PEAP sous des réseaux sans fil unifié avec ACS 5.1 et serveur Windows 2003

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Entreprise 2003 de Windows installée avec IIS, autorité de certification, DN, DHCP (CA)
CA (democa)
Secure ACS 5.1 de Cisco 1121
Installation utilisant l'appliance de la gamme CSACS-1121
Installez le serveur ACS
Configuration de contrôleur de Cisco WLC5508
Créez la configuration nécessaire pour WPAv2/WPA
Authentification PEAP
Installez les modèles de certificat SNAP-dans
Créez le modèle de certificat pour le serveur Web ACS
Activez le nouveau modèle de certificat de serveur Web ACS
Installation de certificat ACS 5.1
Configurez le certificat exportable pour ACS
Installez le certificat en logiciel ACS 5.1
Configurez la mémoire d'identité ACS pour le Répertoire actif
Ajoutez un contrôleur à ACS en tant que client d'AAA
Configurez les stratégies ACS Access pour la radio
Créez la stratégie ACS Access et la règle de service
Configuration de CLIENT pour le PEAP utilisant des Windows Zero Touch
Exécutez une installation et une configuration de base
Installez l'adaptateur réseau sans fil
Configurez la connexion réseau sans fil
Dépannez l'authentification Sans fil avec ACS
L'authentification PEAP échoue avec le serveur ACS
Informations connexes

Introduction

Ce document décrit comment configurer l'accès sans fil sécurisé à l'aide des contrôleurs de

réseau local sans fil, du système d'exploitation Microsoft Windows 2003 et du Cisco Secure Access Control Server (ACS) 5.1 par l'intermédiaire du protocole PEAP avec la version 2 du Protocole d'authentification de négociation par défi Microsoft (MS-CHAP).

Remarque: Pour des informations sur le déploiement de sécurisez la radio, référez-vous au site Web de WiFi de Microsoft et au plan détaillé Sans fil SÛR de Cisco.

Conditions préalables

Conditions requises

Il y a une supposition que l'installateur a la connaissance de l'installation Sans fil de base d'installation de Windows 2003 et de contrôleur LAN de Cisco pendant que ce document couvre seulement les configurations spécifiques pour faciliter les tests.

Pour l'installation initiale et les informations de configuration pour les contrôleurs de gamme Cisco 5508, référez-vous au guide d'installation Sans fil de contrôleur de gamme Cisco 5500. Pour l'installation initiale et les informations de configuration pour les contrôleurs de gamme Cisco 2100, référez-vous au guide de démarrage rapide : Contrôleur LAN sans fil de la gamme Cisco 2100.

Les guides d'installation et de configuration de Microsoft Windows 2003 peuvent être trouvés sous Installer Windows Server 2003 R2.

Avant de commencer, installez Microsoft Windows Server 2003 avec le système d'exploitation SP sur chacun des serveurs dans le laboratoire de test et mettez à jour tous les Services Pack. Installez les contrôleurs et les points d'accès léger (LAP) et assurez-vous que les dernières mises à jour logicielles sont configurées.

Les Windows Server 2003 avec le SP1, Enterprise Edition, sont utilisés de sorte que l'Auto-inscription des Certificats d'utilisateur et de poste de travail pour l'authentification PEAP puisse être configurée. L'Auto-inscription de certificat et autorenewal le facilitent pour déployer des Certificats et pour améliorer la Sécurité automatiquement en expirant et en renouvelant des Certificats.

Composants utilisés

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

- Contrôleur de gamme Cisco 2106 ou 5508 qui passages 7.0.98.0
- Point d'accès léger de Cisco 1142 Protocol (LWAPP) AP
- Entreprise de Windows 2003 avec l'Internet Information Server (IIS), l'Autorité de certification (CA), le DHCP, et le Système de noms de domaine (DNS) installé
- Cisco 1121 sécurisent l'appliance de système de contrôle d'accès (ACS) 5.1
- Windows XP Professionnel avec le fournisseur de services (et les Services Pack mis à jour) et le network interface card Sans fil (NIC) (avec CCX support v3) ou le suppliant de tiers.
- Commutateur de Cisco 3750

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.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Topologie de travaux pratiques Sans fil Cisco Secure
L'objectif principal de ce document est de te fournir la procédure pas à pas pour implémenter le PEAP sous des réseaux sans fil unifié avec ACS 5.1 et le serveur d'entreprise de Windows 2003. L'accent principal est sur l'Auto-inscription du client de sorte que les autos-enrolls de client et prend le certificat du serveur.

Remarque: Afin d'ajouter l'accès protégé par Wi-Fi (WPA)/WPA2 avec la norme de chiffrement du Protocole TKIP (Temporal Key Integrity Protocol) /Advanced (AES) au Windows XP Professionnel avec le fournisseur de services, se rapportent à la mise à jour de l'élément d'information de services de ravitaillement WPA2/Wireless (IE WPS) pour Windows XP avec le Service Pack 2.

Entreprise 2003 de Windows installée avec IIS, autorité de certification, DN, DHCP (CA)

CA (democa)

Le CA est un ordinateur qui exécute les Windows Server 2003 avec le SP2, Enterprise Edition, et exécute ces rôles :

- Un contrôleur de domaine pour le **domaine demo.local** qui exécute IIS
- Un serveur DNS pour le domaine de **DN demo.local**
- Un serveur DHCP
- Racine CA d'entreprise pour le **domaine demo.local**

Exécutez ces étapes afin de configurer le CA pour ces services :

1. Exécutez une installation et une configuration de base.
2. Configurez l'ordinateur comme contrôleur de domaine.
3. Élevez le niveau fonctionnel de domaine.

4. Installez et configurez le DHCP.
5. Installez les services de certificat.
6. Vérifiez les privilèges d'administrateur pour des Certificats.
7. Ajoutez les ordinateurs au domaine.
8. Permettez l'accès à l'ordinateur Sans fil.
9. Ajoutez les utilisateurs au domaine.
10. Permettez l'accès Sans fil aux utilisateurs.
11. Ajoutez les groupes au domaine.
12. Ajoutez les utilisateurs au groupe de wirelessusers.
13. Ajoutez les ordinateurs client au groupe de wirelessusers.

Exécutez l'installation et la configuration de base

Effectuez les étapes suivantes :

1. Installez les Windows Server 2003 avec le SP2, Enterprise Edition, en tant que serveur autonome.
2. Configurez le protocole TCP/IP avec l'adresse IP de *10.0.10.10* et le masque de sous-réseau de *255.255.255.0*.

Configurez l'ordinateur comme contrôleur de domaine

Effectuez les étapes suivantes :

1. Afin de commencer l'assistant d'installation de Répertoire actif, choisissez le **Start > Run**, **tapez dcpromo.exe, et** cliquez sur OK**.**
2. Sur l'accueil à la page d'assistant d'installation de Répertoire actif, cliquez sur Next.
3. Àla page du système d'exploitation de compatibilité, cliquez sur Next.
4. Àla page de type de contrôleur de domaine, le **contrôleur de domaine** choisi **pour un nouveau domaine** et cliquent sur Next.
5. Àla nouvelle page de domaine de création, le **domaine** choisi **dans une nouvelle forêt** et cliquent sur Next.
6. Sur l'installer ou configurez la page de DN, sélectionnez l'**aucun, juste installez et configurez les DN sur cet ordinateur** et cliquez sur Next.
7. Àla page de nouveau nom de domaine, le type **demo.local et** cliquent sur Next**.**
8. Àla page de nom de domaine de Netbios, écrivez le nom NetBIOS de domaine comme **démonstration** et cliquez sur Next.
9. Dans les répertoires de base de données et de log que les emplacements paginent, reçoivent la base de données par défaut et se connectent les répertoires de répertoires et cliquent sur Next.
10. Dans la page partagée de volume de système, vérifiez que l'emplacement de dossier par défaut est correct et cliquez sur Next.
11. Sur les autorisations paginez, vérifiez que des **autorisations compatibles seulement avec le Windows 2000 ou les systèmes d'exploitation Windows Server 2003** est sélectionnées et cliquez sur Next.
12. Sur les services d'annuaire restaurez la page de mot de passe de gestion de mode, laissez le blanc de cadres Password et cliquez sur Next.
13. Examinez les informations à la page récapitulative et cliquez sur Next.

14. Quand vous êtes fait avec l'installation de Répertoire actif, cliquez sur Finish.
15. Une fois incité à redémarrer l'ordinateur, cliquez sur la **reprise maintenant**.

Élevez le niveau fonctionnel de domaine

Effectuez les étapes suivantes :

1. Ouvrez les **domaines et les confiances de Répertoire actif SNAP-**dans du répertoire d'**outils d'administration** (**Start > Programs > Administrative tools > domaines et confiances de Répertoire actif**), et puis cliquez avec le bouton droit l'ordinateur **CA.demo.local de** domaine.
2. Cliquez sur le **niveau fonctionnel de domaine d'augmenter**, et puis sélectionnez les **Windows Server 2003 à la** page de niveau fonctionnel de domaine d'augmenter.
3. Cliquez sur l'**augmenter**, cliquez sur OK, et puis cliquez sur OK de nouveau.

Installez et configurez le DHCP

Effectuez les étapes suivantes :

1. Installez le **protocole DHCP (DHCP)** comme composant de **service de réseau** à l'aide de **ajoutent ou retirent des programmes au** panneau de configuration.
2. Ouvrez le **DHCP SNAP-**dans du répertoire d'**outils d'administration** (**Start > Programs > Administrative tools > DHCP**), et puis mettez en valeur le serveur DHCP, **CA.demo.local.**
3. Cliquez sur l'**action**, et puis cliquez sur **autorisent** afin d'autoriser le service DHCP.
4. Dans l'arborescence de la console, le clic droit **CA.demo.local, et cliquent sur New alors la** portée.
5. Sur l'écran de bienvenue du nouvel assistant de portée, cliquez sur Next.
6. Àla page de nom de portée, type **CorpNet** dans la zone d'identification.
7. Cliquez sur Next et complétez ces paramètres :Adresse IP de début - **10.0.20.1**Adresse IP d'extrémité - **10.0.20.200**Longueur - **24**Masque de sous-réseau - **255.255.255.0**
8. Cliquez sur Next et entrez dans *10.0.20.1* pour l'adresse IP de début et *10.0.20.100* pour que l'adresse IP d'extrémité soit exclue. Cliquez ensuite sur **Next**. Ceci réserve les adresses IP dans la plage de 10.0.20.1 à 10.0.20.100. Ces adresses IP de réserve ne sont pas réparties par le serveur DHCP.
9. Àla page de durée de bail, cliquez sur Next.
10. Sur la page options DHCP de configurer, choisissez **oui, je veux configurer ces options maintenant** et cliquer sur Next.
11. Àla page de routeur (passerelle par défaut) ajoutez l'adresse du routeur par défaut de *10.0.20.1* et cliquez sur Next.
12. Sur le nom de domaine et les serveurs DNS paginez, tapez *demo.local dans le* domaine de domaine de parent, tapez 10.0.10.10 *dans le* domaine d'adresse IP, et puis cliquez sur Addand cliquent sur Next.
13. Àla page de serveurs WINS, cliquez sur Next.
14. Àla page de portée de lancement, choisissez **oui, je veux lancer cette portée maintenant** et cliquer sur Next.
15. Quand vous terminez avec la nouvelle page d'assistant de portée, cliquez sur Finish.

Installez les services de certificat

Effectuez les étapes suivantes :

Remarque: IIS doit être installé avant que vous installiez des services de certificat et l'utilisateur devrait faire partie de l'OU d'admin d'entreprise.

1. Au panneau de configuration, ouvert **ajoutez ou retirez les programmes**, et puis cliquez sur Add**/retirez les composants de Windows**.
2. Dans la page d'assistant de composants de Windows, choisissez les services de certificat, et puis cliquez sur Next.
3. Àla page de type CA, choisissez la racine CA d'entreprise et cliquez sur Next.
4. Dans la page de l'information d'identification CA, *democa de* type dans le nom commun pour cette case CA. Vous pouvez également écrire les autres détails facultatifs. Alors cliquez sur Next et recevez les par défaut sur la page Settings de base de données de certificat.
5. Cliquez sur **Next** (Suivant). À la fin de l'installation, cliquez sur Finish.
6. Cliquez sur OK après que vous ayez lu le message d'avertissement au sujet d'installer IIS.

Vérifiez les privilèges d'administrateur pour des Certificats

Effectuez les étapes suivantes :

1. Choisissez le **début** > les **outils d'administration** > l'**autorité de certification**.
2. **Le democa CA de** clic droit et cliquent sur alors **Properties**.
3. Sur l'onglet Sécurité, les **administrateurs de** clic dans le groupe ou les noms d'utilisateur les répertorient.
4. Dans les autorisations pour des administrateurs le répertoriez, vérifiez que ces options sont placées **de laisser** :Délivrez et gérez les CertificatsGérez le CACertificats de demandeSi l'un de ces sont placés pour refuser ou ne sont pas sélectionnés, placez les autorisations **de laisser**.
5. Cliquez sur OK pour fermer la boîte de dialogue Properties du democa CA, et puis clôturez l'autorité de certification.

Ajoutez les ordinateurs au domaine

Effectuez les étapes suivantes :

Remarque: Si l'ordinateur est déjà ajouté au domaine, poursuivez pour ajouter des utilisateurs au domaine.

1. Ouvrez les **utilisateurs et les ordinateurs de Répertoire actif SNAP-**dans.
2. Dans l'arborescence de la console, développez **demo.local.**
3. Cliquez avec le bouton droit les **ordinateurs**, cliquez sur New, et puis cliquez sur l'**ordinateur**.
4. Dans le nouvel objet – La boîte de dialogue d'ordinateur, introduisent le nom de l'ordinateur dans le domaine de nom de l'ordinateur et cliquent sur Next. Cet exemple utilise le *client de* nom de l'ordinateur.
5. Dans la boîte de dialogue gérée, cliquez sur Next.
6. Dans le nouvel objet – La boîte de dialogue d'ordinateur, cliquent sur Finish.
7. Répétez les étapes 3 à 6 afin de créer des comptes d'ordinateur supplémentaire.

Permettez l'accès à l'ordinateur Sans fil

Effectuez les étapes suivantes :

1. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, cliquez sur le répertoire d'**ordinateurs** et cliquez avec le bouton droit sur l'ordinateur pour lequel vous voulez assigner l'accès Sans fil. Cet exemple affiche la procédure avec le **client d'**ordinateur ce que vous avez ajouté dans le clic **Properties d'**étape 7., et puis va à l'**onglet Numérotation**.
2. Dans l'autorisation d'Accès à distance, choisissez **permettent l'accès** et cliquent sur OK.

Ajoutez les utilisateurs au domaine

Effectuez les étapes suivantes :

1. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, les **utilisateurs de** clic droit, cliquent sur New, et puis cliquent sur l'**utilisateur**.
2. Dans le nouvel objet – La boîte de dialogue d'utilisateur, introduisent le nom de l'utilisateur de sans fil. Cet exemple utilise le *wirelessuser de* nom dans le domaine de prénom, et le *wirelessuser* dans le domaine de nom de connexion d'utilisateur. Cliquez sur **Next** (Suivant).
3. Dans le nouvel objet - boîte de dialogue d'utilisateur, saisissez un mot de passe de votre choix dans le champ mot de passe, puis confirmez les champs du mot de passe. Effacez la case à cocher **User must change password at next logon**, puis cliquez sur **Next**.
4. Dans le nouvel objet - boîte de dialogue d'utilisateur, cliquez sur **Finish**.
5. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

Permettez l'accès sans fil aux utilisateurs

Effectuez les étapes suivantes :

1. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, cliquez sur le répertoire d'**utilisateurs**, cliquez avec le bouton droit le **wirelessuser**, cliquez sur **Properties**, et puis allez à l'**onglet Numérotation**.
2. Dans l'autorisation d'Accès à distance, choisissez **permettent l'accès** et cliquent sur OK.

Ajoutez les groupes au domaine

Effectuez les étapes suivantes :

1. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, les **utilisateurs de** clic droit, cliquent sur New, et puis cliquent sur le **groupe**.
2. Dans la nouvelle boîte de dialogue de groupe d'objets, introduisez le nom du groupe dans la zone d'identification de groupe et cliquez sur OK. Ce document utilise les *wirelessusers de* nom de groupe.

Ajoutez les utilisateurs au groupe de wirelessusers

Effectuez les étapes suivantes :

1. Dans le volet de détails des utilisateurs et des ordinateurs de Répertoire actif, double clic sur le groupe *WirelessUsers*.
2. Allez aux membres l'onglet et cliquez sur Add.
3. Dans les utilisateurs choisis, les contacts, boîte de dialogue d'ordinateurs, ou de groupes, introduisent le nom des utilisateurs que vous voulez ajouter au groupe. Cet exemple affiche comment ajouter le *wirelessuser d'*utilisateur au groupe. Cliquez sur **OK**.
4. Dans les plusieurs noms la boîte de dialogue trouvée, cliquent sur OK. Le compte utilisateur de wirelessuser est ajouté au groupe de wirelessusers.
5. Cliquez sur OK afin de sauvegarder des modifications au groupe de wirelessusers.
6. Répétez cette procédure pour ajouter plus d'utilisateurs au groupe.

Ajoutez les ordinateurs client au groupe de wirelessusers

Effectuez les étapes suivantes :

1. Répétez les étapes 1 et 2 dans les utilisateurs d'ajouter à la section de groupe de wirelessusers de ce document.
2. Dans les utilisateurs choisis, la boîte de dialogue de contacts, ou d'ordinateurs, introduisent le nom de l'ordinateur que vous voulez ajouter au groupe. Cet exemple affiche comment ajouter l'ordinateur nommé *client au* groupe.
3. Cliquez sur les **types d'objet**, effacez la case d'**utilisateurs**, et puis cochez les **ordinateurs**.
4. Cliquez deux fois sur **OK**. Le compte d'ordinateur client est ajouté au groupe de wirelessusers.
5. Répétez la procédure pour ajouter plus d'ordinateurs au groupe.

Secure ACS 5.1 de Cisco 1121

Installation utilisant l'appliance de la gamme CSACS-1121

L'appliance CSACS-1121 est préinstallée avec le logiciel ACS 5.1. Cette section te donne un aperçu du processus d'installation et des tâches que vous devez exécuter avant d'installer ACS.

1. Connectez le CSACS-1121 à la console de réseau et d'appareils. Voir le chapitre 4, des « câbles de connexion. »
2. Alimentation vers le haut de l'appliance CSACS-1121. Voir le chapitre 4, « mettant l'appliance sous tension de la gamme CSACS-1121. »
3. Exécutez la **commande setup à la** demande CLI de configurer les configurations initiales pour le serveur ACS. Voyez exécuter le programme de configuration.

Installez le serveur ACS

Cette section décrit le processus d'installation pour le serveur ACS sur l'appliance de la gamme CSACS-1121.

- Lancez le programme de configuration
- Vérifiez le processus d'installation
- Tâches de post installation

Pour des informations détaillées sur l'installation du serveur de Cisco Secure ACS référez-vous à l'installation et améliorez le guide pour le Cisco Secure Access Control System 5.1.

Configuration de contrôleur de Cisco WLC5508

Créez la configuration nécessaire pour WPAv2/WPA

Effectuez les étapes suivantes :

Remarque: La supposition est que le contrôleur a la Connectivité de base au réseau et l'accessibilité par IP à l'interface de gestion est réussie.

1. Parcourez à **https://10.0.1.10** afin d'ouvrir une session au contrôleur.
2. **Procédure de connexion de** clic.
3. Ouvrez une session avec l'*admin* par défaut d'utilisateur et l'*admin de* mot de passe par défaut.
4. Créez une nouvelle interface pour le mappage VLAN sous le menu de **contrôleur**.
5. **Interfaces de** clic.
6. Cliquez sur **New**.
7. Dans la zone d'identification d'interface, présentez l'*employé*. (Ce champ peut être n'importe quelle valeur que vous aimez.)
8. Dans le domaine d'ID DE VLAN, écrivez *20*. (Ce champ peut être n'importe quel VLAN qui est porté dedans le réseau.)
9. Cliquez sur **Apply**.
10. Configurez les informations comme cette fenêtre d'Interfaces > Edit affiche :Adresse IP d'interface - **10.0.20.2**Netmask - **255.255.255.0**Passerelle - **10.0.10.1**DHCP primaire - **10.0.10.10**
11. Cliquez sur **Apply**.
12. Cliquez sur l'onglet **WLAN**.
13. Choisissez **créent nouveau**, et cliquent sur Go.
14. Écrivez un nom de profil, et, dans le champ SSID WLAN, présentez l'*employé*.
15. Choisissez un ID pour le WLAN, et cliquez sur Apply.
16. Configurez les informations pour ce WLAN quand la fenêtre de WLANs > Edit apparaît.**Remarque:** WPAv2 est la méthode de cryptage choisie de la couche 2 pour ce laboratoire. Afin de permettre au WPA avec des clients TKIP-MIC pour s'associer à ce SSID, vous pouvez également vérifier le **mode compatible WPA** et **permettre aux clients WPA2 TKIP des** cases ou à ces clients qui ne prennent en charge pas la méthode de cryptage 802.11i AES.
17. Sur l'écran de WLANs > Edit, cliquez sur l'**onglet Général**.
18. Assurez-vous que la case d'état est vérifiée **a activé** et l'**interface** appropriée (employé) est choisi. En outre, veillez à cocher la case **activée** pour le Broadcast SSID.
19. Cliquez sur l'onglet **Security**.
20. Sous le sous-menu de la couche 2, contrôle **WPA + WPA2** pour le degré de sécurité de la couche 2. Pour le chiffrement WPA2, contrôle **AES + TKIP** afin de permettre des clients TKIP.
21. Choisissez le **802.1x** comme méthode d'authentification.
22. Ignorez le sous-menu de la couche 3 car on ne l'exige pas. Une fois que le serveur de RAYON est configuré, le serveur compétent peut être choisi du menu d'authentification.

23. **Le QoS** et les **onglets Avancés** peuvent être laissés au par défaut à moins que toutes les configurations spéciales soient exigées.
24. Cliquez sur le **menu Security** pour ajouter le serveur de RAYON.
25. Sous le sous-menu de RAYON, **authentification de** clic. Puis, cliquez sur New.
26. Ajoutez l'adresse IP du serveur de RAYON (10.0.10.20) qui est le serveur ACS configuré plus tôt.
27. Assurez-vous que le principal partagé apparie le client d'AAA configuré dans le serveur ACS. Assurez-vous que la **case Network User** est cochée et cliquez sur Apply.
28. La configuration de base est maintenant complète et vous pouvez commencer à tester le PEAP.

Authentification PEAP

Le PEAP avec la version 2 MS-CHAP exige des Certificats sur les serveurs ACS mais pas sur les clients Sans fil. L'inscription automatique des Certificats d'ordinateur pour les serveurs ACS peut être utilisée pour simplifier un déploiement.

Afin de configurer le serveur CA pour fournir l'Auto-inscription pour l'ordinateur et les certificats utilisateurs, remplissez les procédures dans cette section.

Remarque: Microsoft a changé le modèle de serveur Web avec la release de l'entreprise CA de Windows 2003 de sorte que les clés ne soient plus exportables et l'option soit grisée. Il n'y a aucun autre modèle de certificat fourni avec des services de certificat qui sont pour l'authentification de serveur et donnent la capacité de marquer les clés car exportable qui sont disponibles dans le déroulant ainsi vous devez créer un nouveau modèle qui fait ainsi.

Remarque: Le Windows 2000 tient compte des clés exportables et ces procédures n'ont pas besoin d'être suivies si vous utilisez le Windows 2000.

Installez les modèles de certificat SNAP-dans

Effectuez les étapes suivantes :

1. Choisissez le **Start > Run**, écrivez le *MMC*, et cliquez sur OK.
2. Sur le menu File, cliquez sur Add**/retirez SNAP-dans**, et puis cliquez sur Add.
3. Sous SNAP-dans, les **modèles de certificat de** double clic, **fin de** clic, et cliquent sur OK alors.
4. Dans l'arborescence de la console, **modèles de certificat de** clic. Tous les modèles de certificat apparaissent dans le volet de détails.
5. Afin de sauter les étapes 2 à 4, écrivez *certtmpl.msc SNAP*-dans le*quel* ouvre les modèles de certificat.

Créez le modèle de certificat pour le serveur Web ACS

Effectuez les étapes suivantes :

1. Dans le volet de détails des modèles de certificat SNAP-dans, cliquez sur le modèle de **serveur Web**.
2. Sur le menu Action, **modèle en double de** clic.

3. Dans la zone d'identification d'affichage de modèle, écrivez *ACS*.
4. Allez à l'onglet de **manipulation de demande** et le contrôle **permettent la clé privée à exporter**. Assurez-vous également que la **signature et le cryptage** est sélectionnée du menu déroulant de but.
5. Choisissez les **demandes doit utiliser un du CSPs suivant** et vérifier **Microsoft Base Cryptographic Provider v1.0**. Décochez n'importe quel autre CSPs qui sont vérifiés, et cliquez sur OK.
6. Allez à l'onglet de **nom du sujet**, choisissez l'**approvisionnement** dans la demande, et cliquez sur OK.
7. Allez à l'**onglet Sécurité**, mettez en valeur le **groupe d'admins de domaine**, et assurez-vous que l'option d'**inscription** est vérifiée sous laissé.**Remarque:** Si vous choisissez d'établir de ce contrôle de l'information de Répertoire actif seulement le **nom principal d'utilisateur (UPN)** et décocher le **nom d'email d'inclure** dans le nom du sujet et le courrier électronique nommez parce qu'un nom de courrier électronique n'a pas été écrit pour le compte d'utilisateur de sans fil dans les utilisateurs et les ordinateurs de Répertoire actif SNAP-dans. Si vous ne désactivez pas ces deux options, des tentatives d'Auto-inscription d'utiliser le courrier électronique, qui a comme conséquence une erreur d'Auto-inscription.
8. Il y a des mesures de sécurité supplémentaires si nécessaire d'empêcher des Certificats d'être automatiquement éliminée. Ceux-ci peuvent être trouvés sous l'onglet de conditions requises d'émission. Ceci n'est pas discuté plus loin dans ce document.
9. Cliquez sur OK afin de sauvegarder le modèle et passer à émettre ce modèle de l'autorité de certification SNAP-dans.

Activez le nouveau modèle de certificat de serveur Web ACS

Effectuez les étapes suivantes :

1. Ouvrez l'autorité de certification SNAP-dans. Exécutez les étapes 1 à 3 dans la création le modèle de certificat pour la section de serveur Web ACS, choisissez l'option d'**autorité de certification**, choisissez l'**ordinateur local**, et cliquez sur Finish.
2. Dans l'arborescence de la console d'autorité de certification, développez **ca.demo.local, et puis cliquez avec le bouton droit les modèles de** certificat**.**
3. Allez à **nouveau > modèle de certificat à émettre**.
4. Cliquez sur le **modèle de certificat ACS**.
5. Cliquez sur OK et ouvrez les **utilisateurs et les ordinateurs de Répertoire actif SNAP-dans**.
6. Dans l'arborescence de la console, les **utilisateurs et les ordinateurs de Répertoire actif de** double clic, le clic droit **demo.local, et** cliquent sur alors Properties**.**
7. Sur l'onglet de stratégie de groupe, la **stratégie par défaut de domaine de** clic, et cliquent sur Edit alors. Ceci ouvre l'éditeur d'objet de stratégie de groupe SNAP-dans.
8. Dans l'arborescence de la console, développez la **configuration de l'ordinateur >** les **paramètres de windows >** les **paramètres de sécurité >** des **stratégies de clé publique**, et puis choisissez les **configurations automatiques de demande de certificat**.
9. Cliquez avec le bouton droit les **configurations automatiques de demande de certificat**, et choisissez la **nouvelle > automatique demande de certificat**.
10. Sur l'accueil à la page automatique d'assistant de configuration de demande de certificat, cliquez sur Next.
11. Àla page de modèle de certificat, l'**ordinateur de** clic, et cliquent sur Next alors.
12. Quand vous remplissez la page automatique d'assistant de configuration de demande de

certificat, cliquez sur Finish. Le type de certificat d'ordinateur apparaît maintenant dans le volet de détails de l'éditeur d'objet de stratégie de groupe SNAP-dans.
13. Dans l'arborescence de la console, développez la **configuration utilisateur** > les **paramètres de windows** > les **paramètres de sécurité** > des **stratégies de clé publique**.
14. Dans le volet de détails, **configurations d'Auto-inscription de** double clic.
15. Choisissez **s'inscrivent des Certificats automatiquement** et vérifient les **Certificats expirés Renew, les mettent à jour en attendant des Certificats et retirent les Certificats retirés** et les **Certificats de mise à jour qui utilisent des modèles de certificat**.
16. Cliquez sur **OK**.

Installation de certificat ACS 5.1

Configurez le certificat exportable pour ACS

Remarque: Le serveur ACS doit obtenir un certificat de serveur du serveur de la racine CA d'entreprise afin d'authentifier un client WLAN PEAP.

Remarque: Assurez-vous que le gestionnaire IIS n'est pas ouvert pendant la procédure d'installation de certificat en tant que problèmes de causes avec les informations en cache.

1. Ouvrez une session au serveur ACS avec des droites d'un admin de compte.
2. Allez à l'**administration système** > à la **configuration** > aux **Certificats de serveur local**. Cliquez sur **Add**.
3. Quand vous choisissez une méthode de création de certificat de serveur, choisissez **génèrent la demande de signature de certificat**. Cliquez sur **Next** (Suivant).
4. Écrivez un sujet de certificat et une longueur principale comme exemple, puis cliquez sur Finish :Sujet de certificat - **CN=acs.demo.local**Longueur principale - **1024**
5. ACS incitera qu'une demande de signature de certificat a été générée. Cliquez sur **OK**.
6. Sous l'administration système, allez à la **configuration** > aux **Certificats de serveur local** > des **demandes de signature exceptionnelles**.**Remarque:** La raison pour cette étape est que Windows 2003 ne tient pas compte des clés exportables et vous le besoin de générer une demande de certificat basée sur le certificat ACS que vous avez créé plus tôt cela fait.
7. Choisissez l'entrée de **demande de signature de certificat**, et cliquez sur l'**exportation**.
8. Sauvegardez le fichier du certificat **.pem** ACS à l'appareil de bureau.

Installez le certificat en logiciel ACS 5.1

Effectuez les étapes suivantes :

1. Ouvrez un navigateur et connectez à URL **http://10.0.10.10/certsrv de** serveur CA.
2. La fenêtre de services de certificat de Microsoft apparaît. Choisissez la **demande un certificat**.
3. Cliquez sur pour soumettre une **demande avancée de certificat**.
4. Dans la demande avancée, cliquez sur Submit une **demande de certificat utilisant un base-64-encoded…**
5. Dans le domaine enregistré de demande, si les autorisations de Sécurité de navigateur, parcourent au fichier et à l'insertion précédents de demande de certificat ACS.
6. Les paramètres de sécurité du navigateur peuvent ne pas permettre accéder au fichier sur

un disque. Si oui, cliquez sur OK pour exécuter une pâte manuelle.
7. Localisez le fichier ACS *.pem de l'exportation précédente ACS. Ouvrez le fichier utilisant un éditeur de texte (par exemple, Notepad).
8. Mettez en valeur le contenu entier du fichier, et cliquez sur la **copie**.
9. Revenez à la fenêtre de demande de certificat de Microsoft. **Collez le** contenu copié dans le champ enregistré de demande.
10. Choisissez **ACS** comme modèle de certificat, et cliquez sur Submit.
11. Une fois le certificat est délivré, choisit la **base 64 encodée**, et clique sur Download le **certificat**.
12. **Sauvegarde de** clic afin de sauvegarder le certificat à l'appareil de bureau.
13. Allez à **ACS > administration système > configuration > Certificats de serveur local**. Choisissez le **certificat signé du grippage CA**, et cliquez sur Next.
14. Cliquez sur **parcourent**, et localisent le certificat enregistré.
15. Choisissez le certificat ACS qui a été délivré par le serveur CA, et cliquez sur **ouvert**.
16. En outre, cochez la case de Protocol pour l'**EAP**, et cliquez sur Finish.
17. Le certificat Ca-émis ACS apparaîtra dans le certificat local ACS.

Configurez la mémoire d'identité ACS pour le Répertoire actif

Effectuez les étapes suivantes :

1. Connectez à ACS et à procédure de connexion au compte d'admin.
2. Allez aux **utilisateurs et l'identité enregistre > identité externe enregistre > Répertoire actif**.
3. Entrez dans le domaine *demo.local de* Répertoire actif*, entrez le* mot de passe du serveur, et cliquez sur TestConnection**.** Commande du **clic** OKIN à continuer.
4. **Modifications de sauvegarde de** clic.**Remarque:** Pour plus d'informations sur la procédure d'intégration ACS 5.x référez-vous à ACS 5.x et plus tard : Intégration avec l'exemple de configuration de Microsoft Active Directory.

Ajoutez un contrôleur à ACS en tant que client d'AAA

Effectuez les étapes suivantes :

1. Connectez à ACS, et allez aux **ressources de réseau >** aux **périphériques de réseau et aux clients d'AAA**. Cliquez sur **Create**.
2. Entrez dans ces champs :Nom - **wlc**IP - **10.0.1.10**Case à cocher de RAYON - **Vérifié**Secret cisco partagé
3. Cliquez sur Submit une fois terminé. Le contrôleur apparaîtra car une entrée dans la liste de périphériques de réseau ACS.

Configurez les stratégies ACS Access pour la radio

Effectuez les étapes suivantes :

1. Dans ACS, allez à **Access les stratégies >** les **services d'accès**.
2. Dans la fenêtre de services d'accès, le clic **créent**.
3. Créez un service d'accès, et écrivez un nom (par exemple WirelessAD). Choisissez **basé sur le modèle de service**, et cliquez sur **choisi**.

4. Dans le dialogue de page Web, choisissez l'**accès au réseau – simple**. Cliquez sur **OK**.
5. Dans le dialogue de page Web, choisissez l'**accès au réseau – simple**. Cliquez sur **OK**. Une fois que le modèle est sélectionné, cliquez sur Next.
6. Sous des protocoles permis, vérifiez les cases pour **Allow MS-CHAPv2** et **permettez le PEAP**. Cliquez sur **Finish** (Terminer).
7. Quand ACS vous incite à lancer le nouveau service, cliquez sur **oui**.
8. Au nouveau service d'accès qui a été juste créé/lancé, développez et choisissez l'**identité**. Pour la source d'identité, clic **choisi**.
9. Choisissez **AD1** pour le Répertoire actif qui a été configuré dans ACS, cliquent sur OK.
10. Confirmez la source d'identité est AD1, et la **sauvegarde de** clic **change**.

Créez la stratégie ACS Access et la règle de service

Effectuez les étapes suivantes :

1. Allez à **Access les stratégies** > les **règles de sélection de service**.
2. Le clic **créent** dans la fenêtre de stratégie de sélection de service. Donnez à la nouvelle règle un nom (par exemple, *WirelessRule*). Cochez la case pour que **Protocol** apparie le **rayon**.
3. Choisissez le **rayon**, et cliquez sur OK.
4. Sous des résultats, choisissez **WirelessAD** pour le service (créé dans l'étape précédente).
5. Une fois que la nouvelle règle Sans fil est créée, choisissez et **déplacez** cette règle jusqu'au dessus, qui sera la première règle d'identifier l'authentification Sans fil de rayon utilisant le Répertoire actif.

Configuration de CLIENT pour le PEAP utilisant des Windows Zero Touch

Dans notre exemple, le CLIENT est un ordinateur qui exécute le Windows XP Professionnel avec le fournisseur de services qui agit en tant que client sans fil et obtient l'accès aux ressources en intranet par le point d'accès sans fil. Remplissez les procédures dans cette section afin de configurer le CLIENT en tant que client sans fil.

Exécutez une installation et une configuration de base

Effectuez les étapes suivantes :

1. Connectez le CLIENT au segment de réseau d'intranet utilisant un câble Ethernet connecté au hub.
2. Sur le CLIENT, installez le Windows XP Professionnel avec le SP2 comme ordinateur de membre nommé CLIENT du domaine demo.local.
3. Installez le Windows XP Professionnel avec le SP2. Ceci doit être installé afin d'avoir le support PEAP.**Remarque:** Le pare-feu Windows est automatiquement activé dans le Windows XP Professionnel avec le SP2. N'arrêtez pas le Pare-feu.

Installez l'adaptateur réseau sans fil

Effectuez les étapes suivantes :

1. Arrêtez l'ordinateur client.
2. Démontez l'ordinateur client du segment de réseau d'intranet.
3. Redémarrez l'ordinateur client, et puis ouvrez une session utilisant le compte administrateur local.
4. Installez l'adaptateur réseau sans fil.**Remarque:** N'installez pas le logiciel de la configuration du fabricant pour l'adaptateur Sans fil. Installez les gestionnaires d'adaptateur réseau sans fil utilisant l'assistant de matériel d'ajouter. En outre, une fois incité, fournissez au CD équipé par le fabricant ou un disque les gestionnaires mis à jour pour l'usage en Windows XP Professionnel de SP2.

Configurez la connexion réseau sans fil

Effectuez les étapes suivantes :

