53:01.613:
scep: SenderNonce in reply: BF4EE64D4169584D90B2502ECCC0C133
scep: recipientNonce in reply: 089AC8C4604FCEB10C1F30E045073B10
scep: Http response is <HTTP/1.1 200 OK>
```

```
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Wed, 23 Nov 2011 06:53:02 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 2549>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#706:53:13.488:
scep: PKCS#7 payload size: 2549 bytes8:
scep: PKCS#7 contains 2023 bytes of enveloped data
scep: verifying signature 06:53:13.489:
scep: signature ok Nov 23 06:53:13.490:
scep: finding signed attributes:13.490:
scep: finding attribute transId:13.490:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: A984A2DFE20DA7E0FE702DC8EC307F33
scep: finding attribute messageType490:
scep: allocating 1 bytes for attribute.
scep: reply message type is good13.490:
scep: finding attribute senderNonce490:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus3.491:
scep: allocating 1 bytes for attribute.
scep: pkistatus: SUCCESS3 06:53:13.491: scep: reading inner PKCS#706:53:13.491: scep: decrypting
inner PKCS#753:13.492: scep: found certificate: subject: /serialNumber= PID:AIR-LAP1262N-A-K9
SN:FTX1433K60R/C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=AP3G1-f866f267577e/emailAddress= tls@ccie.com
issuer: /DC=com/DC=ccie/CN=AD scep: PKCS#7 payload size: 1580 bytes:53:13.518: Digital
Signature, Key Encipherment scep: waiting for 10 secs 06:53:13.520:
```

C'est un exemple d'un cas où il échoue :

```
Fail log
WLC
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 23 00:57:52.407:
scep: waiting for 10 secs 00:58:05.415:
scep: waiting for 10 secs 00:58:18.423:
scep: waiting for 10 secs 00:58:31.431:
scep: waiting for 10 secs 00:58:44.439:
scep: waiting for 10 secs 00:58:57.447:
scep: waiting for 10 secs 00:59:10.455:
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 00:59:22.486:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 00:59:22 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
```

```
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 00:59:23.463:

AP:
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 22 18:06:22.100:
scep: waiting for 10 secs 18:06:35.108:
scep: waiting for 10 secs 18:06:48.116:
scep: waiting for 10 secs 18:07:01.124:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:04.631:
scep: data payload size: 536 bytes:
scep: successfully encrypted payload
scep: envelope size: 838 bytes.633:
scep: Sender Nonce before send: F8BBA9EB06579188A62635A1DFA6510A
scep: creating outer PKCS#7:04.634:
scep: signature added successfully:
scep: adding signed attributes.634:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.655:
scep: base64 encoded payload size: 3055 bytes

scep: Sent 3280 bytesed: Operation now in progress*sshpmLscTask: Nov 22 18:07:04.690:
scep: SenderNonce in reply: 69A4BF610ED41746B1066B5BEC4427F0
scep: recipientNonce in reply: F8BBA9EB06579188A62635A1DFA6510A
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Tue, 22 Nov 2011 18:07:04 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 540>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#718:07:14.133:
scep: PKCS#7 payload size: 540 bytes33:
scep: PKCS#7 contains 1 bytes of enveloped data
scep: verifying signature 18:07:14.134:
scep: signature ok Nov 22 18:07:14.135:
scep: finding signed attributes:14.135:
scep: finding attribute transId:14.135:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: 3DA1646840CD4FFEB1534EA8F1D45F76
scep: finding attribute messageType135:
scep: allocating 1 bytes for attribute.
scep: reply message type is good14.135:
scep: finding attribute senderNonce135:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus4.136:
```

```
scep: allocating 1 bytes for attribute.
scep: pkistatus: FAILURE2 18:07:14.136:
scep: finding attribute failInfo14.136: scep: allocating 1 bytes for attribute. scep: reason:
Transaction not permitted or supported scep: waiting for 10 secs 18:07:14.136: scep: waiting for
10 secs 18:07:27.144: scep: waiting for 10 secs 18:07:40.152: scep: waiting for 10 secs
18:07:53.160: scep: waiting for 10 secs 18:08:06.168: scep: waiting for 10 secs 18:08:19.176:
scep: waiting for 10 secs 18:08:32.184: scep: waiting for 10 secs 18:08:45.192: scep: waiting
for 10 secs 18:08:58.200: scep: waiting for 10 secs 18:09:11.208:
```

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 5.2
- Génération de la demande de signature de certificat (CSR) pour un tiers certificat sur un contrôleur WLAN (WLC)
- Génération de demande de signature de certificat pour un tiers certificat et procédure pour télécharger les Certificats enchaînés au WLC
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems