Configurez le réseau sans fil unifié pour l'authentification contre la base de données eDirectory du Novell

Contenu

Introduction

Dans l'espace de la formation K-12, il y a eu un besoin croissant d'authentifier des utilisateurs de sans fil par l'intermédiaire des comptes créés dans le Novell eDirectory. En raison de la nature distribuée de l'environnement K-12, les différentes écoles ne pourraient pas avoir les ressources pour placer un serveur de RAYON à chaque site ni font elles désirent le temps système supplémentaire de configurer ces serveurs de RAYON. La seule manière d'accomplir ceci est à l'aide du LDAP à communiquer entre le contrôleur LAN Sans fil (WLC) et un serveur LDAP. Les contrôleurs LAN Sans fil de Cisco prennent en charge l'authentification EAP locale contre les bases de données externes de LDAP telles que la Microsoft Active Directory. Ce documents papier blancs qu'un Cisco WLC a configurés pour l'authentification EAP locale contre eDirectory du Novell activé en tant que serveur LDAP complet. Une mise en garde à noter – les clients examinés avaient l'habitude Cisco Aironet Desktop Utility pour exécuter l'authentification de 802.1x. Le Novell actuellement ne prend en charge pas le 802.1x avec leur client à ce moment. En conséquence, selon le client, un processus en deux étapes de procédure de connexion a pu se produire. Notez ces références :

Déclaration de 802.1x de Novell

« Actuellement, ils doivent ouvrir une session deux fois. Quand le client Novell est installé, un utilisateur doit ouvrir une session utilisant la case de poste de travail seulement sur le dialogue de procédure de connexion initiale pour permettre l'authentification de l'utilisateur de 802.1x quand l'appareil de bureau est initialisé, et alors ils doivent ouvrir une session au réseau Novell utilisant l'utilitaire de procédure de connexion « N rouge ». Ceci désigné sous le nom d'une procédure de connexion à deux étages. »

Une alternative à la « procédure de connexion de poste de travail seulement » est de configurer le client Novell pour utiliser « le Novell initial Login=Off » dans les configurations avancées de procédure de connexion (le par défaut est « Novell initial Login=On »). Le pour en savoir plus, se rapportent à l'authentification de 802.1x et au client Novell pour Windows .

Les clients de tiers tels que le client d'Aeigs de temple (Cisco Secure Services Client) un partenaire technologique de Novell peuvent ne pas avoir besoin d'une double procédure de connexion. Le pour en savoir plus, se rapportent à l'ÉGIDE SecureConnect .

Un autre contournement viable pour le client Novell est d'avoir l'ordinateur (ou l'utilisateur) authentifient (802.1x) au WLAN avant le Novell GINA étant exécutée.

En testant une solution pour simple connectez-vous avec le client Novell et le 802.1x est hors de portée de ce livre blanc.

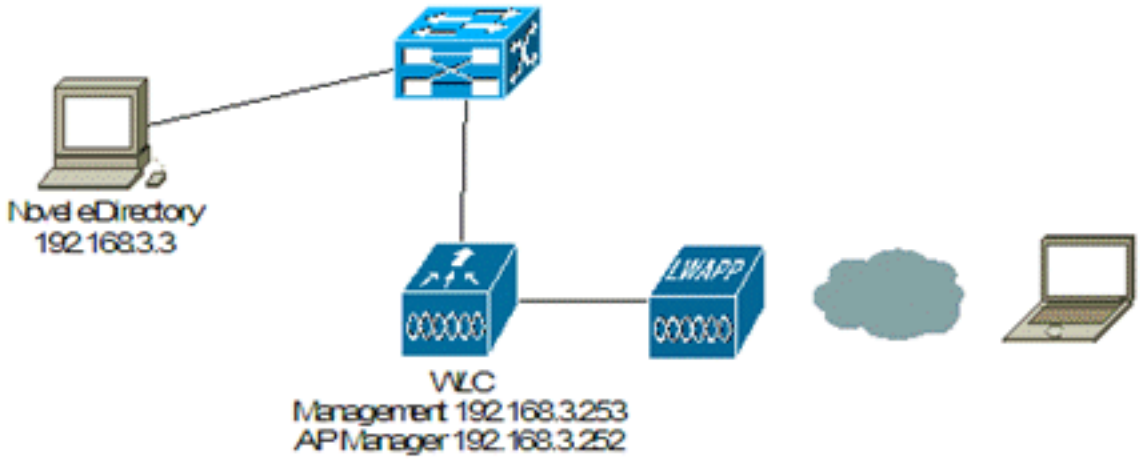
Topologie testée

Solution testée

- Contrôleur LAN Sans fil de Cisco avec le logiciel de 6.0.188.0
- Cisco Aironet LWAPP AP 1242AG
- Windows XP avec Cisco Aironet Desktop Utility 4.4
- Windows Server 2003 avec le Novell 8.8,5 eDirectory
- Novell ConsoleOne 1.3.6h (utilitaire de gestion eDirectory)

Topologie du réseau

Figure 1



Périphérique	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Novell eDirectory	192.168.3.3	255.255.255.0	192.168.3.254
Commutateur de la couche 3	192.168.3.254	255.255.255.0	-
AP	Assigné par	255.255	192.168

	l'intermédiaire du DHCP du commutateur L3	.255.0	.3.254
Interface de gestionnaire de l'interface de gestion WLC AP WLC	192.168.3.253 192.168.3.252	255.255 .255.0	192.168 .3.254

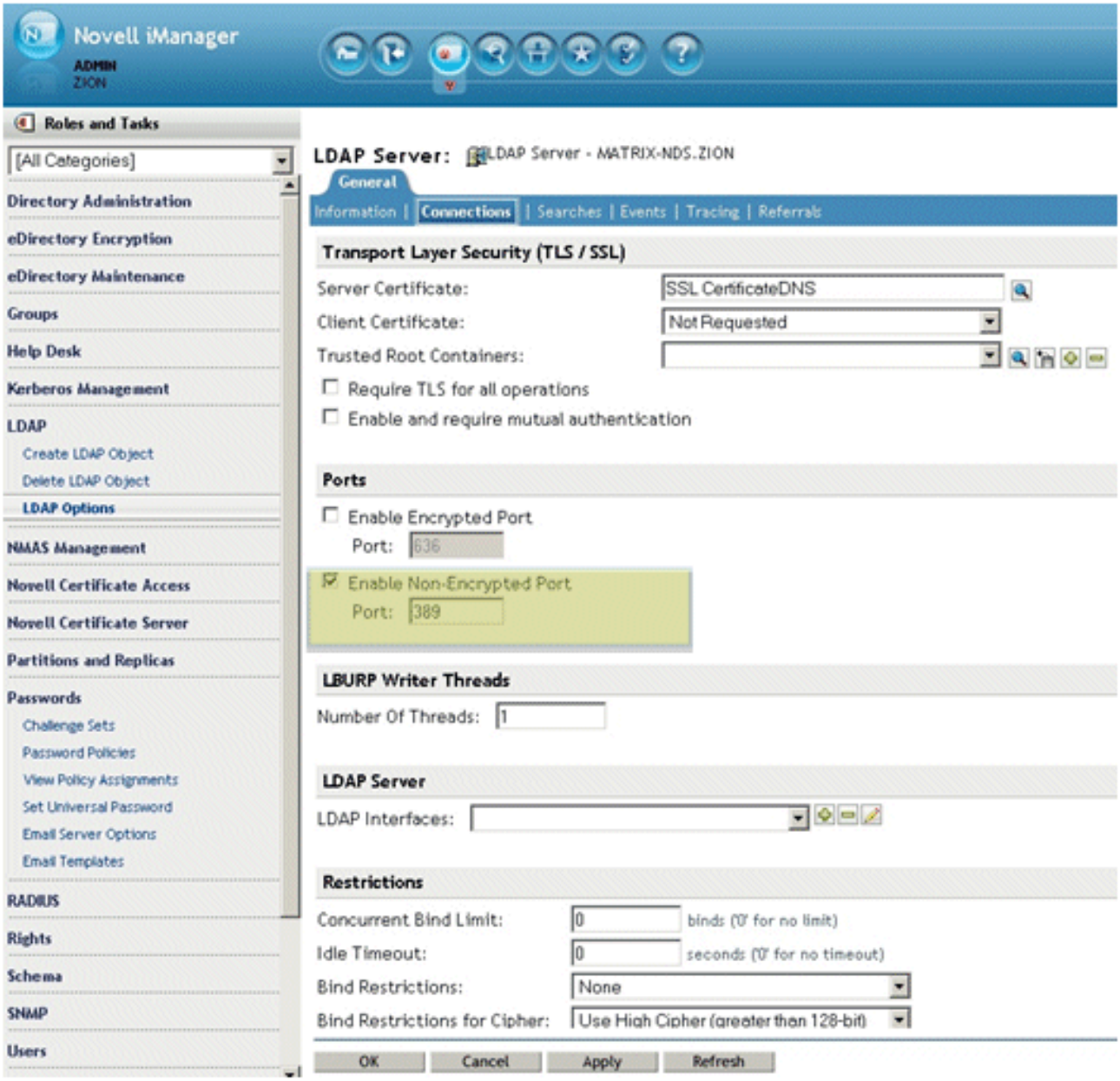
Configuration

Configuration eDirectory de Novell

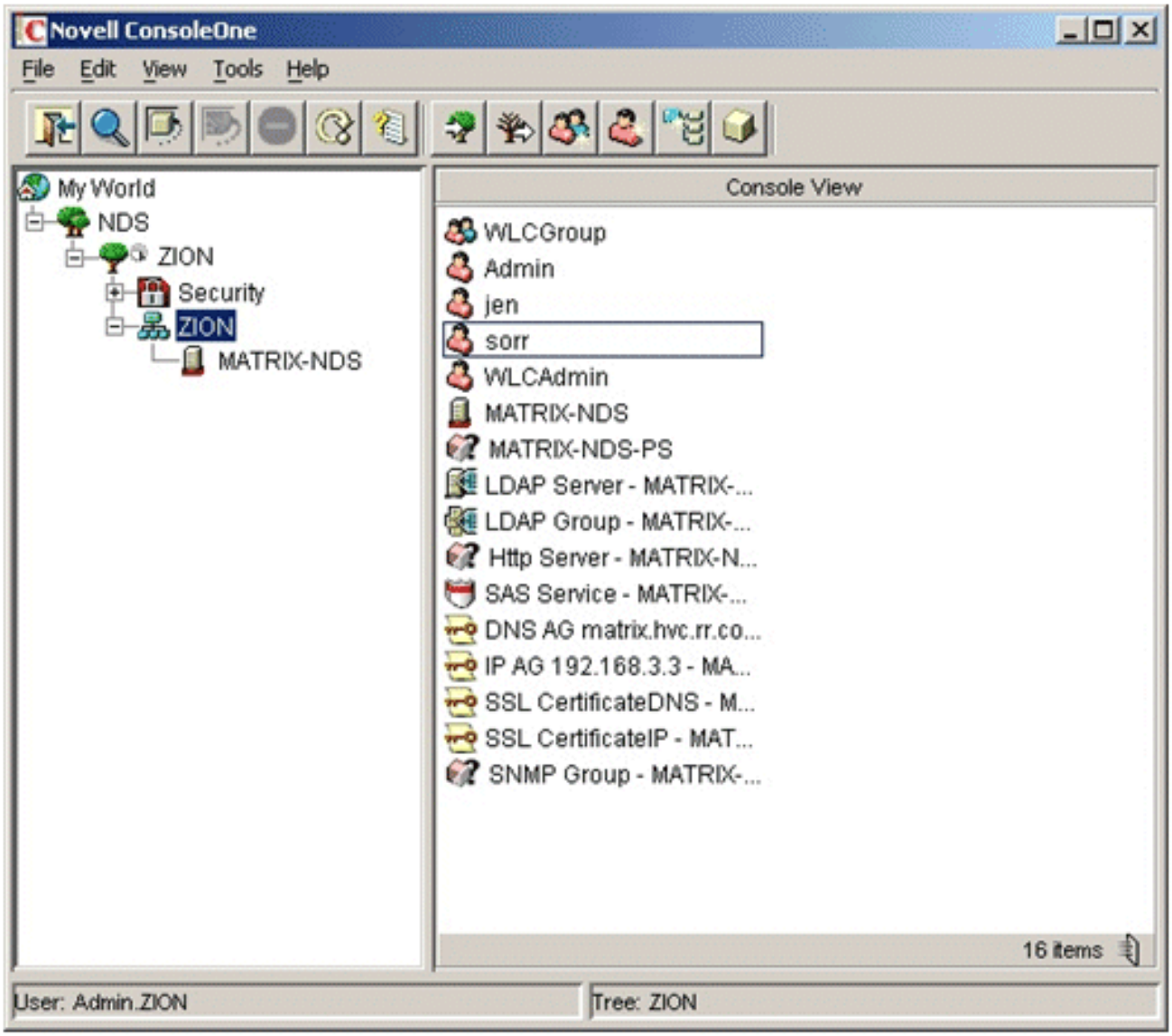
L'installation eDirectory et la configuration de plein Novell est hors de portée de ce livre blanc. Le Novell eDirectory doit être installé aussi bien que les composants correspondants de LDAP.

Les paramètres de configuration principaux exigés sont que le Simple Password doit être activé pour les comptes utilisateurs et le LDAP authentifié doit être configuré. Utilisant le TLS pour le LDAP a été pris en charge dans les versions préalables du code WLC (4.2) ; cependant, le LDAP sécurisé n'est plus pris en charge sur le logiciel contrôleur de WLAN Cisco.

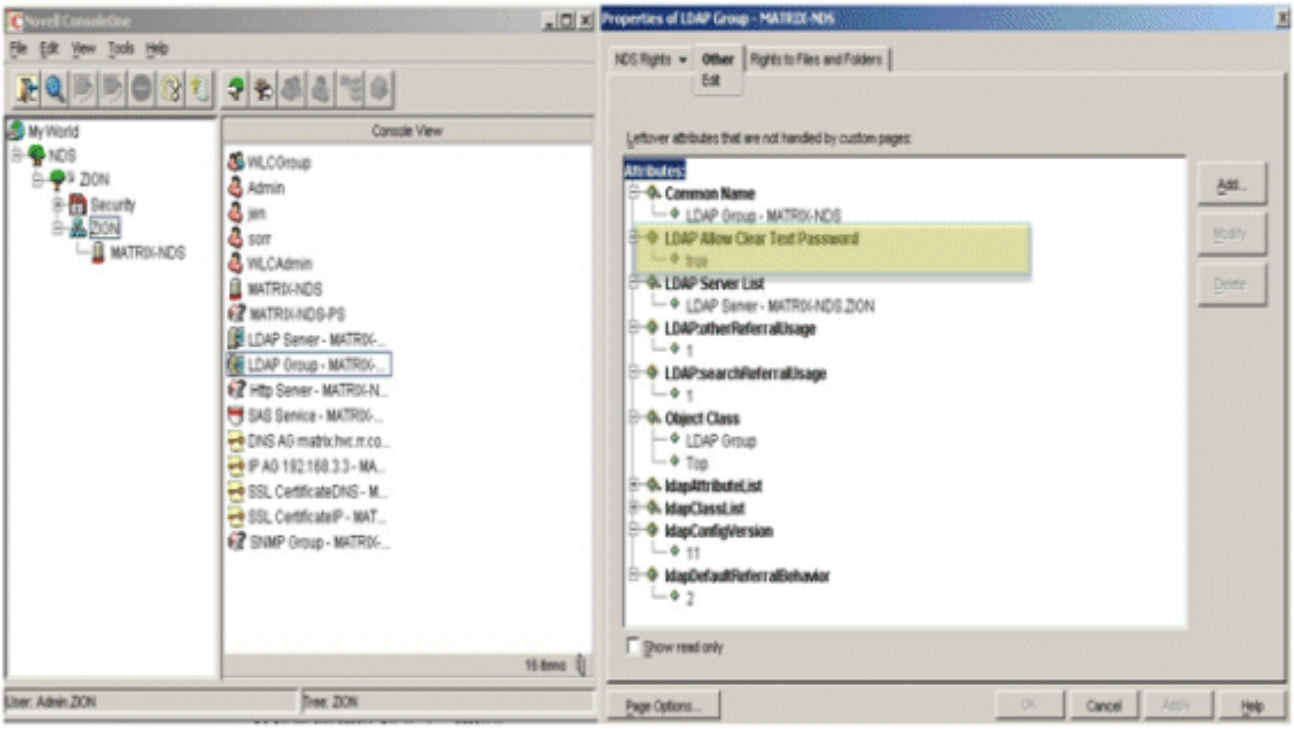
1. En configurant la partie de serveur LDAP d'eDirectory, assurez-vous que les ports non chiffrés de LDAP (389) sont activés. Voir la figure 2 de l'application d'iManager de Novell.**Figure 2**



2. Pendant l'installation eDirectory, il te demandera la structure arborescente ou le nom de domaine, etc. Si eDirectory est déjà installé, ConsoleOne du Novell (le schéma 3) est un outil facile par lequel pour visualiser la structure eDirectory. Il est essentiel de trouver ce que sont les schémas appropriés en essayant d'établir la transmission au WLC. Vous devez également faire créer un compte qui permettra au WLC pour exécuter un grippage authentifié au serveur LDAP. Pour la simplicité, dans ce cas, le compte eDirecotry d'admin de Novell est utilisé pour le grippage authentifié.**Figure 3**

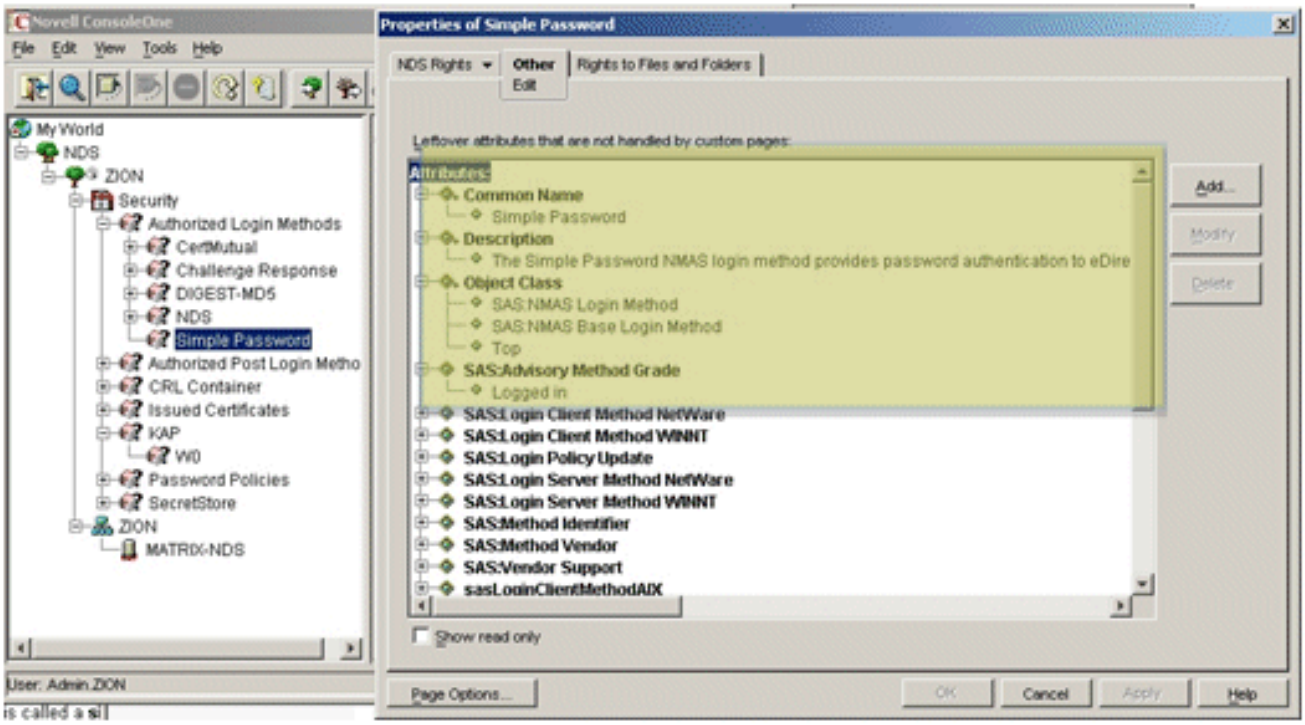


3. Employez ConsoleOne afin de vérifier que le groupe de LDAP permet des **mots de passe des textes clairs.Figure 4**



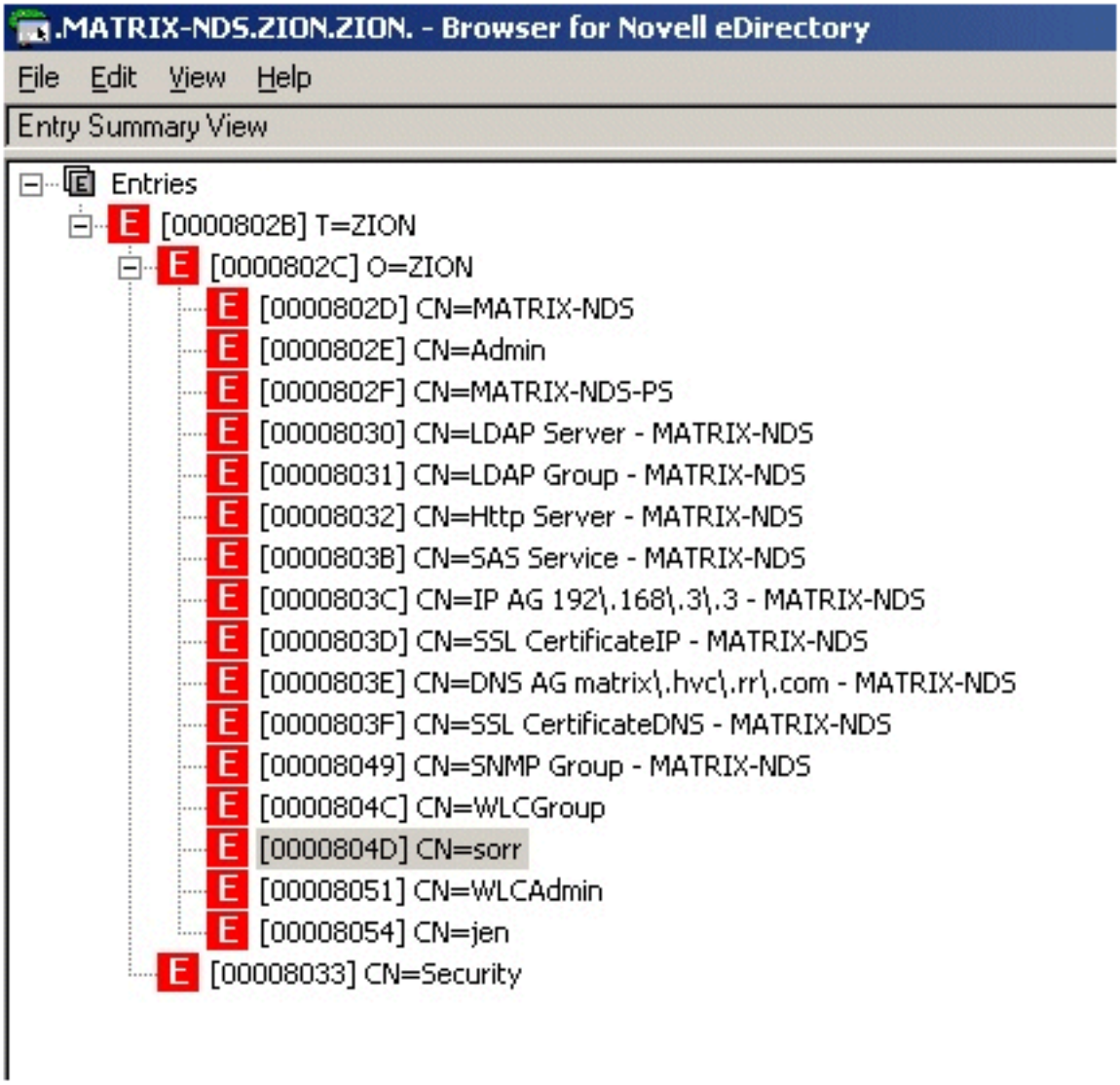
4. Vérifiez cela sous l'OU, des paramètres de sécurité que le **Simple Password** est

activé.**Figure 5**



Un autre outil utile par lequel visualiser la structure eDirectory de Novell est le navigateur a inclus avec l'installation par défaut.

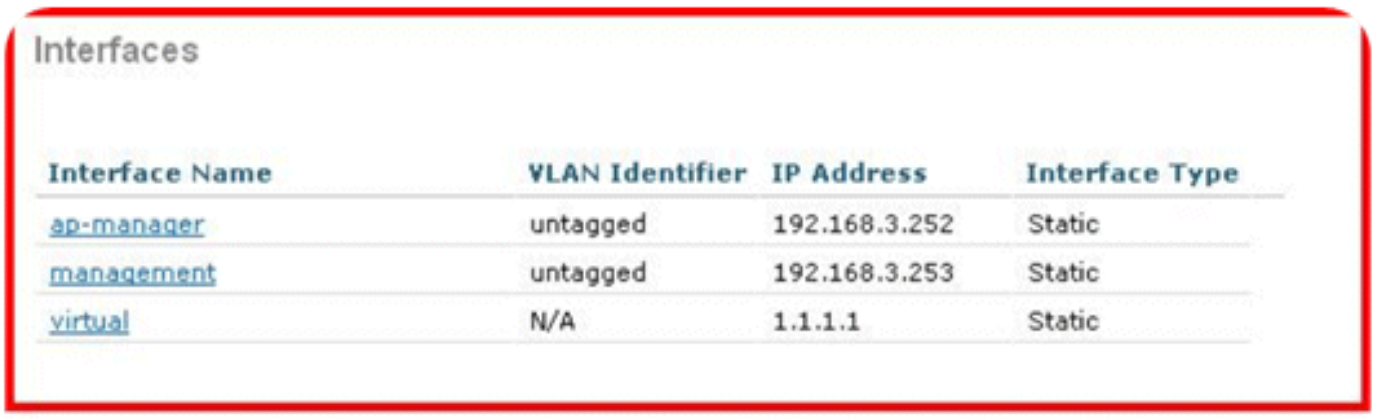
Figure 6



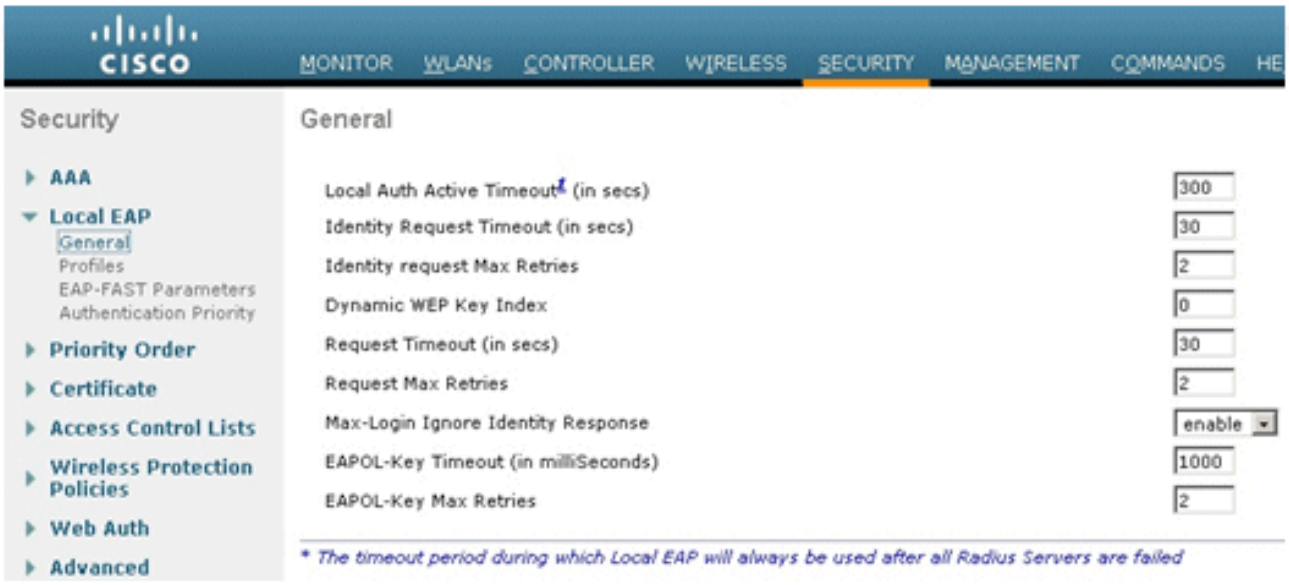
Configuration WLC

Référez-vous à la figure 1 pour la topologie physique du réseau de test. Le WLC utilisé dans ce test a été configuré selon la technique normalisée avec l'AP-gestionnaire et les interfaces de gestion sur le même sous-réseau et non-marqué d'un point de vue VLAN.

Figure 7



1. Configurez l'authentification EAP locale : **Sécurité > EAP local > général**.Des par défaut standard n'ont pas été changés.**Figure 8**



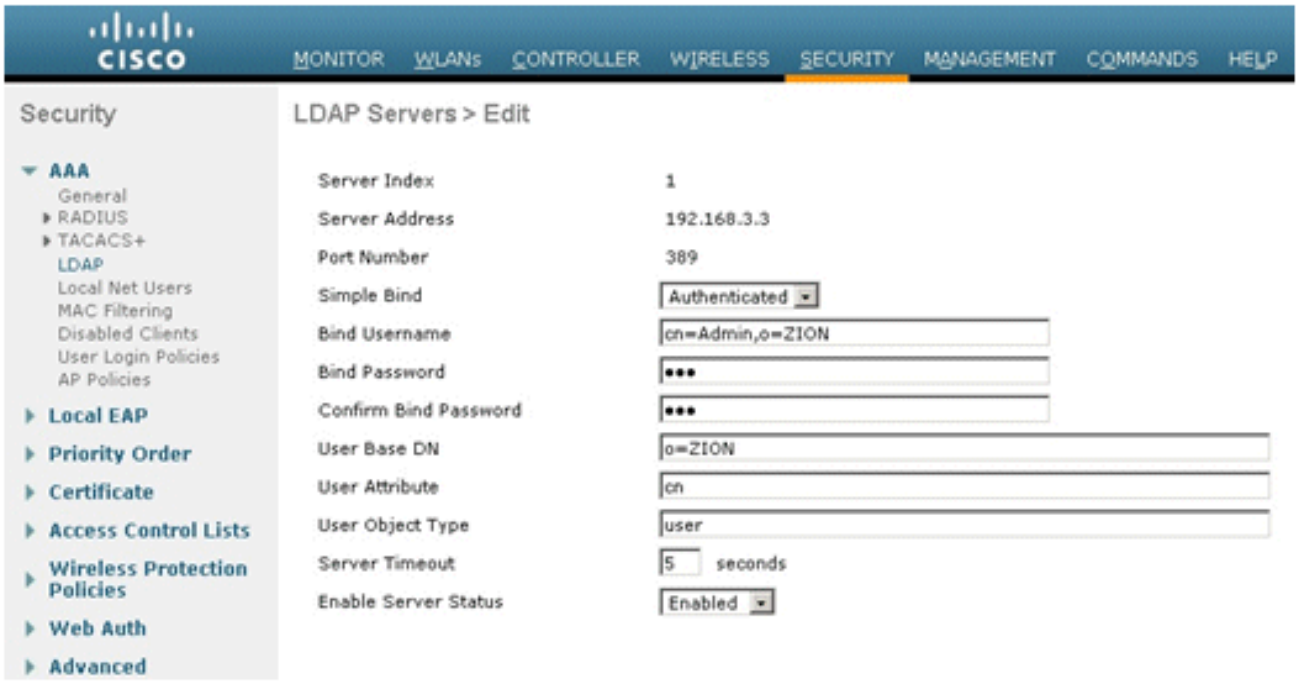
2. Créez un nouvel eap profile local : **Sécurité > EAP local > profils**.Pour ce cas de test, le nom local d'eap profile choisi était eDirectory. Les méthodes d'authentification choisies étaient LEAP, EAP-FAST et PEAP ; cependant, seulement le PEAP a été testé dans ce document.**Figure 9**

Quand vous configurez l'authentification EAP locale pour le PEAP, vous devez avoir un certificat installé sur le WLC. Dans ce cas, afin de tester, Cisco d'origine délivrent un certificat a été utilisé ; cependant, un certificat provisioned par client peut également être installé. Des Certificats de côté client ne sont pas exigés pour l'usage de PEAP-GTC, mais ils peuvent être activés s'il y a lieu pour la méthode intérieure PEAP.**Figure 10**

3. Fixez l'authentication priority pour le LDAP : **Sécurité > EAP local > authentication priority**.**Figure 11**

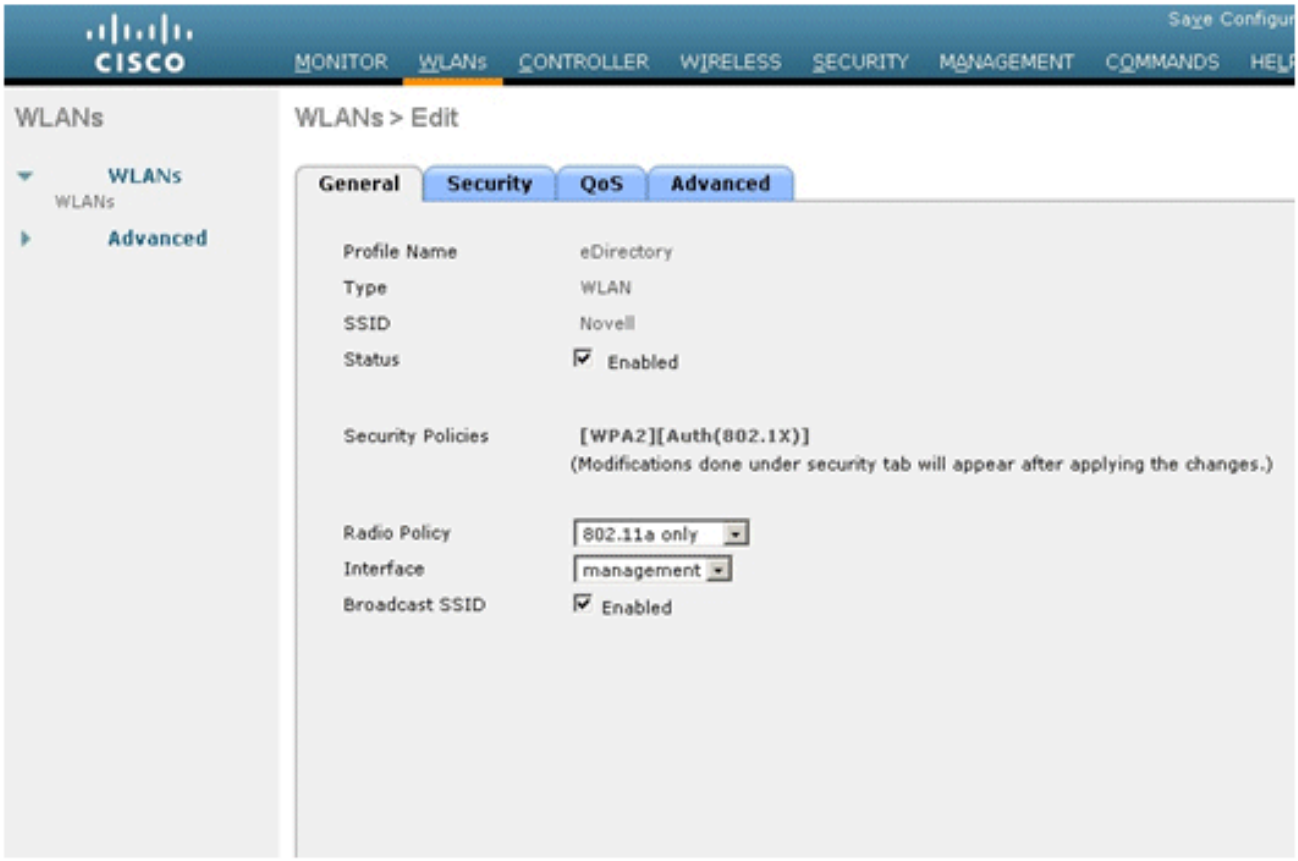
4. Ajoutez le serveur LDAP au WLC : **Security > AAA > LDAP**.**Figure 12**

5. Configurez le WLC pour utiliser eDirecotry nouvel (voir la figure 13) :Choisissez **authentifié** pour la méthode simple de grippage.Écrivez le nom d'utilisateur de grippage. C'est le compte qui a été créé à dans eDirectory qui sera utilisé pour que le WLC lie à eDirectory.**Remarque:** Assurez-vous que vous écrivez les attributs corrects de répertoire pour le nom d'utilisateur. Pour ce cas de test, le « cn=Admin, o=ZION » a été utilisé.Entrez le mot de passe de grippage. C'est le mot de passe pour le compte utilisateur de grippage.Écrivez le DN de base de clients. C'est le nom de domaine où les comptes d'utilisateur de sans fil se trouvent. Dans le cas de test, les utilisateurs se sont trouvés à la racine du DN (o=Zion). S'ils sont imbriqués dans d'autres groupes/organismes, enchaînez-les ainsi qu'une virgule (par exemple, « o=ZION, o=WLCUser »).Écrivez l'attribut d'utilisateur. C'est le nom commun (NC) (voir le schéma 6).Type d'objet utilisateur – Ceci est placé à l'*utilisateur*.**Figure 13**

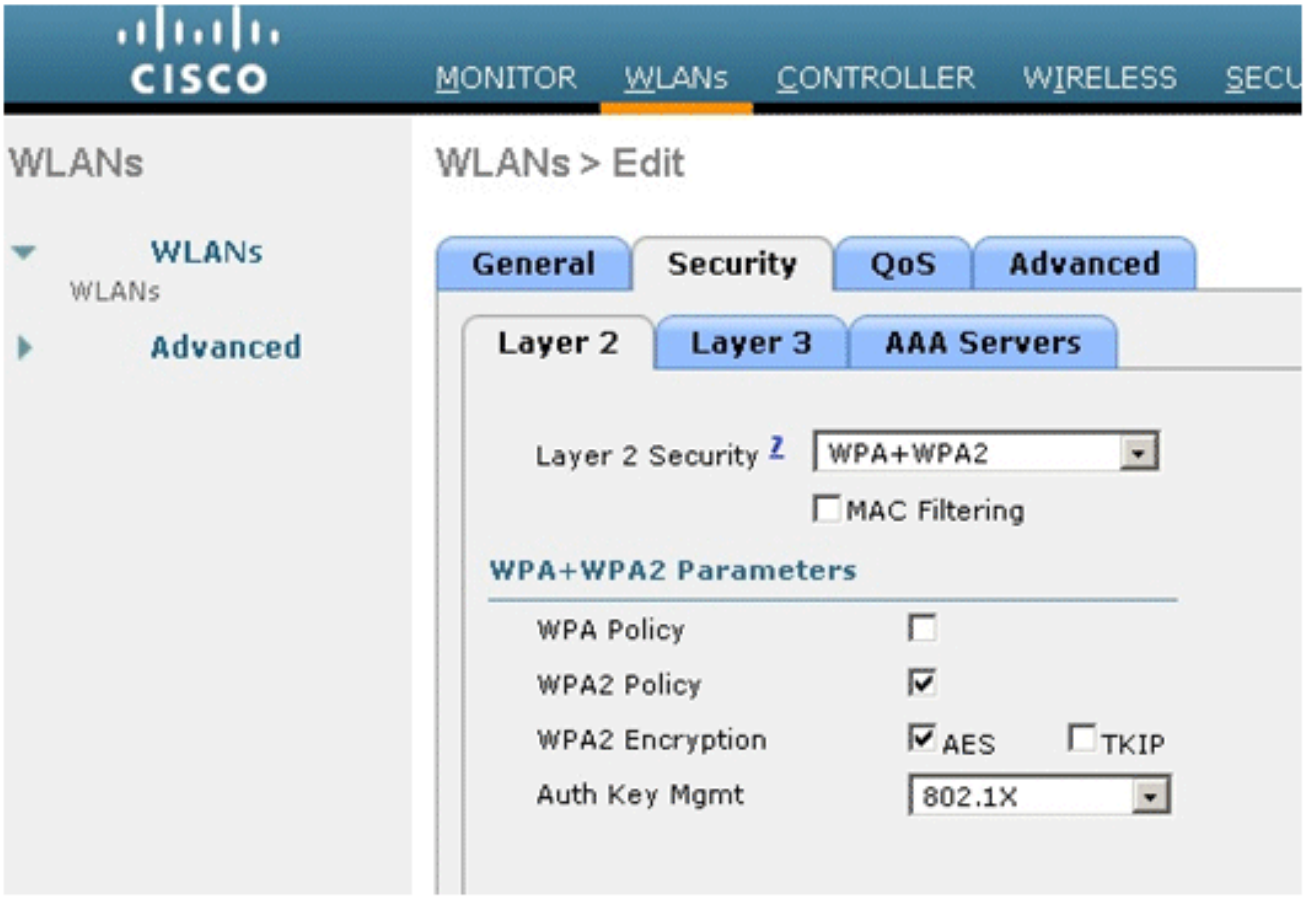


6. Créez le WLAN que vous voulez que les clients eDirectory de Novell les utilisent. Pour ce cas de test, le nom de profil WLAN est *eDirectory* et le SSID est *Novell* (voir la figure 14).**Figure 14**

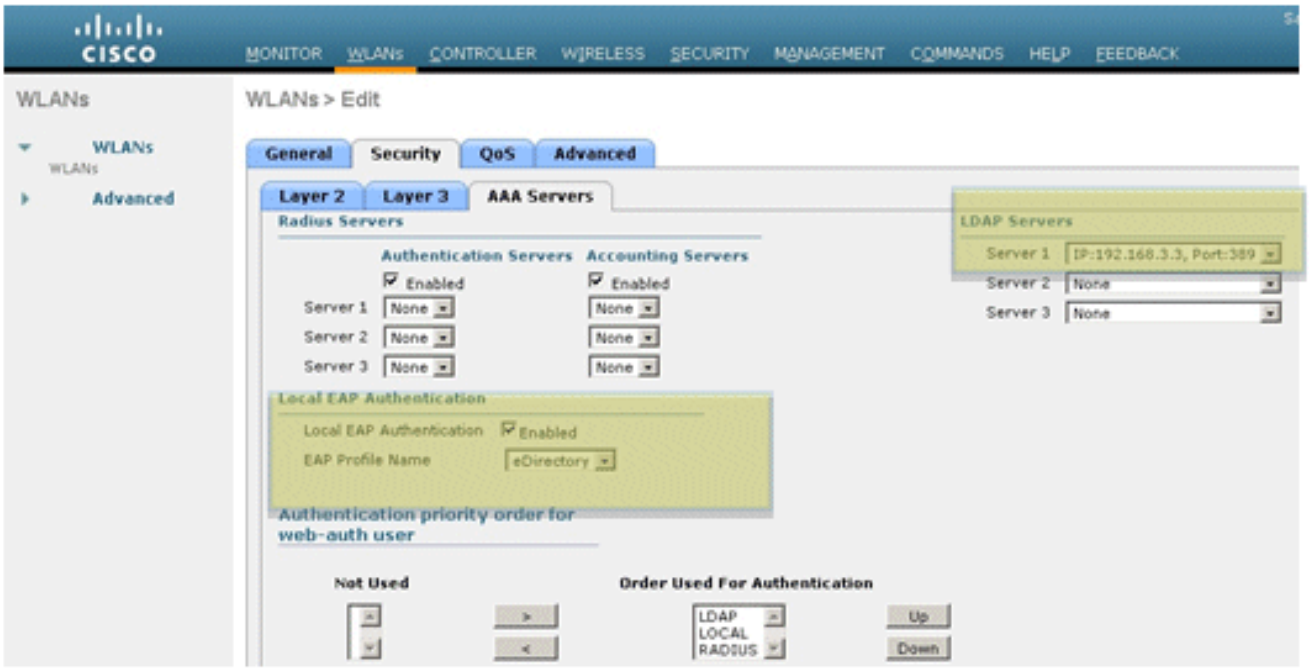
7. Activez le WLAN et appliquez la stratégie par radio appropriée et reliez. Pour ce cas de test, le Novell SSID a été seulement activé pour le réseau 802.11a et a été attaché à l'interface de gestion.**Figure 15**



8. Configurez les paramètres de sécurité appropriés de la couche 2. Pour ce cas de test, la Sécurité WPA+WPA2, la stratégie WPA2, le cryptage AES, et le 802.1x pour la gestion des clés ont été sélectionnés.**Figure 16**



9. Pour se terminer la configuration locale d'authentification EAP, configurez le WLAN pour l'authentification EAP locale utilisant le serveur LDAP :Choisissez l'**authentification EAP locale activée** et appliquez l'eap profile créé (**eDirectory**).Sous les serveurs LDAP, choisissez l'adresse IP du serveur eDirectory configuré (**192.168.3.3**).**Figure 17**

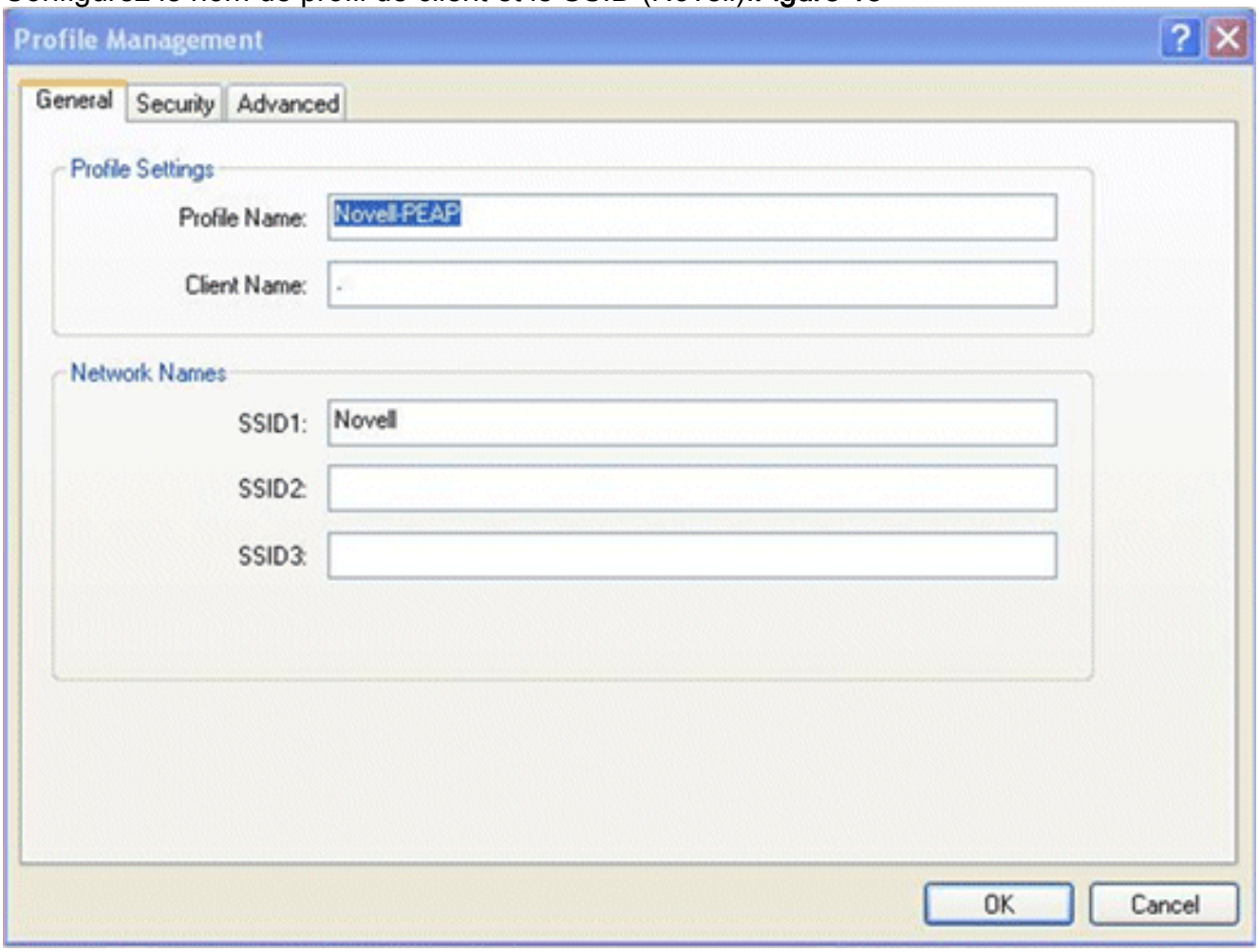


Configuration du client

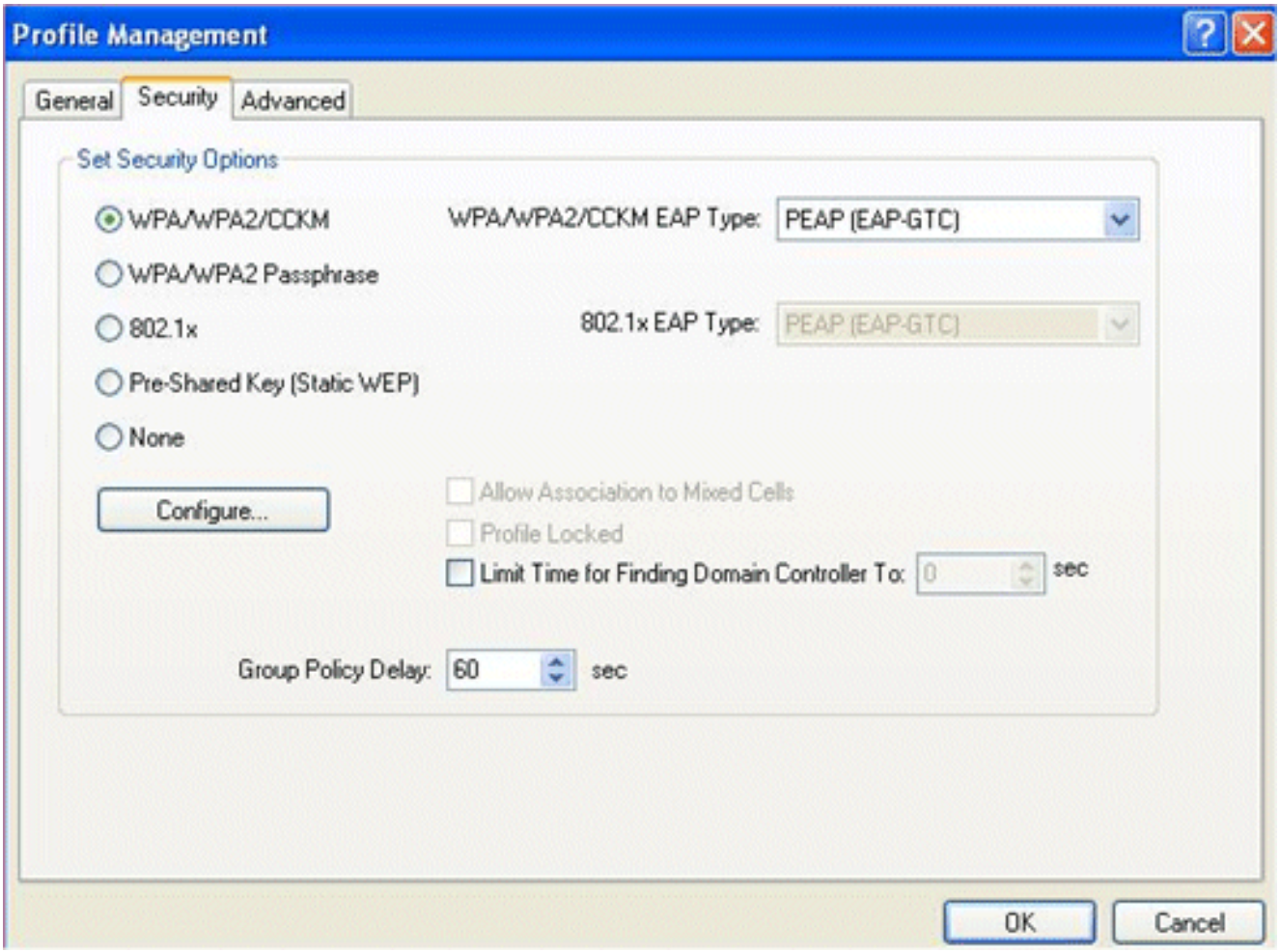
PEAP-GTC est la condition requise en cours d'authentification pour la majorité des écoles K-12. WLC ne prend en charge pas MSCHAPv2 pour l'authentification EAP locale. En conséquence, vous devez choisir GTC pour le type d'authentification EAP sur le client.

Les figures suivantes sont une revue du projet de la configuration de Cisco Aironet Desktop Utility pour que PEAP-GTC connecte au Novell WLAN SSID. Des configurations semblables sont réalisées avec le client indigène de Microsoft avec le support PEAP-GTC.

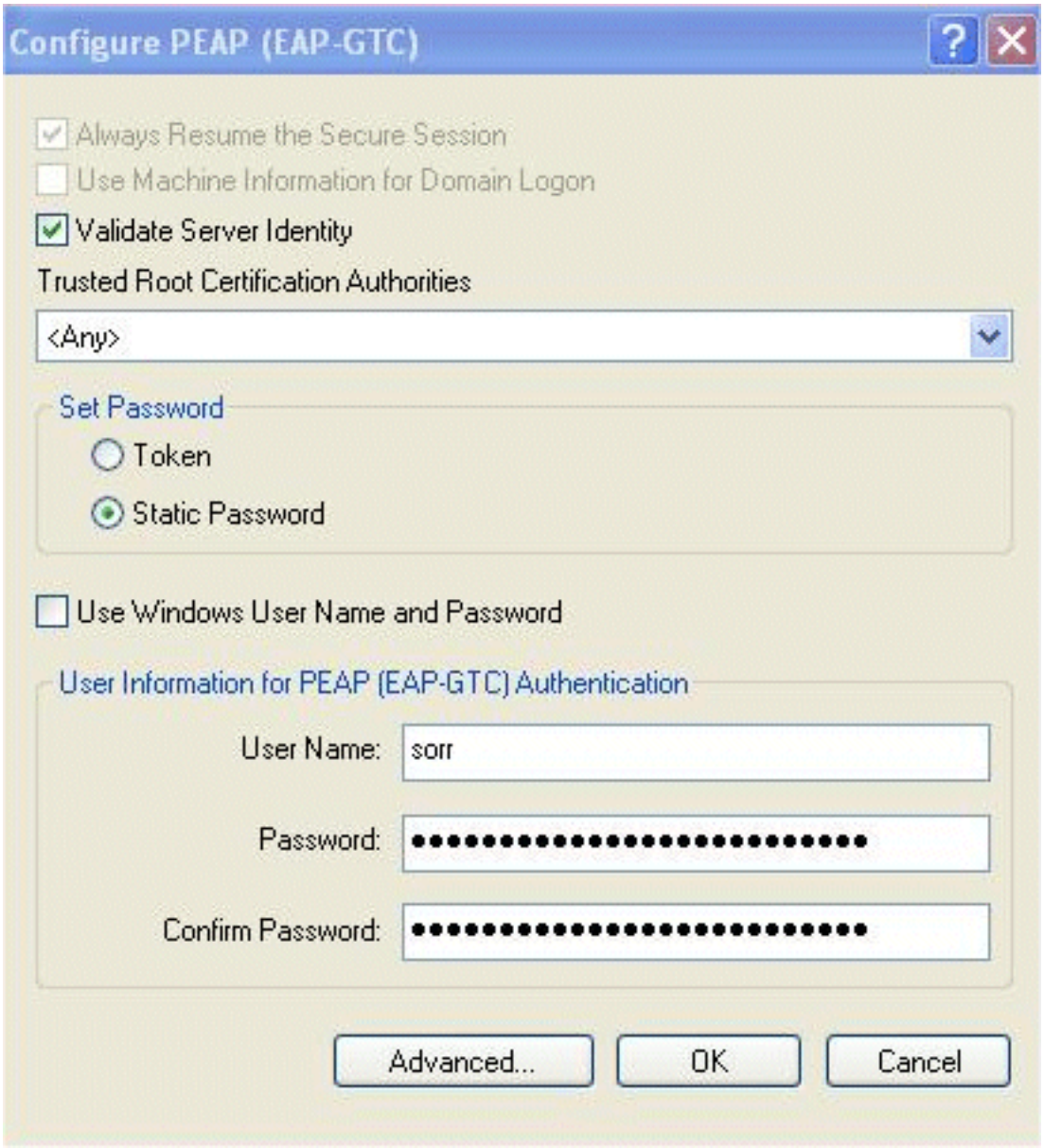
1. Configurez le nom de profil de client et le SSID (Novell).**Figure 18**



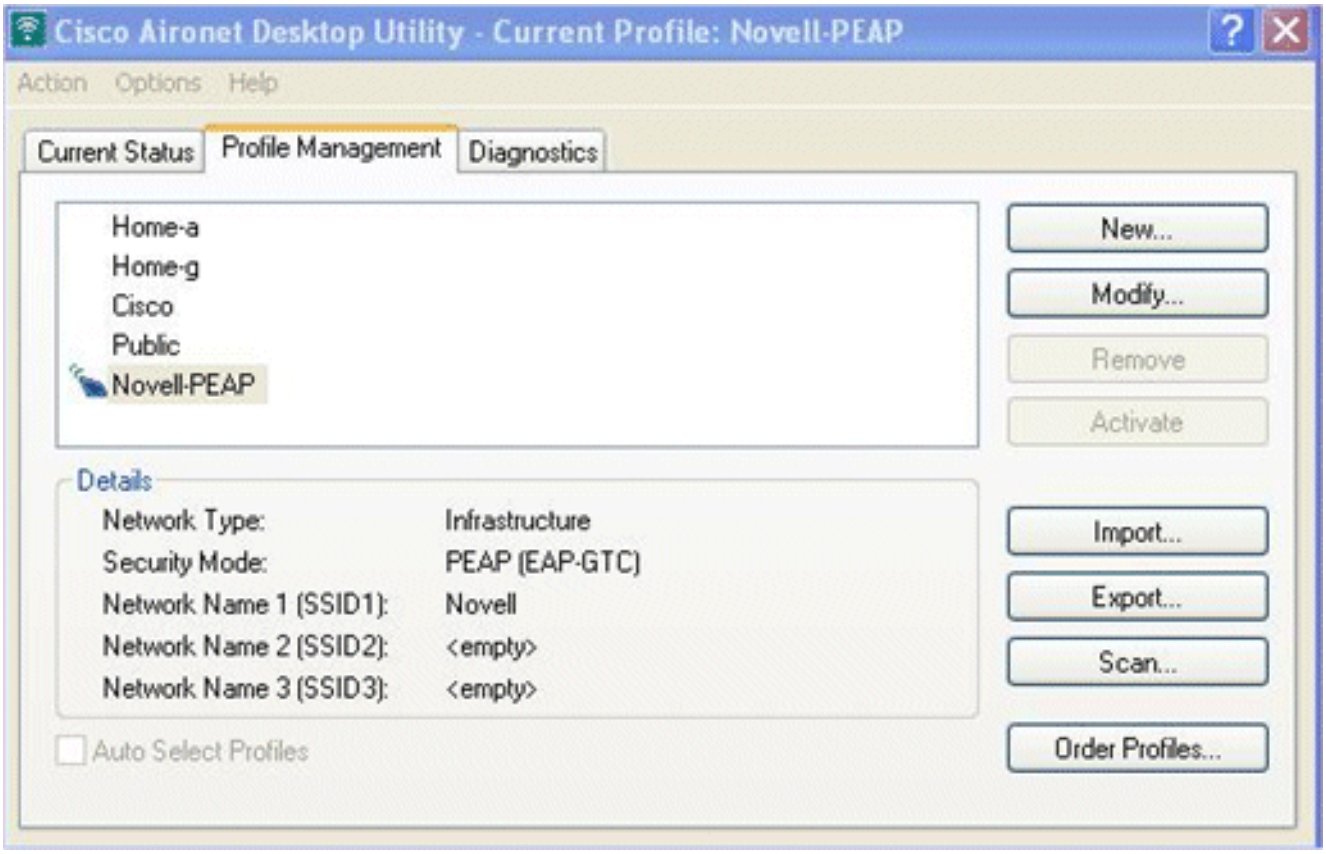
2. Choisissez **WPA/WPA2/CCKM** pour la Sécurité et le **PEAP (EAP-GTC)** pour le type d'EAP.**Figure 19**



3. Configurez PEAP-GTC :Choisissez **valident l'identité de serveur** et le **mot de passe statique**.Écrivez le nom d'utilisateur et mot de passe pour le compte ou le suppliant incitera pour les qualifications à la connexion.N'entrez pas dans le schéma de répertoire de Novell **<ANY>**, comme ceci n'est pas exigé.**Figure 20**

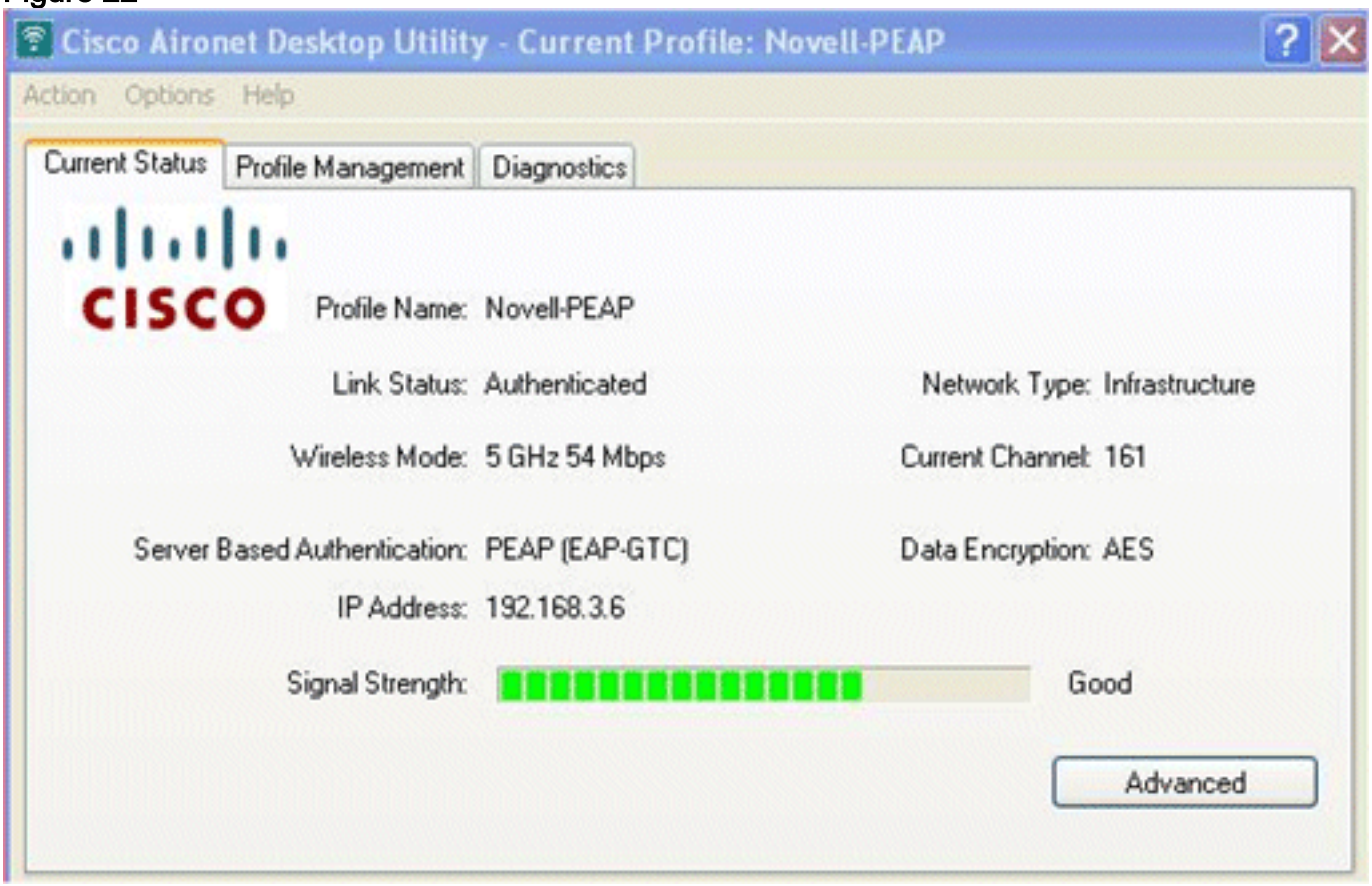


4. Une fois que le profil est terminé, lancez-le et la procédure d'authentification devrait commencer.**Figure 21**



La figure 22 dépeint une association et une authentification réussies par l'intermédiaire de PEAP-GTC.

Figure 22



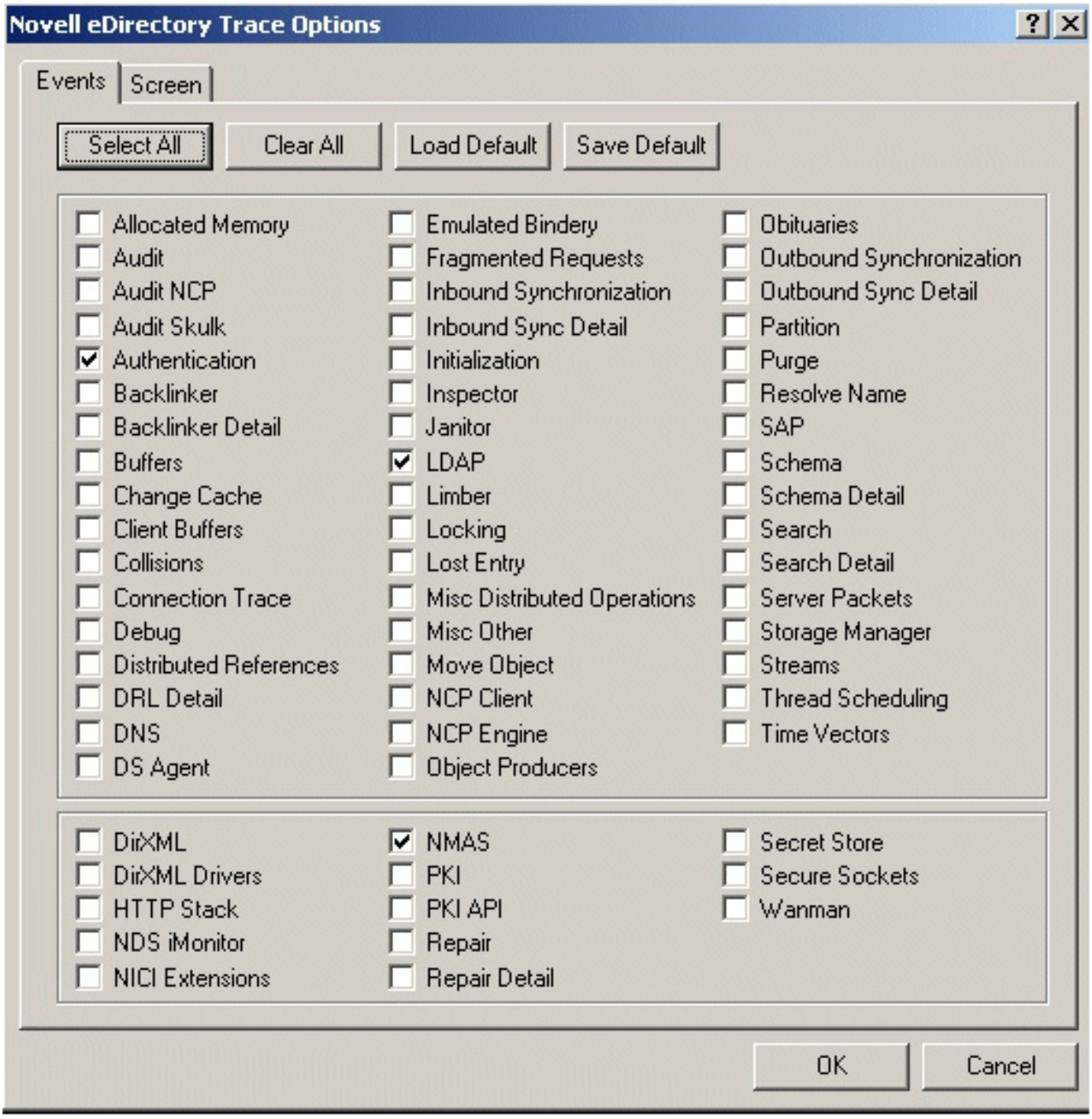
Debugs

Pour vérifier que vous pouvez exécuter un GRIPPAGE authentifié aussi bien que l'authentification

de l'utilisateur, activent ces options de suivi pour eDirectory :

- **Authentification**
- **LDAP**
- **NMAS**

Figure 23



Suivant les indications du débogage, une réponse réussie d'authentification LDAP est fournie au contrôleur LAN Sans fil chez 192.168.3.253 :

```
LDAP   : (192.168.3.253:36802)(0x0020:0x63) DoSearch on connection
    0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
```

```
      attribute: "dn"
      attribute: "userPassword"
Auth   : Starting SEV calculation for conn 23, entry .sorr.ZION.ZION..
Auth   : 1 GlobalGetSEV.
Auth   : 4 GlobalGetSEV succeeded.
Auth   : SEV calculation complete for conn 23, (0:0 s:ms).
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) DoSearch on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) DoBind on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Bind name:cn=sorr,o=ZION, version:3,
    authentication:simple
Auth   : [0000804d] <.sorr.ZION.ZION.> LocalLoginRequest. Error success, conn:
    22.
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Sending operation result 0:"":"" to
    connection 0x34367d0
Auth   : UpdateLoginAttributesThread page 1 processed 1 login in 0 milliseconds
```

Remarque: certaines des lignes du résultat du débogage ont été renvoyées à la ligne à cause des contraintes d'espace.

Pour s'assurer que le WLC fait une demande d'authentification réussie au serveur eDirectory, émettez ces commandes de **débogage** sur le WLC :

```
debug aaa ldap enable

debug aaa local-auth eap method events enable

debug aaa local-auth db enable
```

Sortie témoin d'une authentification réussie :

```
*Dec 23 16:57:04.267: LOCAL_AUTH: (EAP) Sending password verify request profile
    'sorr' to LDAP
*Dec 23 16:57:04.267: AuthenticationRequest: 0xcdb6d54
*Dec 23 16:57:04.267:   Callback.....................................0x84cab60
*Dec 23 16:57:04.267:   protocolType.................................0x00100002
*Dec 23 16:57:04.267:   proxyState...................................
    00:40:96:A6:D6:CB-00:00
*Dec 23 16:57:04.267:   Packet contains 3 AVPs (not shown)
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from method
*Dec 23 16:57:04.267: ldapTask [1] received msg 'REQUEST' (2) in state
    'CONNECTED' (3)
*Dec 23 16:57:04.267: disabled LDAP_OPT_REFERRALS
*Dec 23 16:57:04.267: LDAP_CLIENT: UID Search (base=o=ZION,
    pattern=(&(objectclass=user)(cn=sorr)))
*Dec 23 16:57:04.269: LDAP_CLIENT: ldap_search_ext_s returns 0 85
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned 2 msgs including 0 references
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 1 type 0x64
```

```
*Dec 23 16:57:04.269: LDAP_CLIENT: Received 1 attributes in search entry msg
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 2 type 0x65
*Dec 23 16:57:04.269: LDAP_CLIENT : No matched DN
*Dec 23 16:57:04.269: LDAP_CLIENT : Check result error 0 rc 1013
*Dec 23 16:57:04.269: LDAP_CLIENT: Received no referrals in search result msg
*Dec 23 16:57:04.269: ldapAuthRequest [1] called lcapi_query base="o=ZION"
    type="user" attr="cn" user="sorr" (rc = 0 - Success)
*Dec 23 16:57:04.269: Attempting user bind with username cn=sorr,o=ZION
*Dec 23 16:57:04.273: LDAP ATTR> dn = cn=sorr,o=ZION (size 14)
*Dec 23 16:57:04.273: Handling LDAP response Success
*Dec 23 16:57:04.274: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.274: LOCAL_AUTH: (EAP:448) Password verify credential callback
    invoked
*Dec 23 16:57:04.274: eap_gtc.c-TX-AUTH-PAK:
*Dec 23 16:57:04.274: eap_core.c:1484: Code:SUCCESS  ID:0x 8  Length:0x0004
    Type:GTC
*Dec 23 16:57:04.274: EAP-EVENT: Received event 'EAP_METHOD_REPLY' on handle
    0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: Handling asynchronous method response for
    context 0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method state: Done
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method decision: Unconditional Success
*Dec 23 16:57:04.274: EAP-EVENT: Sending method directive 'Free Context' on
    handle 0xBB000075
*Dec 23 16:57:04.274: eap_gtc.c-EVENT: Free context
*Dec 23 16:57:04.274: id_manager.c-AUTH-SM: Entry deleted fine id 68000002 -
    id_delete
*Dec 23 16:57:04.274: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xBB000075
*Dec 23 16:57:04.274: peap_inner_method.c-AUTH-EVENT: EAP_SUCCESS from inner
    method GTC
*Dec 23 16:57:04.278: LOCAL_AUTH: EAP: Received an auth request
*Dec 23 16:57:04.278: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.278: LOCAL_AUTH: (EAP:448) Sending the Rxd EAP packet (id 9) to
    EAP subsys
*Dec 23 16:57:04.280: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) ---> [KEY AVAIL] send_len 64,
    recv_len 64
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) received keys waiting for success
*Dec 23 16:57:04.280: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xEE000074
*Dec 23 16:57:04.281: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Received success event
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Processing keys success
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] AAA response 'Success'
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] Returning AAA response
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb AAA Message 'Success' received for
    mobile 00:40:96:a6:d6:cb
```

Remarque: Certaines des lignes dans la sortie ont été dues enveloppé aux contraintes de l'espace.

Car plus d'écoles K-12 adoptent l'architecture de WLAN Cisco, il y aura un besoin croissant de prendre en charge l'authentification d'utilisateur de sans fil au Novell eDirectory. Ce document a vérifié qu'un Cisco WLC peut authentifier des utilisateurs contre la base de données eDirectory du LDAP du Novell une fois configuré pour l'authentification EAP locale. Une configuration semblable peut également être faite avec le Cisco Secure ACS authentifiant des utilisateurs au Novell eDirectory. Des recherches plus approfondies doivent être faites pour simple se connectent avec d'autres clients WLAN tels que la configuration zéro de Cisco Secure Services Client et de Microsoft Windows.

Informations connexes

- Exemple de configuration d'authentification EAP locale sur le contrôleur de réseau local sans fil avec un serveur EAP-FAST et LDAP
- Exemple de configuration d'un serveur EAP local dans un réseau sans fil unifié Cisco
- Exemple de configuration d'authentification EAP-FAST avec des contrôleurs de réseau local sans fil et un serveur RADIUS externe
- Support et documentation techniques - Cisco Systems