1. Fermez une session et puis ouvrez une session utilisant le compte de **WirelessUser** dans le **domaine demo.local**.
2. Choisissez le **début >** le **panneau de configuration**, double-cliquer les **connexions réseau**, et puis cliquez avec le bouton droit la **connexion réseau sans fil**.
3. Cliquez sur **Properties**, allez à l'**onglet Wireless Networks**, et assurez-vous que l'**utilisation Windows de configurer mes paramètres de réseau sans fil** est vérifiée.
4. Cliquez sur **Add**.
5. Sous l'onglet d'association, présentez l'*employé* dans le domaine du nom de réseau (SSID).
6. Choisissez le **WPA** pour l'authentification de réseau, et assurez-vous que le chiffrement de données est placé au **TKIP**.
7. Cliquez sur l'onglet d'**authentification**.
8. Validez que le type d'EAP est configuré pour utiliser l'**EAP protégé (PEAP)**. S'il n'est pas, choisissez-le du menu déroulant.
9. Si vous voulez que l'ordinateur soit authentifié avant la procédure de connexion (qui permet des scripts de connexion ou des poussers de stratégie de groupe d'être appliqué), le contrôle **authentifient comme ordinateur quand les informations d'ordinateur sont disponibles**.
10. Cliquez sur **Properties**.
11. Comme le PEAP comporte l'authentification du serveur par le client, assurez-vous que le **certificat de serveur de validation** est vérifié. En outre, assurez-vous que le CA qui a émis le certificat ACS est vérifié sous le menu d'Autorités de certification racine approuvée.
12. Choisissez le **mot de passe sécurisé (EAP-MSCHAP v2)** sous la méthode d'authentification comme elle est utilisée pour l'authentification intérieure.
13. Assurez-vous que la case d'**Enable Fast Reconnect** est cochée. Puis, cliquez sur OK trois fois.
14. Cliquez avec le bouton droit l'icône de connexion réseau sans fil dans systray, et puis cliquez sur les **réseaux sans fil disponibles de vue**.
15. Cliquez sur le réseau Sans fil des employés, et puis cliquez sur **se connectent**. Le client sans fil affichera **connecté** si la connexion est réussie.
16. Après l'authentification est réussie, vérifiez la configuration TCP/IP pour l'adaptateur Sans fil à l'aide des connexions réseau. Il devrait avoir une plage d'adresses de 10.0.20.100-10.0.20.200 de la portée de DHCP ou de la portée créée pour les clients sans fil de CorpNet.
17. Afin de tester la fonctionnalité, ouvrez un navigateur et parcourez à **http://10.0.10.10** (ou à l'adresse IP du serveur CA).

Dépannez l'authentification Sans fil avec ACS

Effectuez les étapes suivantes :

1. Allez à **ACS > surveillance et états**, et cliquez sur la **surveillance et la visionneuse de rapports de lancement**.
2. Une fenêtre distincte ACS s'ouvrira. **Tableau de bord de** clic.
3. Dans la ma section d'états préférée, **authentifications de** clic **– RAYON – aujourd'hui**.
4. Un log affichera toutes les authentifications de RAYON car passage ou échouer. Dans une entrée loggée, cliquez sur en fonction l'**icône de loupe** dans la colonne de détails.
5. Le détail d'authentification de RAYON fournira beaucoup d'informations au sujet des tentatives loggées.
6. Le nombre de hits de service ACS peut fournir un aperçu des tentatives appariant les règles créées dans ACS. Allez à **ACS > stratégies > services d'accès d'Access**, et cliquez sur les **règles de sélection de service**.

L'authentification PEAP échoue avec le serveur ACS

Quand votre client échoue authentification PEAP avec un serveur ACS, vérifiez si vous trouvez le message d'erreur `reproduit par NAS de tentative d'authentification` dans l'option d'**essais ratés** sous le menu d'**état et d'activité de l'**ACS.

Vous pourriez recevoir ce message d'erreur quand Microsoft Windows XP SP2 est installé sur la machine cliente et les Windows XP SP2 authentifient contre un serveur de tiers autre qu'un serveur de Microsoft IAS. En particulier, le serveur de RAYON de Cisco (ACS) emploie une différente méthode pour calculer le type d'Extensible Authentication Protocol : Longueur : ID du format de valeur (EAP-TLV) que les utilisations de Windows XP de méthode. Microsoft a identifié ceci comme défaut dans le suppliant de XP SP2.

Pour un correctif, le contact Microsoft et se rapportent à l'authentification de l'article PEAP n'est pas réussi quand vous vous connectez à un tiers serveur de RAYON . Le problème intrinsèque est celui sur le côté client, avec l'utilitaire de fenêtres, le rapide rebranchent l'option est désactivé pour le PEAP par défaut. Cependant, cette option est activée par défaut sur le côté serveur (ACS). Afin de résoudre ce problème, décochez le rapide rebranchent l'option sur le serveur ACS (sous des options de Global System). Alternativement, vous pouvez activer le rapide rebranchez l'option sur le côté client de résoudre le problème.

Perorm ces étapes afin d'activer rapide rebranchent sur le client qui exécute Windows XP utilisant l'utilitaire Windows :

1. Allez au **début** > aux **configurations** > au **panneau de configuration**.
2. Double-cliquer l'icône de **connexions réseau**.
3. Cliquez avec le bouton droit l'icône de **connexion réseau sans fil**, et puis cliquez sur **Properties**.
4. Cliquez sur l'**onglet Wireless Networks**.
5. Choisissez l'**utilisation Windows de configurer mon** option de **paramètres de réseau sans fil** afin de permettre à des fenêtres de configurer l'adaptateur de client.
6. Si vous avez déjà configuré un SSID, choisissez le SSID et cliquez sur **Properties**. Sinon, cliquez sur New afin d'ajouter un nouveau WLAN.

7. Écrivez le SSID sous l'association tableau s'assurent que l'authentification de réseau est **ouverte** et le chiffrement de données est placé au **WEP**.
8. **Authentification de** clic.
9. Choisissez l'**authentification de 802.1x d'IEEE d'enable pour cette option Network**.
10. Choisissez le **PEAP** comme type d'EAP, et cliquez sur **Properties**.
11. Choisissez l'option d'**Enable Fast Reconnect au** bas de page.

Informations connexes

- PEAP sous des réseaux sans fil unifiés avec ACS 4.0 et Windows 2003
- Exemple Sans fil du contrôleur LAN de Cisco (WLC) et de la configuration de Cisco ACS 5.x (TACACS+) pour l'authentification Web
- Installation et guide de mise à jour pour le Cisco Secure Access Control System 5.1
- Support et documentation techniques - Cisco Systems