Exemple de configuration d'authentification Web avec LDAP sur les contrôleurs de réseau local sans fil

Table des matières

Introduction

Ce document décrit comment configurer un contrôleur de réseau local sans fil (WLC) pour l'authentification Web. Il explique comment configurer un serveur LDAP (Lightweight Directory Access Protocol) comme base de données principale pour l'authentification Web afin de récupérer les informations d'identification de l'utilisateur et de l'authentifier.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la configuration des points d'accès légers (LAP) et des WLC Cisco
- Connaissance du contrôle et du provisionnement du protocole CAPWAP (Wireless Access Point Protocol)
- Connaissance de la configuration du protocole LDAP (Lightweight Directory Access Protocol), d'Active Directory et des contrôleurs de domaine

Composants utilisés

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

- WLC Cisco 5508 exécutant la version de microprogramme 8.2.100.0
- LAP de la gamme Cisco 1142
- Adaptateur client sans fil Cisco 802.11a/b/g.
- Serveur Microsoft Windows 2012 Essentials qui joue le rôle de serveur LDAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Conventions

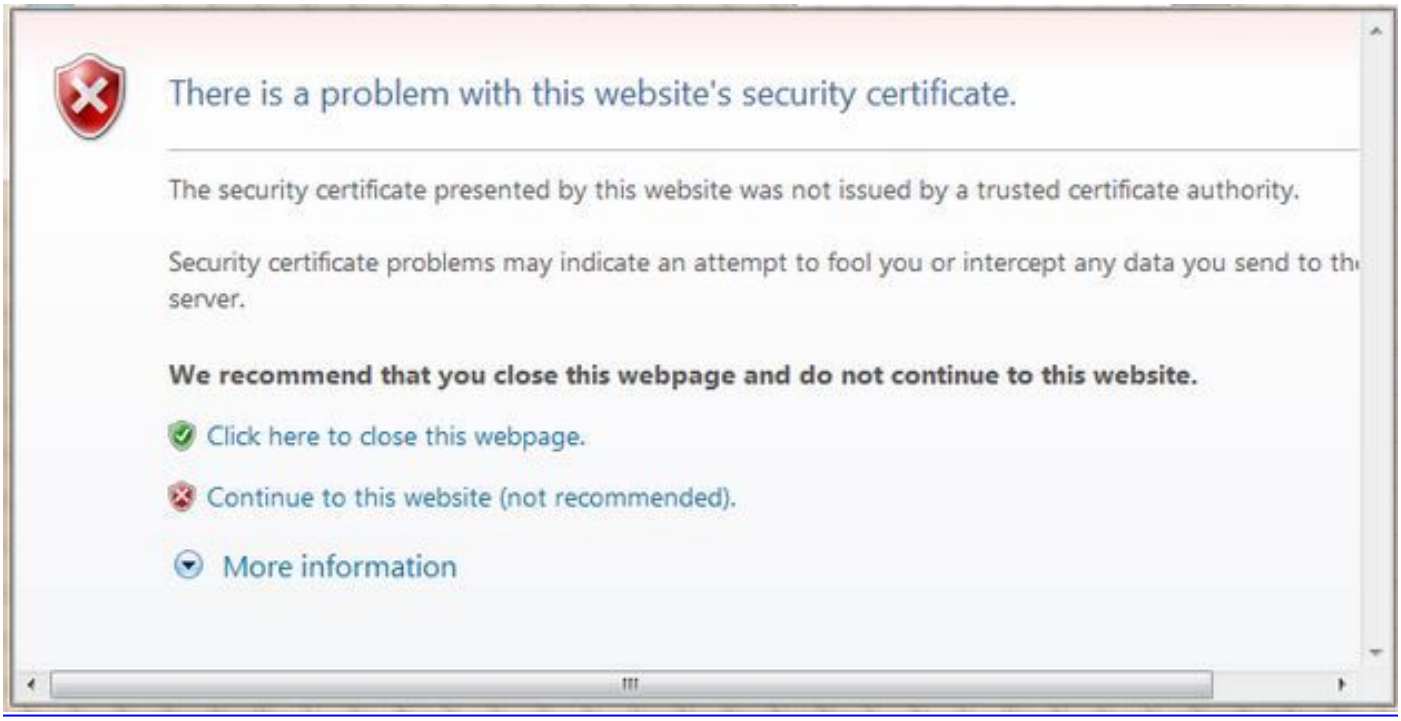
Pour plus d’informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Procédé d'authentification Web

L'authentification Web est une fonctionnalité de sécurité de couche 3 qui amène le contrôleur à interdire le trafic IP (à l'exception des paquets DHCP et DNS) à partir d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur et un mot de passe valides. Lorsque vous utilisez l'authentification Web pour authentifier des clients, vous devez définir un nom d'utilisateur et un mot de passe pour chaque client. Ensuite, lorsque les clients tentent de se connecter au réseau local sans fil, ils doivent saisir le nom d'utilisateur et le mot de passe lorsqu'une page de connexion leur demande de le faire.

Lorsque l'authentification Web est activée (sous Sécurité de couche 3), les utilisateurs reçoivent occasionnellement une alerte de sécurité de navigateur Web la première fois qu'ils tentent d'accéder à une URL.

> **Conseil** : pour supprimer cet avertissement de certificat, revenez au guide suivant sur l'installation d'un certificat de confiance tiers http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html



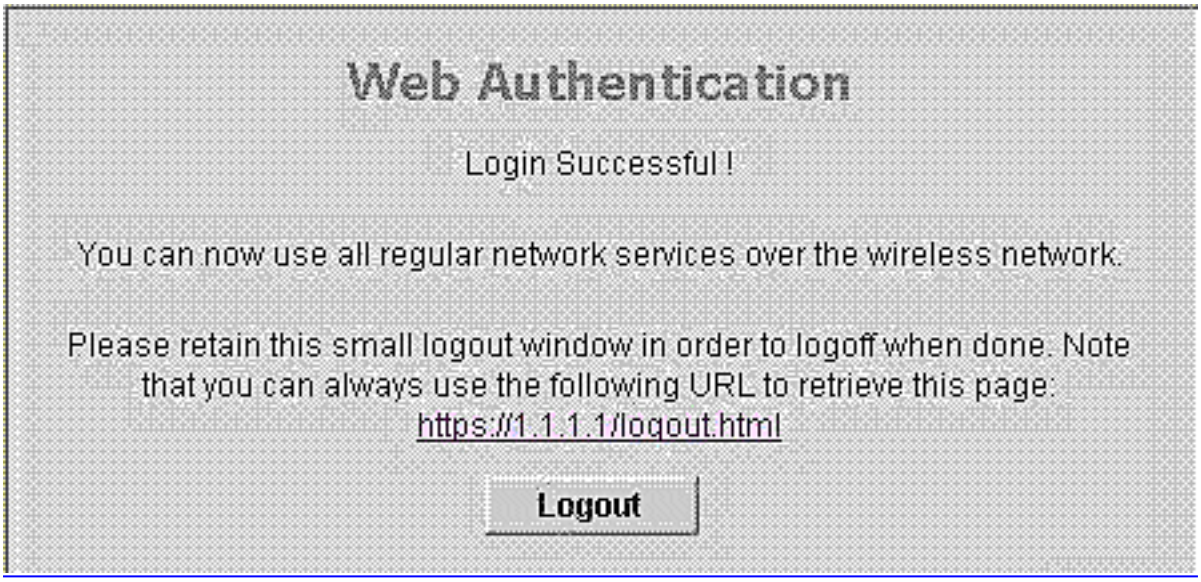
Après avoir cliqué sur **Yes** pour continuer (ou plus précisément **Continue to this website (not Recommended)** pour le navigateur Firefox par exemple), ou si le navigateur du client n'affiche pas d'alerte de sécurité, le système d'authentification Web redirige le client vers une page de connexion, comme illustré dans l'image :

La page de connexion par défaut contient un logo Cisco et un texte spécifique à Cisco. Vous pouvez choisir que le système d'authentification Web affiche l'une des options suivantes :

- La page de connexion par défaut
- Version modifiée de la page de connexion par défaut
- Une page de connexion personnalisée que vous configurez sur un serveur Web externe

- Une page de connexion personnalisée que vous téléchargez sur le contrôleur

Lorsque vous entrez un nom d'utilisateur et un mot de passe valides sur la page de connexion d'authentification Web et cliquez sur **Submit**, vous êtes authentifié en fonction des informations d'identification envoyées et d'une authentification réussie à partir de la base de données principale (LDAP dans ce cas). Le système d'authentification Web affiche alors une page de connexion réussie et redirige le client authentifié vers l'URL demandée.



La page de connexion réussie par défaut contient un pointeur vers l'adresse URL d'une passerelle virtuelle : https://1.1.1.1/logout.html. L'adresse IP que vous définissez pour l'interface virtuelle du contrôleur sert d'adresse de redirection pour la page de connexion.

Ce document explique comment utiliser la page Web interne sur le WLC pour l'authentification Web. Cet exemple utilise un serveur LDAP comme base de données principale pour l'authentification Web afin de récupérer les informations d'identification et d'authentification de l'utilisateur.

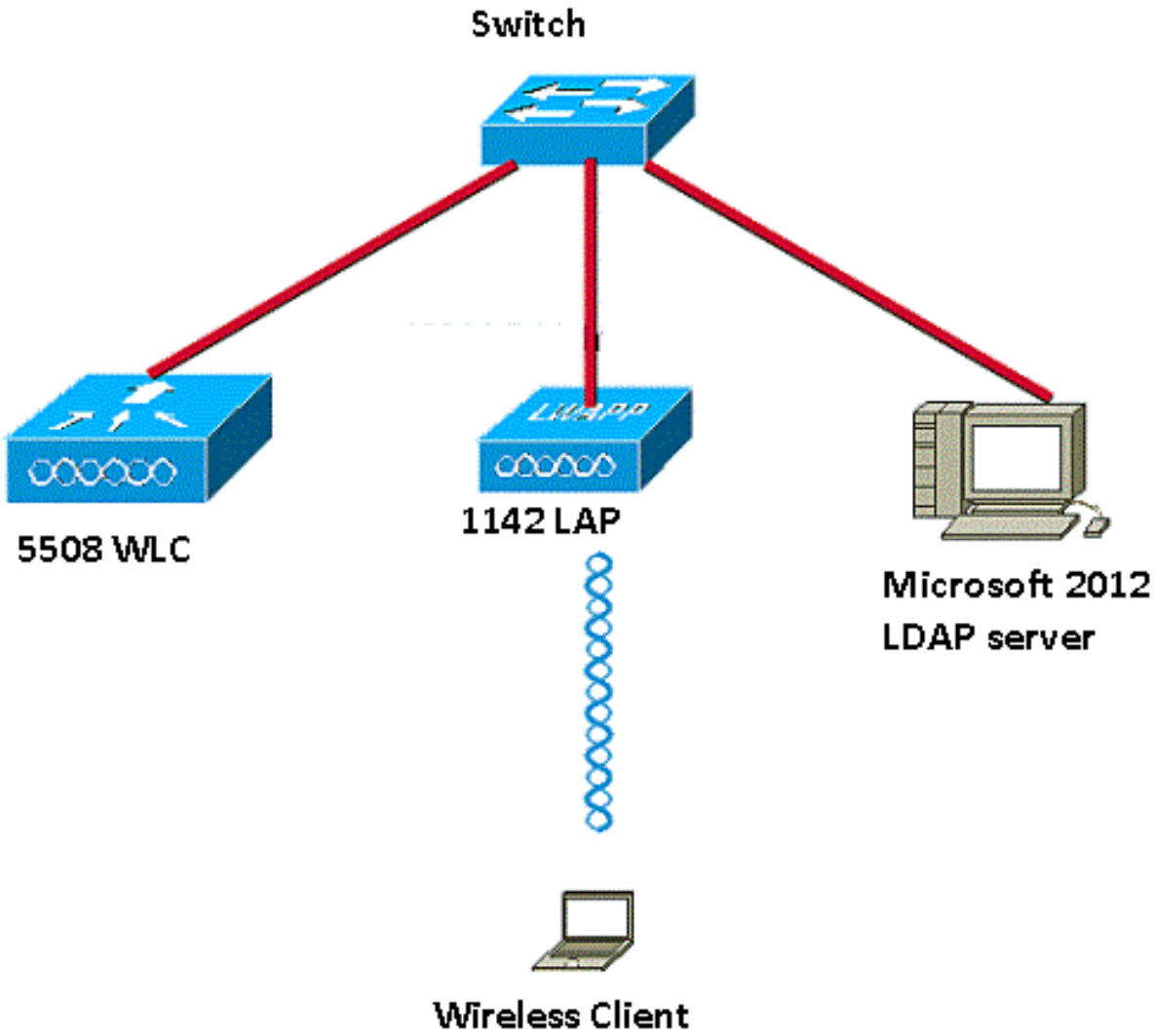
Configurer

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

> **Remarque** : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Complétez ces étapes afin d'implémenter avec succès cette configuration :

- Configurez le serveur LDAP.
- Configurez le WLC pour le serveur LDAP.
- Configurez le WLAN pour l'authentification Web.

Configuration du serveur LDAP

La première étape consiste à configurer le serveur LDAP, qui sert de base de données principale pour stocker les informations d'identification des utilisateurs des clients sans fil. Dans cet exemple, le serveur Microsoft Windows 2012 Essentials est utilisé comme serveur LDAP.

La première étape de la configuration du serveur LDAP consiste à créer une base de données utilisateur sur le serveur LDAP afin que le WLC puisse interroger cette base de données pour authentifier l'utilisateur.

Créer des utilisateurs sur le contrôleur de domaine

Une unité d'organisation contient plusieurs groupes qui contiennent des références à des entrées personnelles dans un profil de personne. Une personne peut être membre de plusieurs groupes.

Toutes les définitions de classe d'objet et d'attribut sont des définitions de schéma LDAP par défaut. Chaque groupe contient des références (dn) pour chaque personne qui lui appartient.

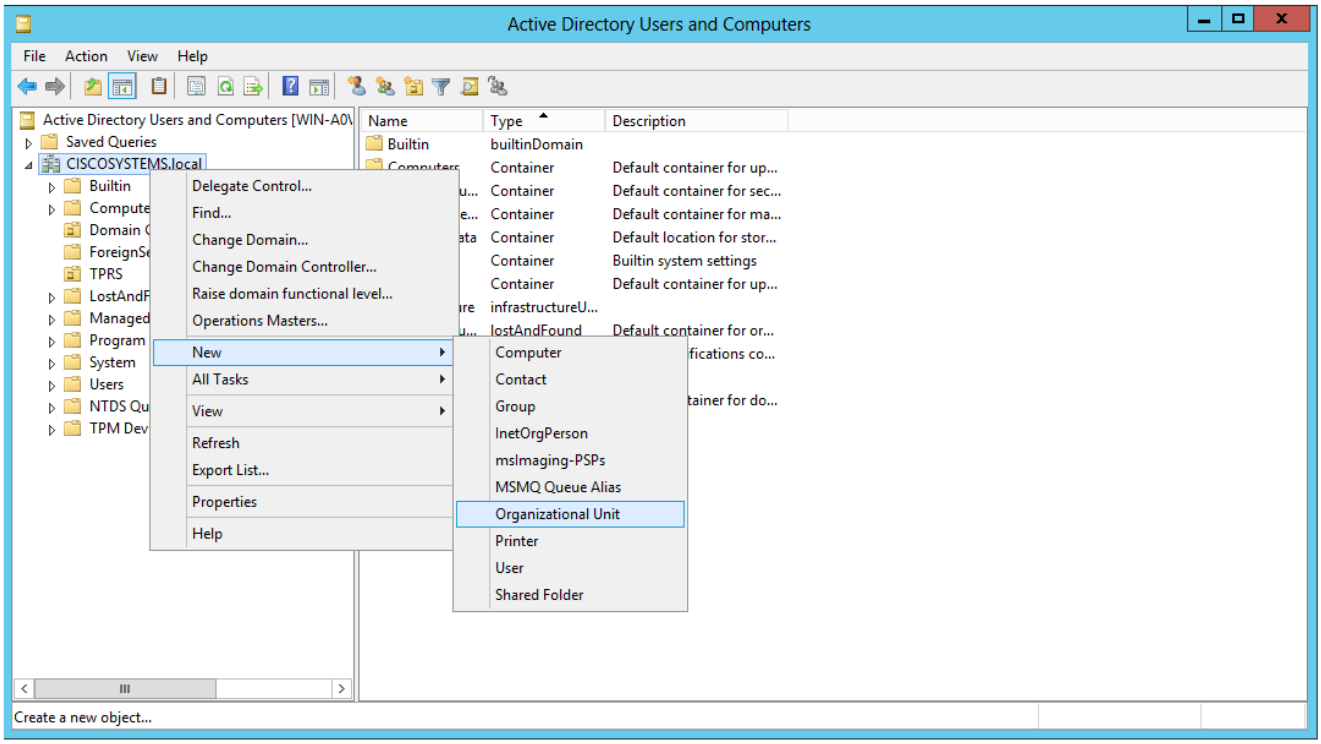
Dans cet exemple, une nouvelle unité d'organisation LDAP-USERS est créée et l'utilisateur User1 est créé sous cette unité d'organisation. Lorsque vous configurez cet utilisateur pour l'accès LDAP, le WLC peut interroger cette base de données LDAP pour l'authentification des utilisateurs.

Le domaine utilisé dans cet exemple est **CISCOSYSTEMS.local**.

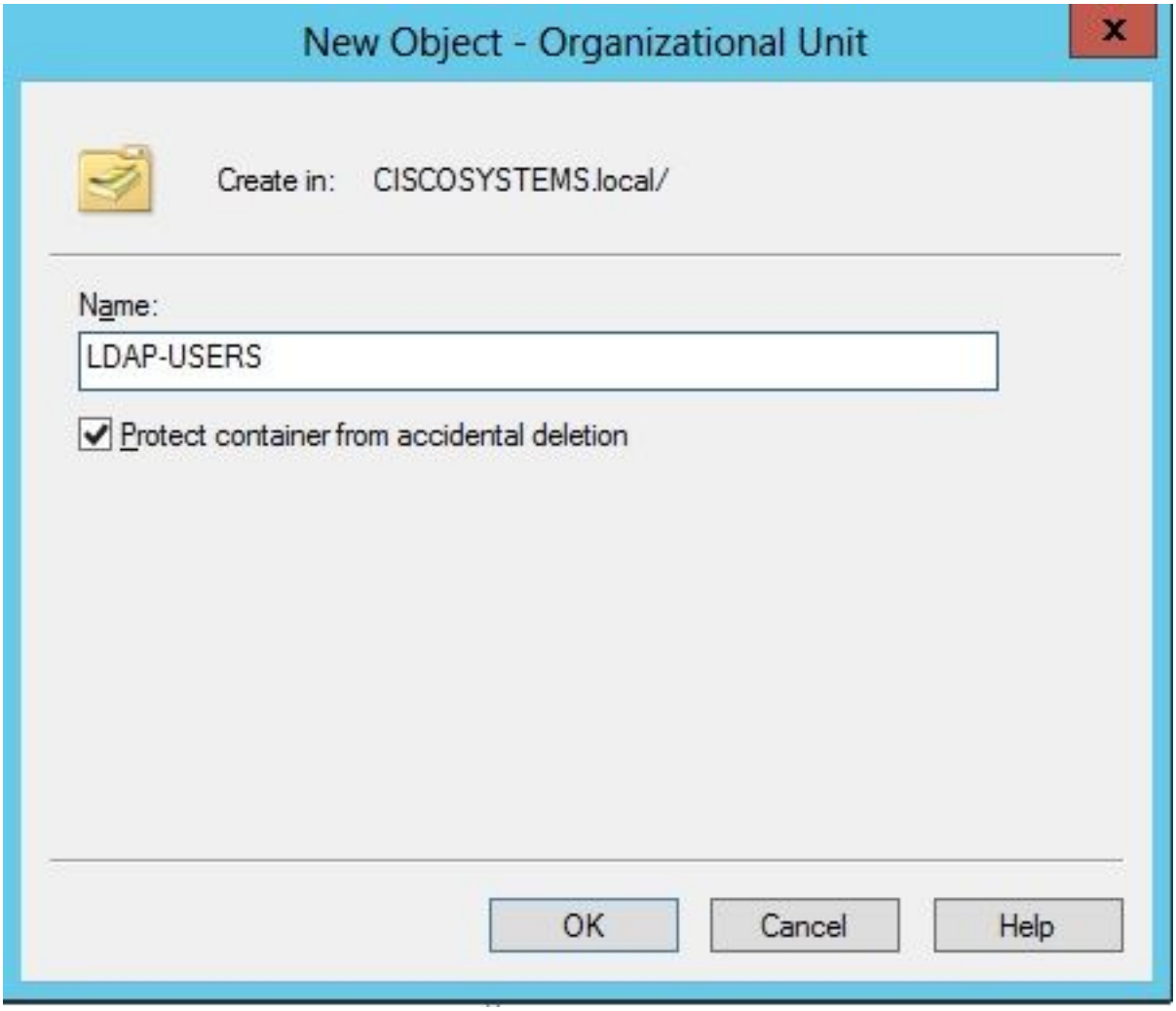
Créer une base de données utilisateur sous une unité organisationnelle

Cette section explique comment créer une nouvelle unité d'organisation dans votre domaine et créer un nouvel utilisateur sur cette unité d'organisation.

1. Ouvrez Windows PowerShell et tapez **servermanager.exe**
2. Dans la fenêtre Gestionnaire de serveur, cliquez sur **AD DS.** Cliquez ensuite avec le bouton droit sur le nom de votre serveur pour choisir **Utilisateurs et ordinateurs Active Directory.**
3. Cliquez avec le bouton droit sur votre nom de domaine, qui est **CISCOSYSTEMS.local** dans cet exemple, puis accédez à **Nouveau > Unité d'organisation** à partir du menu contextuel afin de créer une nouvelle unité d'organisation.

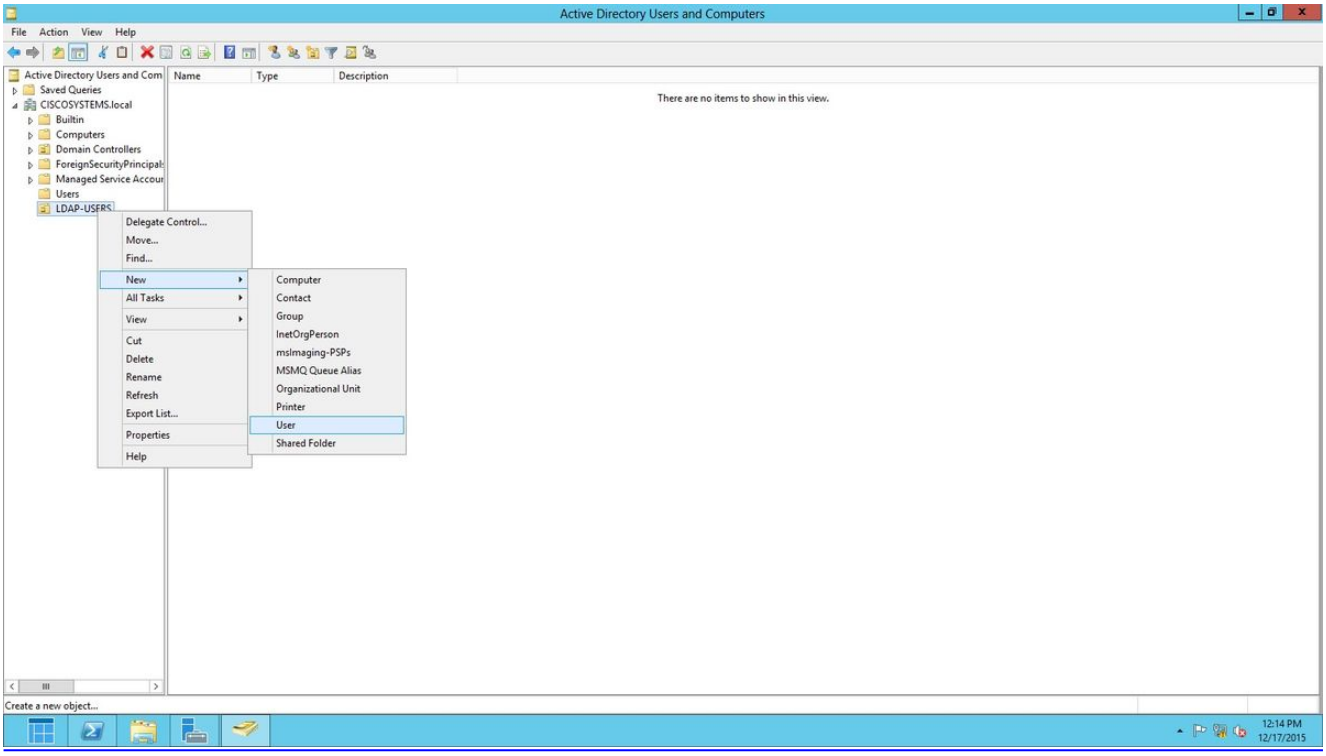


4. Attribuez un nom à cette unité d'organisation et cliquez sur **OK**, comme illustré dans l'image :



Maintenant que la nouvelle unité d'organisation LDAP-USERS est créée sur le serveur LDAP, l'étape suivante consiste à créer l'utilisateur **User1** sous cette unité d'organisation. Pour ce faire, procédez comme suit :

1. Cliquez avec le bouton droit sur la nouvelle unité organisationnelle créée. Accédez à **LDAP-USERS> New > User** à partir des menus contextuels résultants afin de créer un nouvel utilisateur, comme indiqué dans l'image :

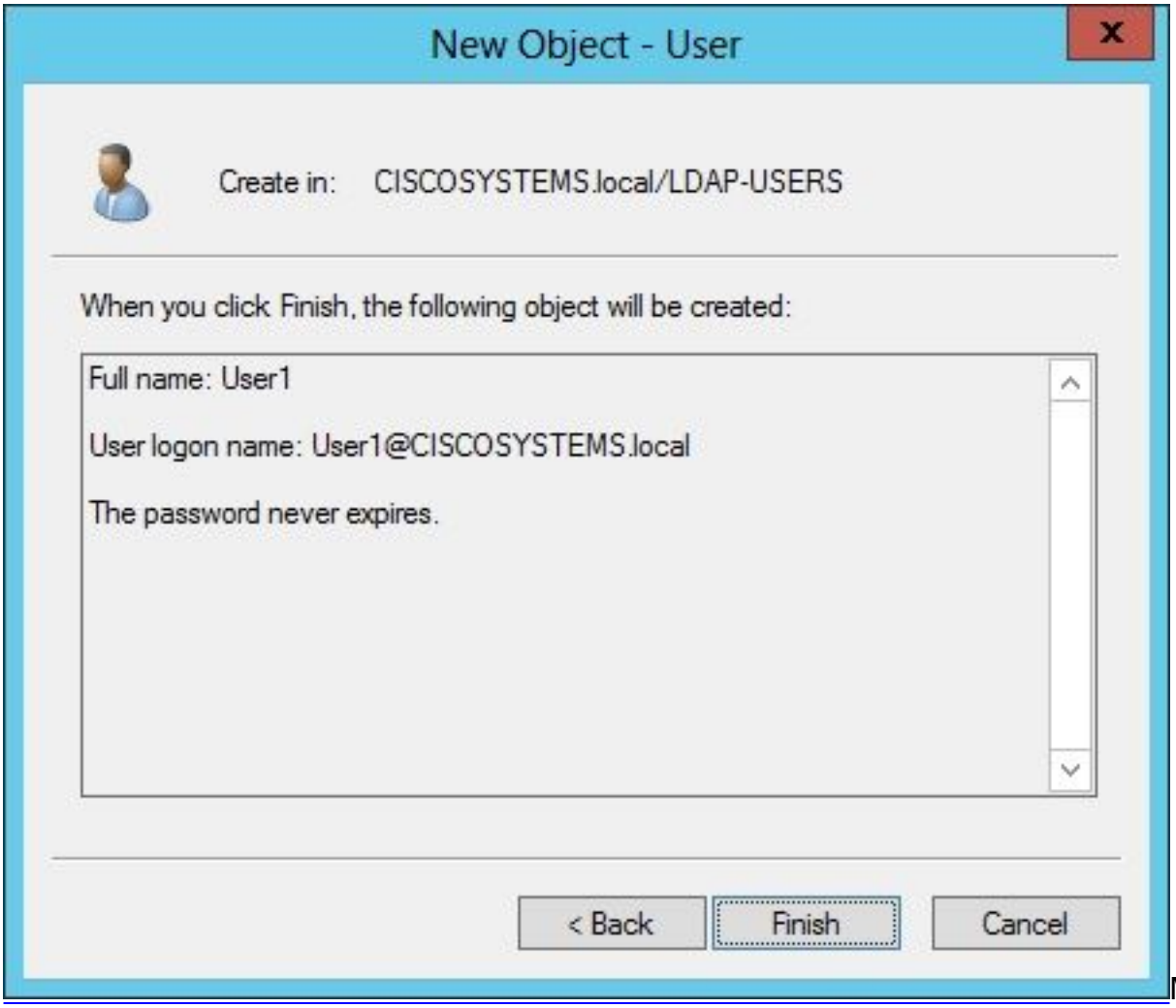


2. Dans la page User setup, renseignez les champs obligatoires comme indiqué dans cet exemple. Dans cet exemple, **User1** figure dans le champ **User logon name**.Il s'agit du nom d'utilisateur vérifié dans la base de données LDAP pour authentifier le client. Cet exemple utilise User1 dans les champs Prénom et Nom complet. Cliquez sur **Next** (Suivant).

3. Entrez un mot de passe et confirmez-le. Sélectionnez l'option **Password never expires** et

cliquez sur **Next**.

4. Cliquez sur **Finish** (Terminer).Un nouvel utilisateur User1 est créé sous l'unité d'organisation LDAP-USERS. Voici les informations d'identification de l'utilisateur :username : **Utilisateur1**password (mot de passe) : **Ordinateur portable123**



Maintenant que l'utilisateur est créé sous une unité d'organisation, l'étape suivante consiste à configurer cet utilisateur pour l'accès LDAP.

Configurer l'utilisateur pour l'accès LDAP

Vous pouvez choisir **Anonymous** ou **Authenticated** pour spécifier la méthode de liaison d'authentification locale pour le serveur LDAP. La méthode Anonymous permet un accès anonyme au serveur LDAP. La méthode Authenticated nécessite la saisie d'un nom d'utilisateur et d'un mot de passe pour sécuriser l'accès. La valeur par défaut est Anonymous.

Cette section explique comment configurer les méthodes Anonymous et Authenticated.

Liaison anonyme

> **Remarque** : l'utilisation de la liaison anonyme n'est pas recommandée. Un serveur LDAP qui autorise la liaison anonyme ne nécessite aucun type d'authentification avec informations d'identification. Un pirate peut utiliser l'entrée de liaison anonyme pour afficher des fichiers sur le répertoire LDAP.

Suivez les étapes de cette section afin de configurer l'utilisateur anonyme pour l'accès LDAP.

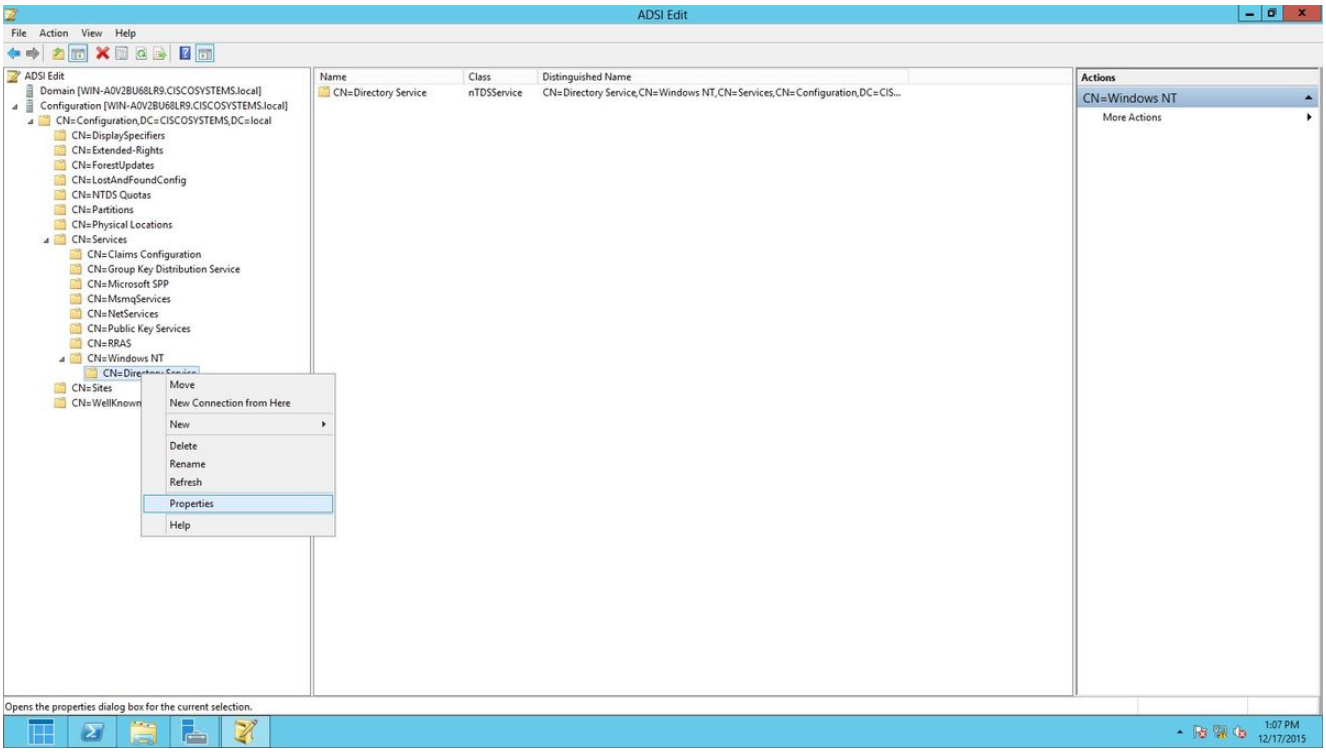
Activer la fonctionnalité de liaison anonyme sur Windows 2012 Essentials Server

Pour que des applications tierces (dans notre cas, WLC) puissent accéder à Windows 2012 AD

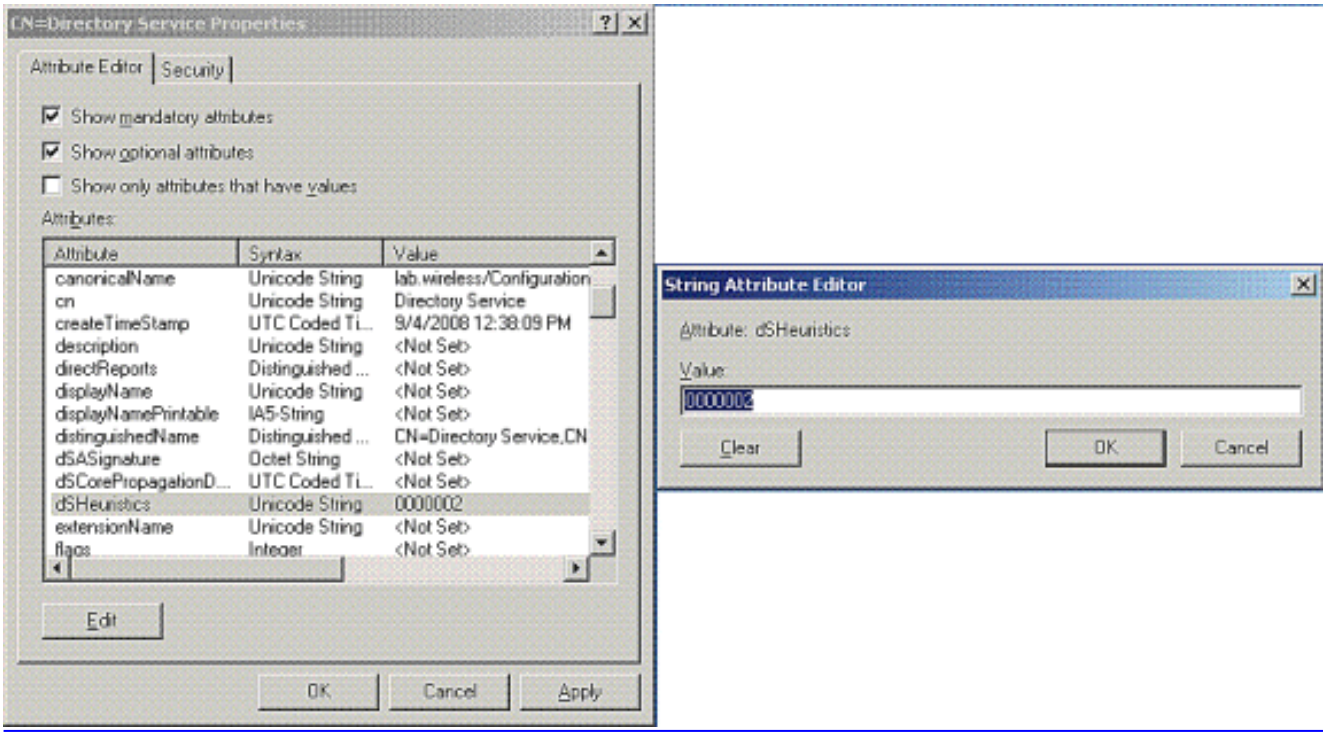
sur le LDAP, la fonctionnalité de liaison anonyme doit être activée sur Windows 2012. Par défaut, les opérations LDAP anonymes ne sont pas autorisées sur les contrôleurs de domaine Windows 2012. Procédez comme suit afin d'activer la fonctionnalité de liaison anonyme :

1. Lancez l'outil d'édition ADSI en tapant : **ADSIEdit.msc** dans Windows PowerShell. Cet outil fait partie des outils de support de Windows 2012.

2. Dans la fenêtre Édition ADSI, développez le domaine racine (Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).Accédez à **CN=Services > CN=Windows NT > CN=Directory Service**. Cliquez avec le bouton droit sur le conteneur **CN=Directory Service**, et choisissez **Properties** dans le menu contextuel, comme illustré dans l'image :



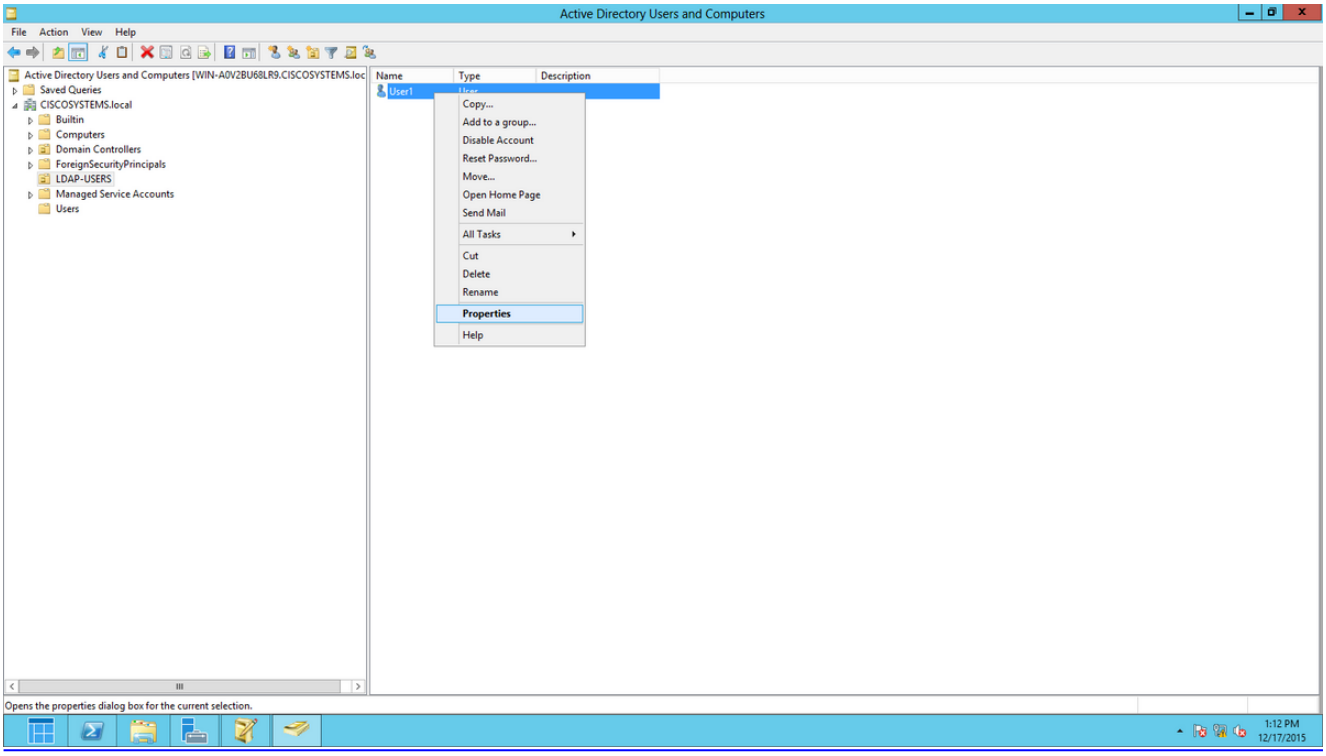
3. Dans la fenêtre CN=Directory Service Properties, sous **Attributes**, cliquez sur l'attribut **dsHeuristics** sous le champ Attribute et choisissez **Edit**. Dans la fenêtre Éditeur d'attributs de chaîne de cet attribut, entrez la valeur **000002** ; cliquez sur **Appliquer** et sur **OK**, comme indiqué dans l'image. La fonctionnalité de liaison anonyme est activée sur le serveur Windows 2012.**Remarque** : le dernier (septième) caractère est celui qui contrôle la façon dont vous pouvez établir une liaison avec le service LDAP. 0 (zéro) ou aucun septième caractère signifie que les opérations LDAP anonymes sont désactivées. Si vous définissez le septième caractère sur 2, il active la fonction Lien anonyme.



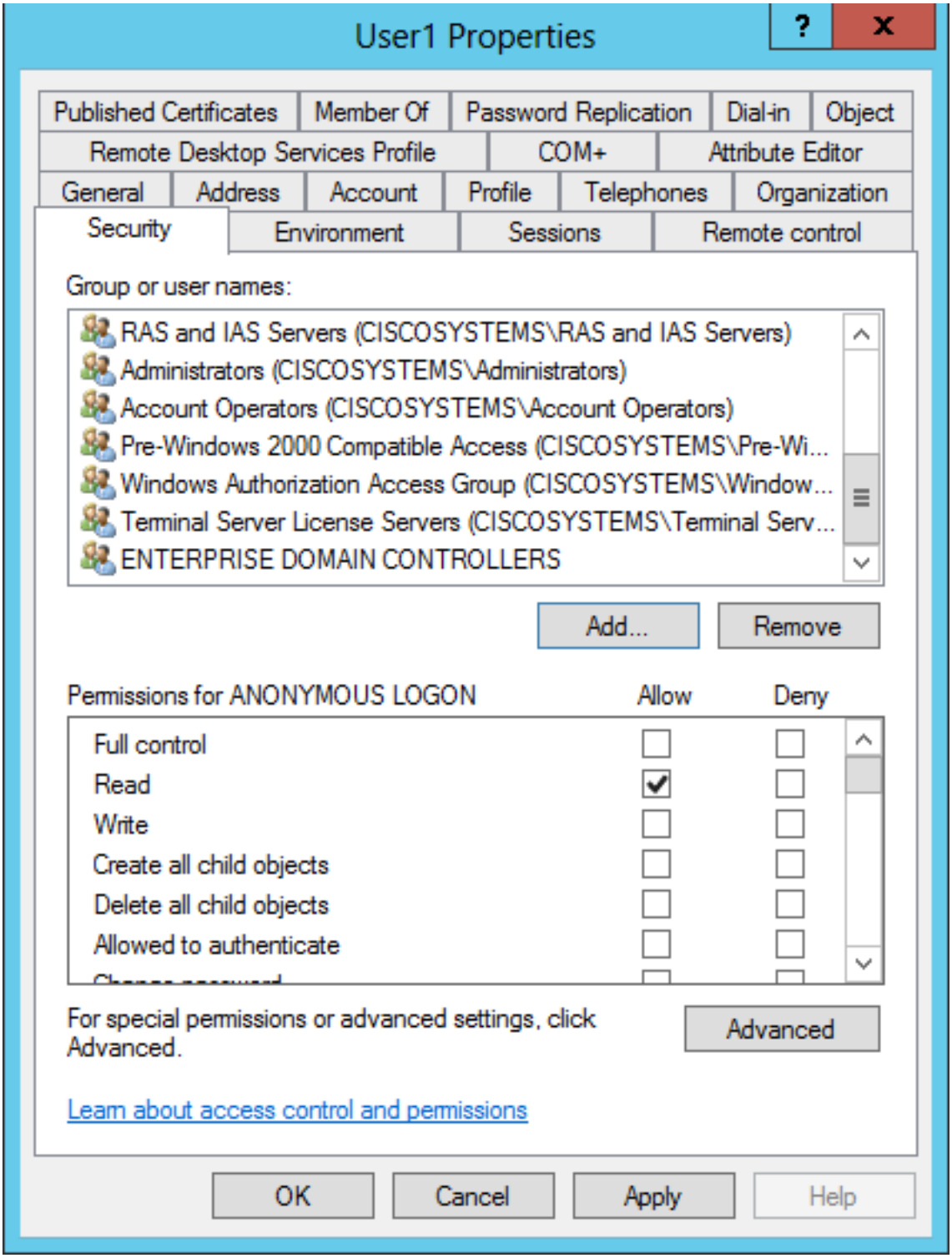
Octroi de l'accès ANONYME à l'utilisateur

L'étape suivante consiste à accorder l'accès CONNEXION ANONYME à l'utilisateur User1. Complétez ces étapes afin d'atteindre ceci :

1. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Assurez-vous que la case **Afficher les fonctionnalités avancées** est cochée.
3. Accédez à l'utilisateur User1 et cliquez dessus avec le bouton droit. Choisissez **Propriétés** dans le menu contextuel. Cet utilisateur est identifié par le prénom User1.

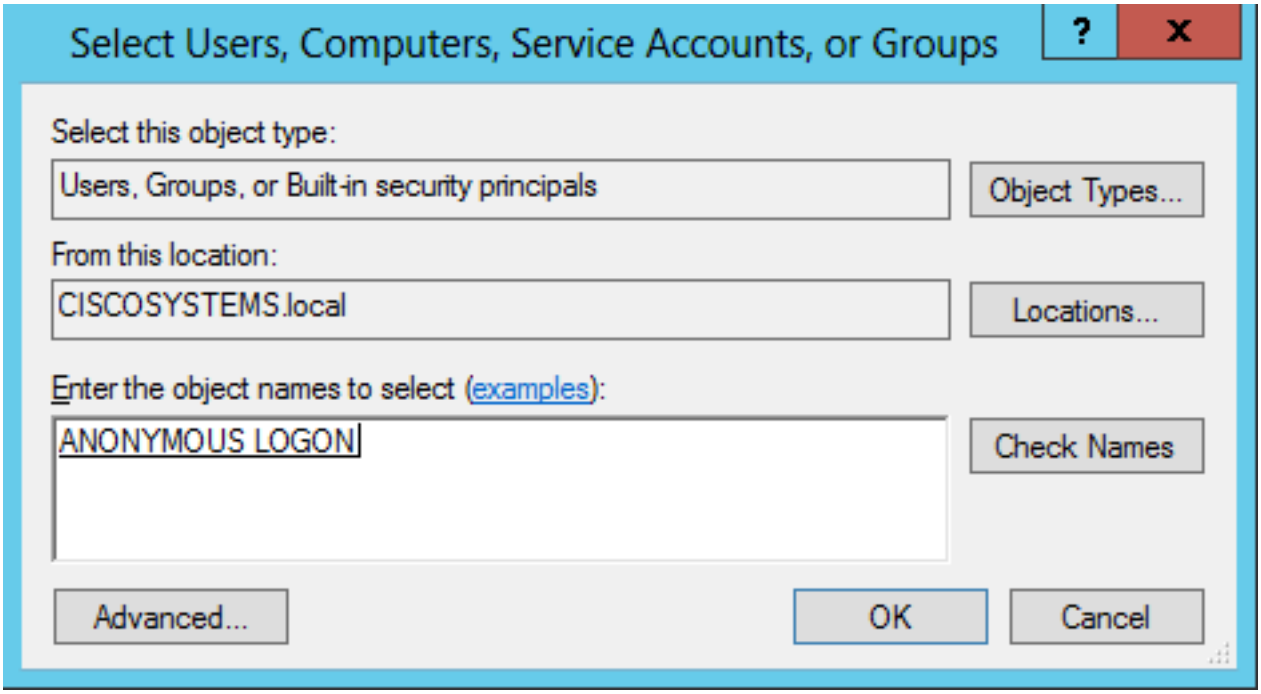


4. Cliquez sur l'onglet **Security**, comme illustré dans l'image :

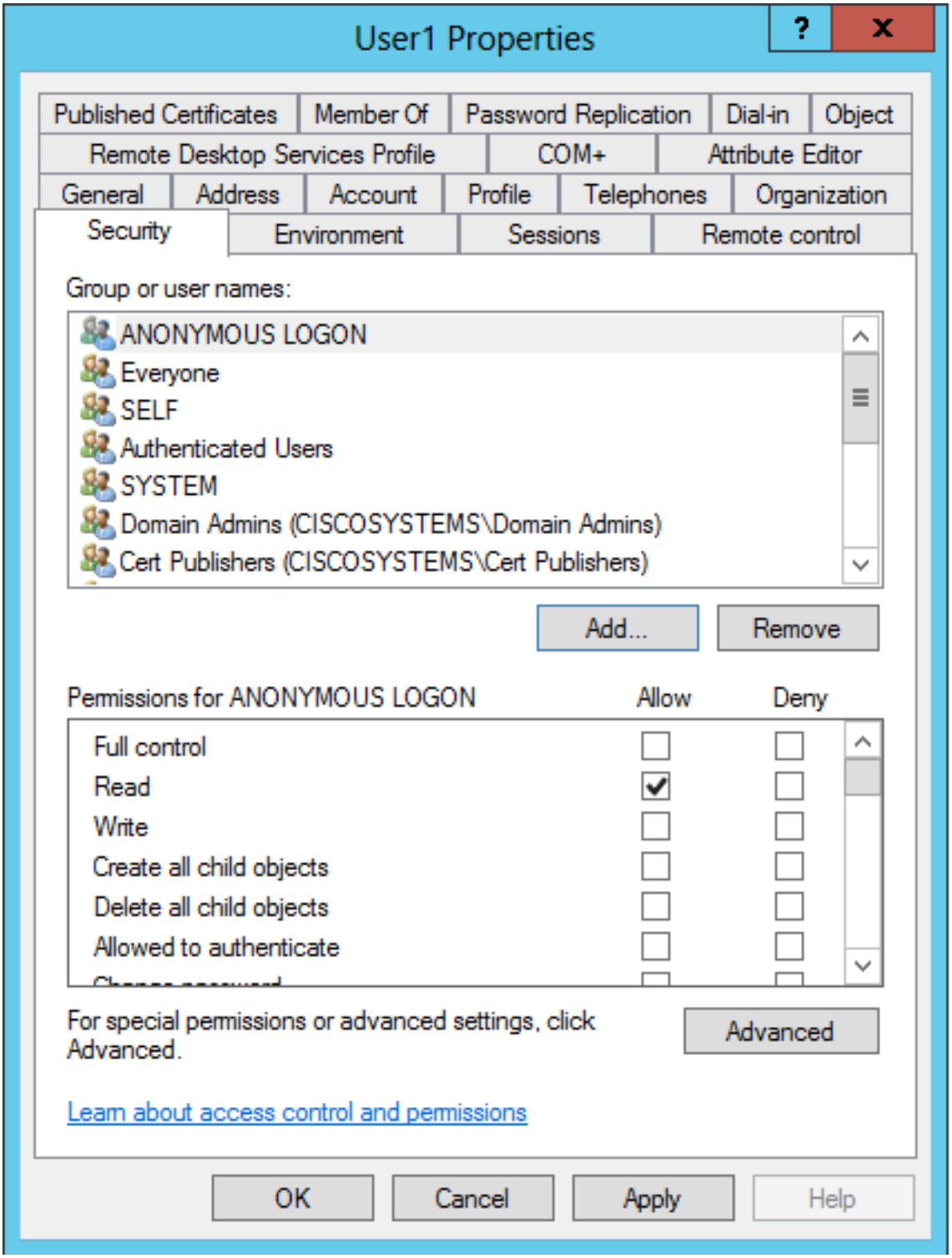


5. Cliquez sur **Add** dans la fenêtre résultante.

6. Entrez **ANONYMOUS LOGON** sous la zone *Entrez les noms des objets à sélectionner* et accédez à la boîte de dialogue, comme illustré dans l'image :



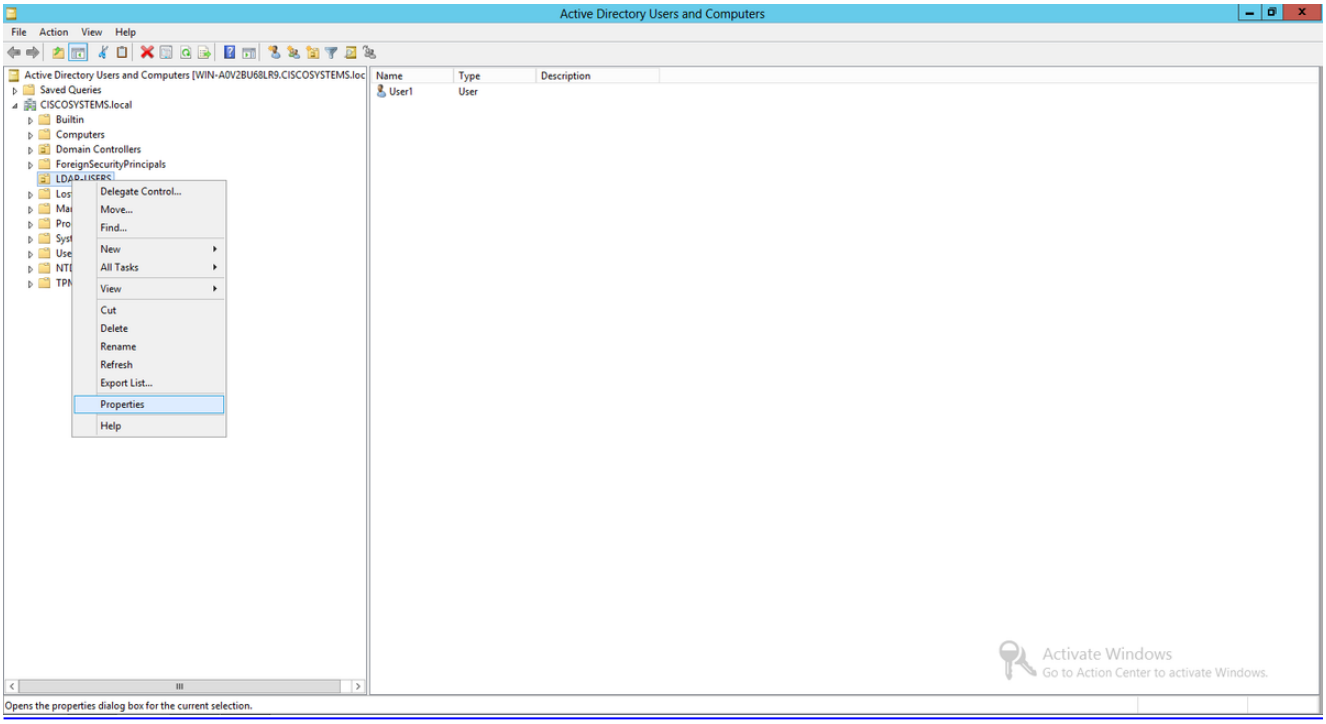
7. Dans la liste de contrôle d’accès, notez que l’OUVERTURE DE SESSION ANONYME a accès à certains jeux de propriétés de l’utilisateur. Click OK. L'accès OUVERTURE DE SESSION ANONYME est accordé à cet utilisateur, comme indiqué dans l'image :



Autorisation du contenu de la liste d'autorisation sur l'unité organisationnelle

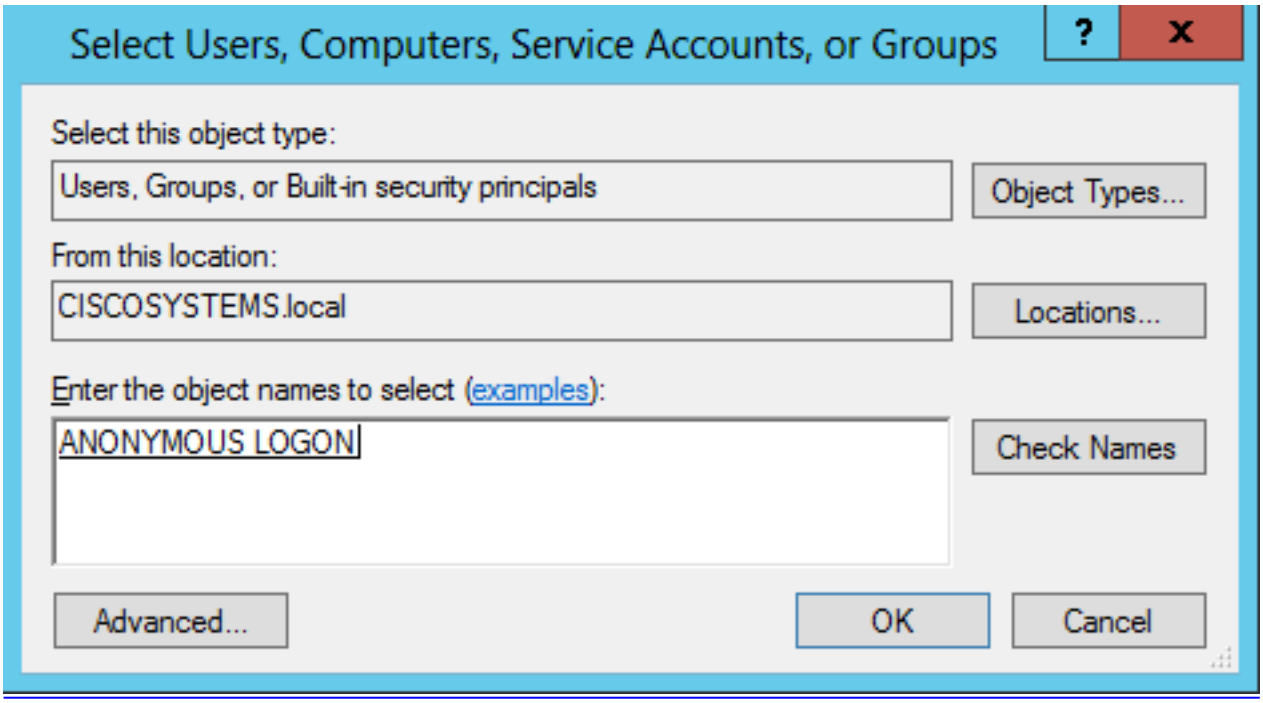
L'étape suivante consiste à accorder au moins l'autorisation List Contents à l'OUVERTURE DE SESSION ANONYME sur l'unité d'organisation dans laquelle se trouve l'utilisateur. Dans cet exemple, User1 se trouve sur l'unité d'organisation LDAP-USERS. Complétez ces étapes afin d'atteindre ceci :

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **OU LDAP-USERS** et choisissez **Properties**, comme illustré dans l'image :



2. Cliquez sur **Sécurité**.

3. Cliquez sur **Add**. Dans la boîte de dialogue qui s'ouvre, entrez **ANONYMOUS LOGON** et Accusez réception de la boîte de dialogue, comme illustré dans l'image :



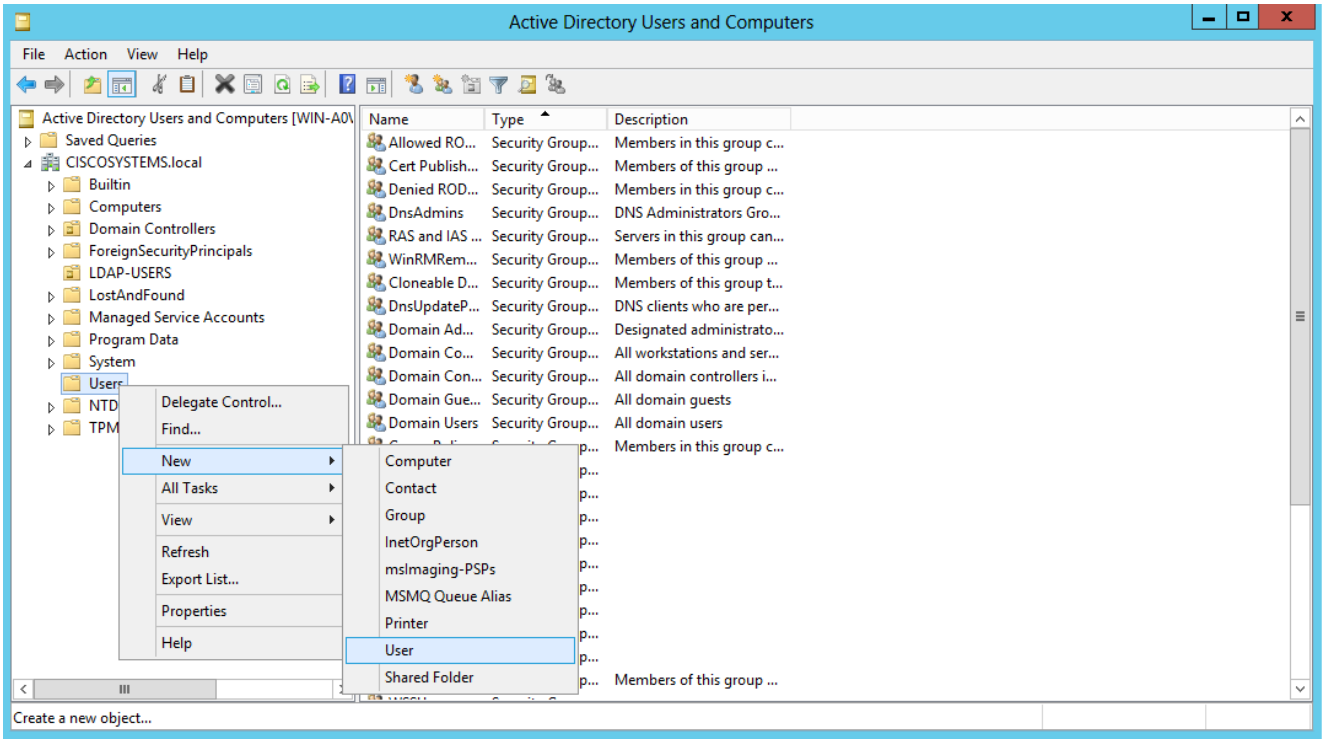
Liaison authentifiée

Suivez les étapes de cette section afin de configurer un utilisateur pour l'authentification locale au serveur LDAP.

1. Ouvrez Windows PowerShell et tapez **servermanager.exe**

2. Dans la fenêtre Gestionnaire de serveur, cliquez sur **AD DS.** Cliquez ensuite avec le bouton droit sur le nom de votre serveur pour choisir **Utilisateurs et ordinateurs Active Directory.**

3. Cliquez avec le bouton droit sur **Utilisateurs**. Accédez à **New > User** à partir des menus contextuels résultants afin de créer un nouvel utilisateur.



4. Dans la page User setup, renseignez les champs obligatoires comme indiqué dans cet exemple. Cet exemple a **WLC-admin** dans le champ **User logon name**. Il s'agit du nom d'utilisateur à utiliser pour l'authentification locale au serveur LDAP. Cliquez sur **Next** (Suivant).

5. Entrez un mot de passe et confirmez-le. Sélectionnez l'option **Password never expires** et cliquez sur **Next**.

6. Cliquez sur **Finish** (Terminer).Un nouvel utilisateur WLC-admin est créé sous le conteneur **Users**. Voici les informations d'identification de l'utilisateur :nom d'utilisateur : **WLC-admin**password : **Admin123**

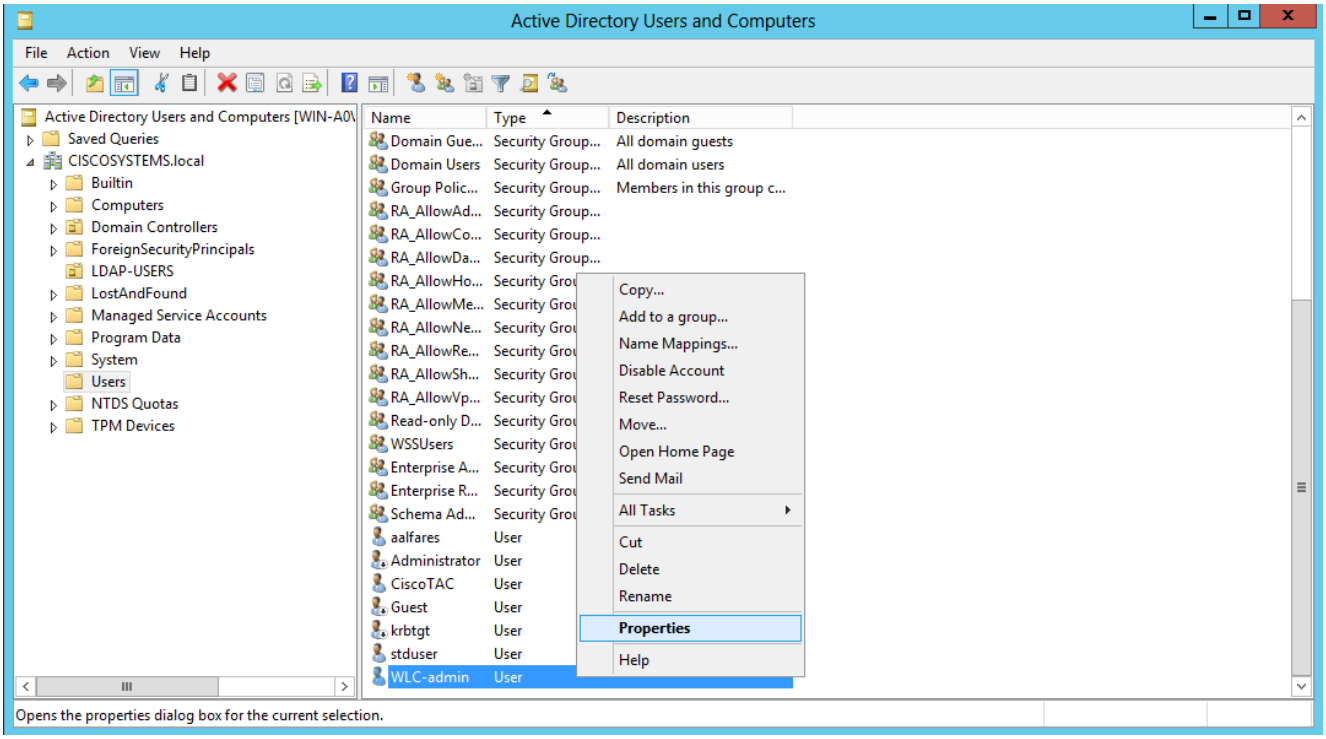
Octroi de privilèges d'administrateur à WLC-admin

Maintenant que l'utilisateur d'authentification locale est créé, nous devons lui accorder des privilèges d'administrateur. Complétez ces étapes afin d'atteindre ceci :

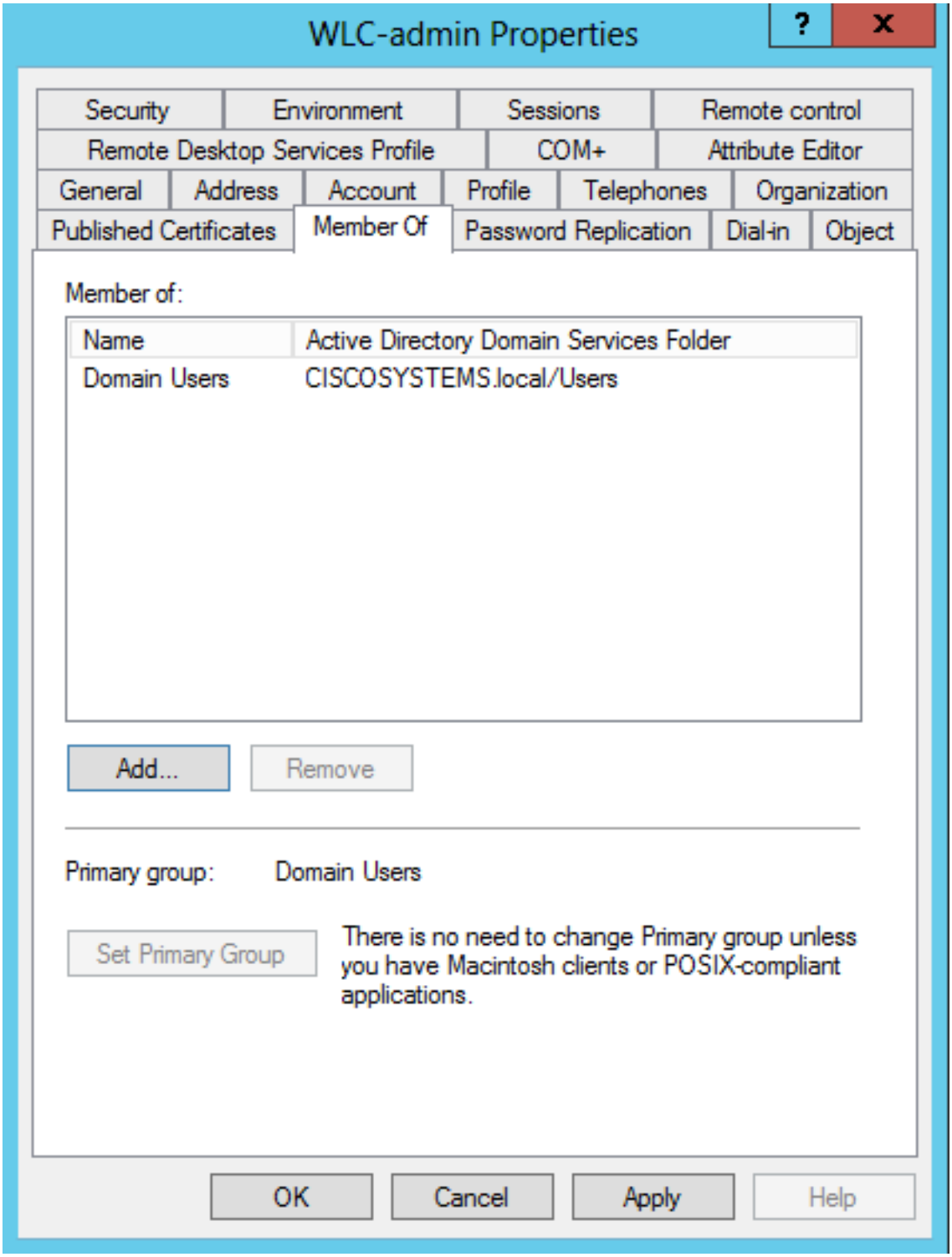
1. Ouvrez **Utilisateurs et ordinateurs Active Directory**.

2. Assurez-vous que la case **Afficher les fonctionnalités avancées** est cochée.

3. Accédez à l'utilisateur **WLC-admin** et cliquez dessus avec le bouton droit. Choisissez **Properties** dans le menu contextuel, comme illustré dans l'image. Cet utilisateur est identifié par le prénom WLC-admin.

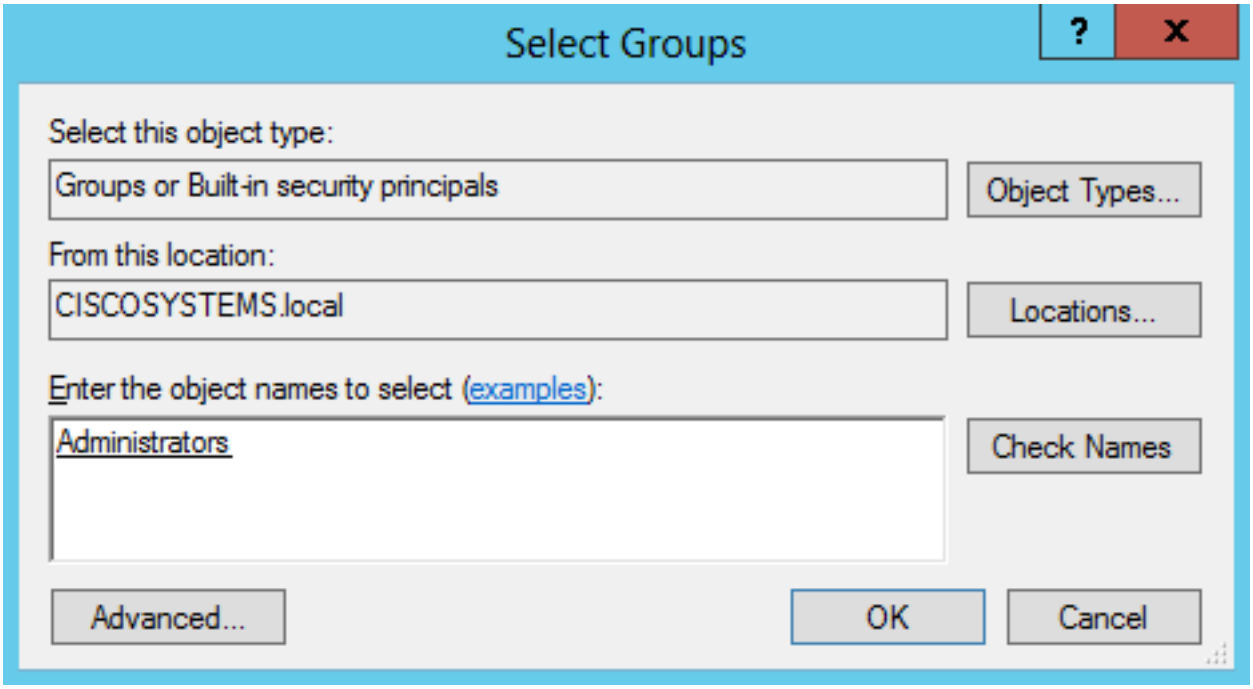


4. Cliquez sur l'onglet **Member Of**, comme indiqué dans l'image :



::

5. Cliquez sur **Add**. Dans la boîte de dialogue qui s'ouvre, entrez **Administrators** et cliquez sur **OK**, Comme le montre l'image :



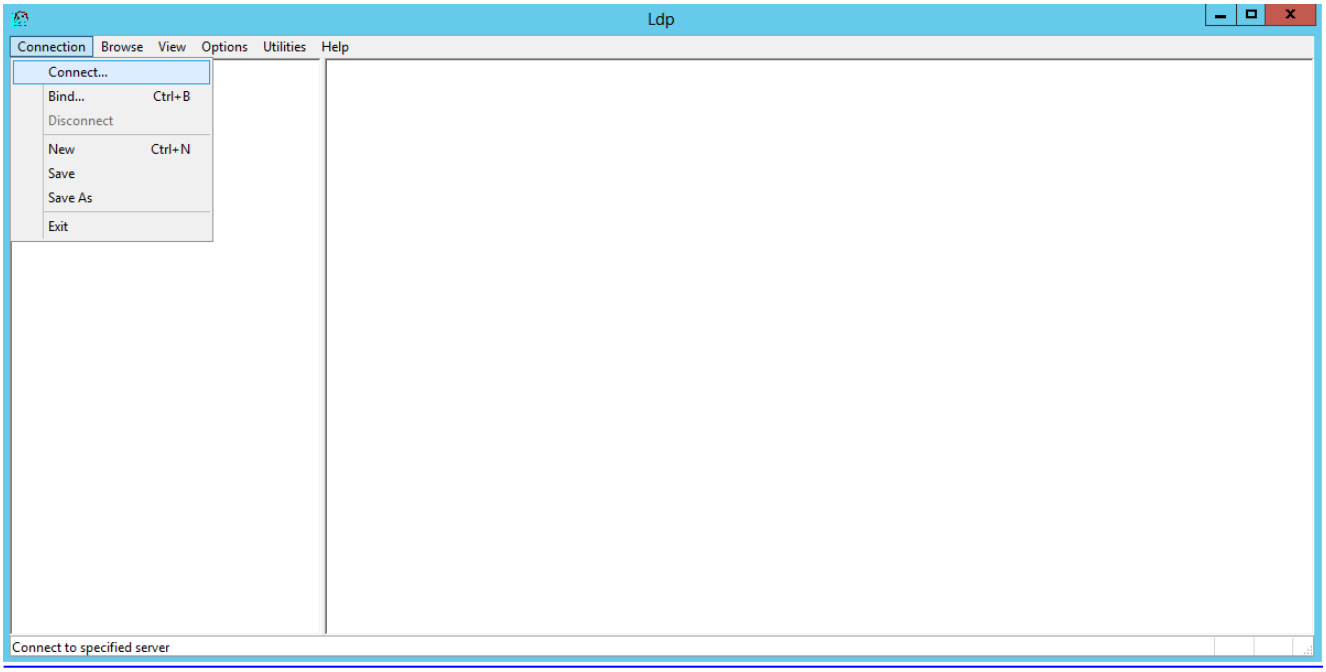
Utiliser le protocole LDP pour identifier les attributs utilisateur

Cet outil GUI est un client LDAP qui permet aux utilisateurs d'effectuer des opérations, telles que la connexion, la liaison, la recherche, la modification, l'ajout ou la suppression, sur n'importe quel répertoire compatible LDAP, tel qu'Active Directory. Le protocole LDP permet d'afficher les objets stockés dans Active Directory, ainsi que leurs métadonnées, telles que les descripteurs de sécurité et les métadonnées de réplication.

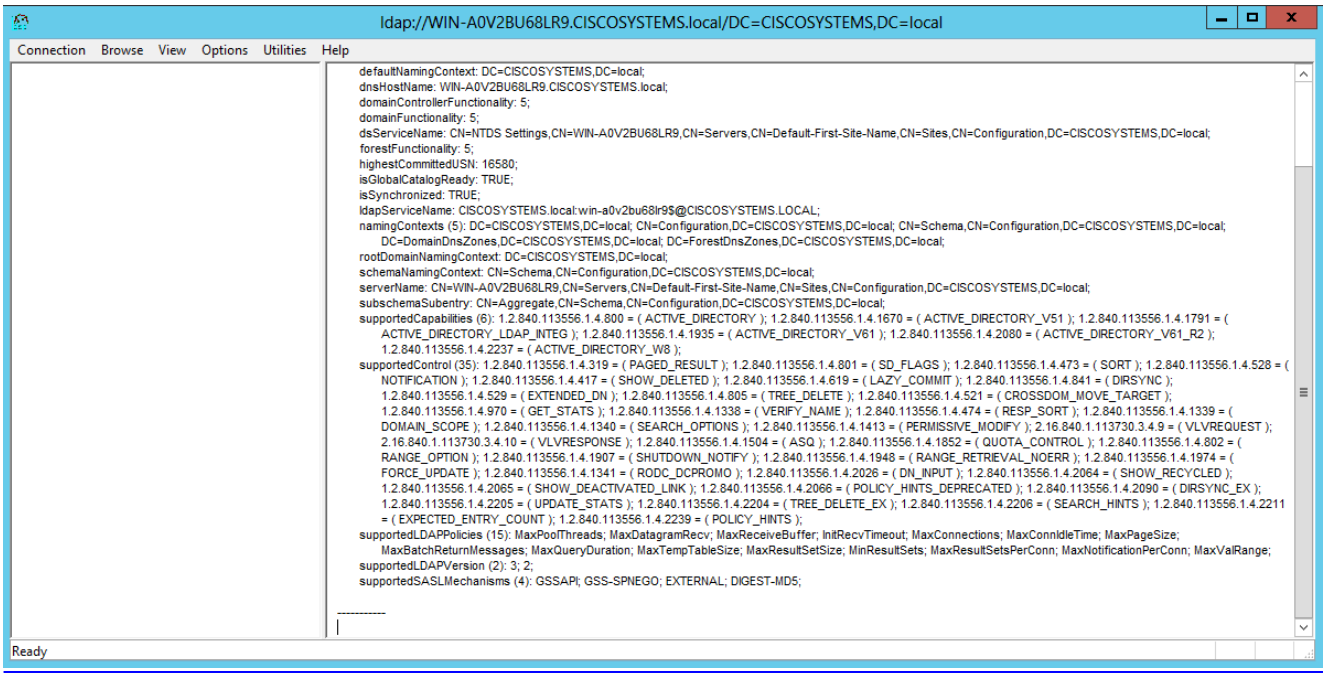
L'outil LDP GUI est inclus lorsque vous installez les outils de support de Windows Server 2003 à partir du CD du produit. Cette section explique comment utiliser l'utilitaire LDP pour identifier les attributs spécifiques associés à l'utilisateur User1. Certains de ces attributs sont utilisés pour remplir les paramètres de configuration du serveur LDAP sur le WLC, tels que le type d'attribut d'utilisateur et le type d'objet d'utilisateur.

1. Sur le serveur Windows 2012 (même sur le même serveur LDAP), ouvrez Windows PowerShell et entrez **LDP** afin d'accéder au navigateur LDP.

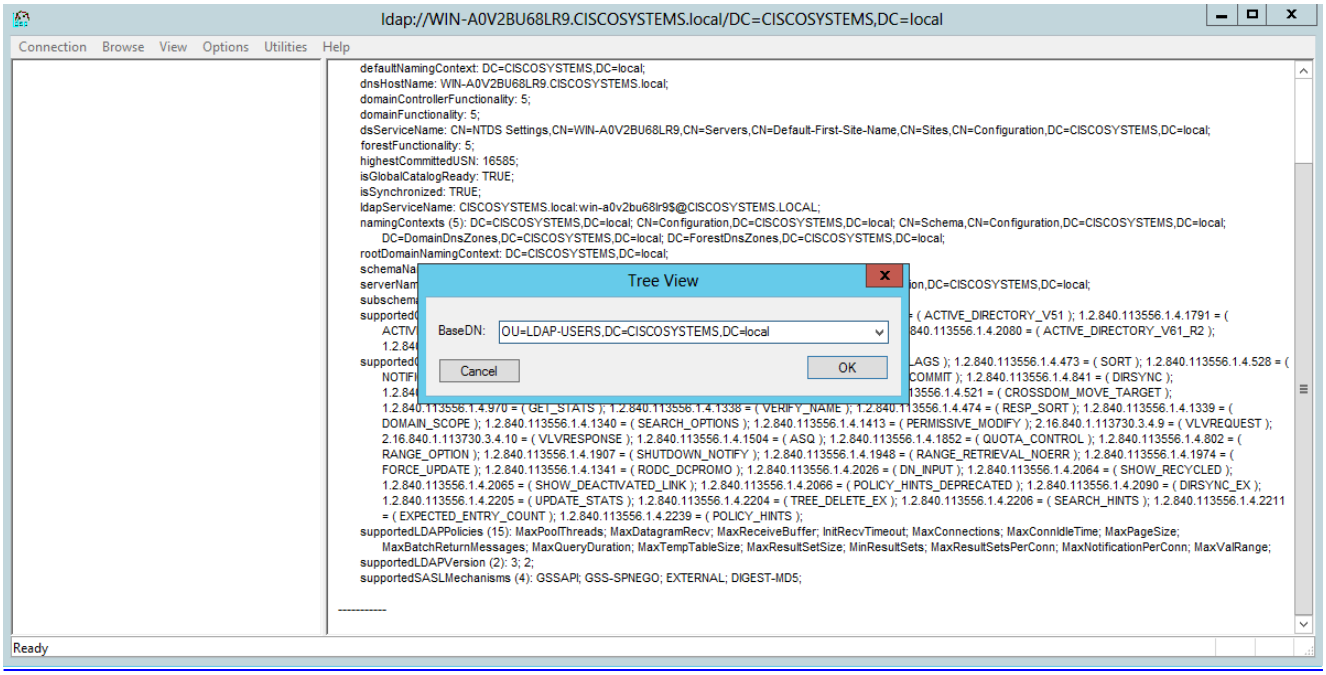
2. Dans la fenêtre principale de LDP, accédez à **Connection > Connect** et connectez-vous au serveur LDAP lorsque vous entrez l'adresse IP du serveur LDAP, comme indiqué dans l'image.



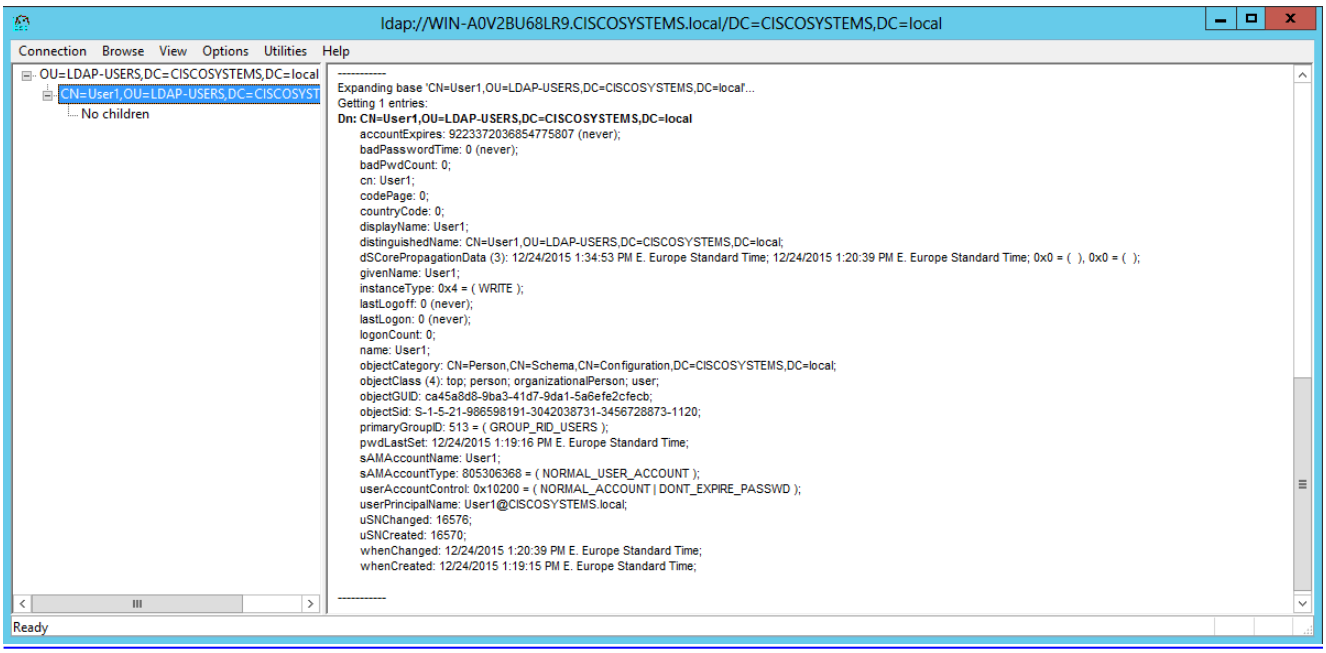
3. Une fois connecté au serveur LDAP, choisissez **View** dans le menu principal et cliquez sur **Tree**, comme indiqué dans l'image :



4. Dans la fenêtre Arborescence résultante, entrez le **BaseDN** de l'utilisateur. Dans cet exemple, User1 se trouve sous l'unité d'organisation « LDAP-USERS » sous le domaine CISCOSYSTEMS.local. Cliquez sur **OK**, comme illustré dans l'image :



5. Le côté gauche du navigateur LDP affiche l'arborescence complète qui apparaît sous le nom de domaine de base spécifié (OU=LDAP-USERS, dc=CISCOSYSTEMS, dc=local). Développez l'arborescence pour localiser l'utilisateur User1. Cet utilisateur peut être identifié par la valeur CN qui représente le prénom de l'utilisateur. Dans cet exemple, il s'agit de CN=User1. Double-cliquez sur **CN=User1**. Dans le volet de droite du navigateur LDP, LDP affiche tous les attributs associés à User1, comme illustré dans l'image :



6. Lorsque vous configurez le WLC pour le serveur LDAP, dans le champ *Attribut d'utilisateur*, entrez le nom de l'attribut dans l'enregistrement d'utilisateur qui contient le nom d'utilisateur. À partir de cette sortie LDP, vous pouvez voir que sAMAccountName est un attribut qui contient le nom d'utilisateur « User1 », donc entrez l'attribut sAMAccountName qui correspond au champ User Attribute sur le WLC.

7. Lorsque vous configurez le WLC pour le serveur LDAP, dans le champ *User Object Type*, entrez la valeur de l'attribut objectType LDAP qui identifie l'enregistrement en tant qu'utilisateur. Souvent, les enregistrements utilisateur ont plusieurs valeurs pour l'attribut objectType, certains étant propres à l'utilisateur et certains étant partagés avec d'autres

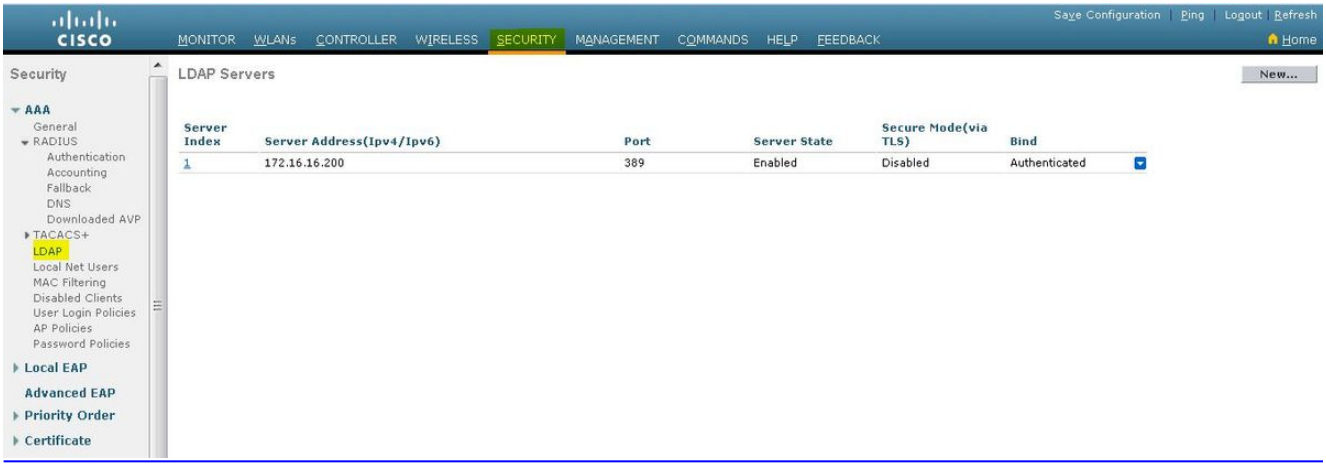
types d'objet. Dans la sortie LDP, CN=Person est une valeur qui identifie l'enregistrement comme un utilisateur, donc spécifiez **Person** comme attribut Type d'objet utilisateur sur le WLC.L'étape suivante consiste à configurer le WLC pour le serveur LDAP.

Configurer le WLC pour le serveur LDAP

Maintenant que le serveur LDAP est configuré, l'étape suivante consiste à configurer le WLC avec les détails du serveur LDAP. Complétez ces étapes sur la GUI du WLC :

> **Remarque** : ce document suppose que le WLC est configuré pour un fonctionnement de base et que les LAP sont enregistrés auprès du WLC. Si vous êtes un nouvel utilisateur qui veut configurer le WLC pour le fonctionnement de base avec les LAP, référez-vous à Enregistrement de LAP (Lightweight AP) à un contrôleur LAN sans fil (WLC).

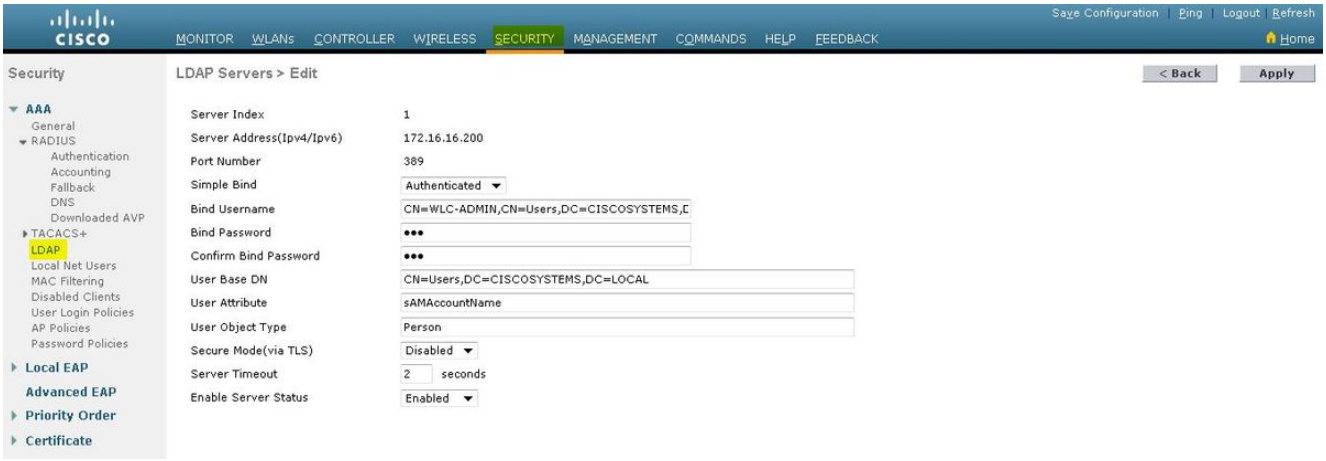
1. Dans la page Security du WLC, choisissez **AAA > LDAP** dans le volet de tâches de gauche afin de passer à la page de configuration du serveur LDAP.



Afin d'ajouter un serveur LDAP, cliquez sur **New**. La page LDAP Servers > New apparaît.

2. Dans la page LDAP Servers Edit, spécifiez les détails du serveur LDAP, tels que l'adresse IP du serveur LDAP, le numéro de port, l'état Enable Server, etc.Choisissez un nombre dans la liste déroulante Index du serveur (Priorité) pour spécifier l'ordre de priorité de ce serveur par rapport à tout autre serveur LDAP configuré. Vous pouvez configurer jusqu'à dix-sept serveurs. Si le contrôleur ne peut pas atteindre le premier serveur, il essaie le second dans la liste, etc.Entrez l'**adresse IP** du serveur LDAP dans le champ Server IP Address.Saisissez le **numéro de port TCP** du serveur LDAP dans le champ Port Number. La plage valide s'étend de 1 à 65535, et la valeur par défaut est 389.pour la liaison simple, nous avons utilisé Authenticated, pour le nom d'utilisateur bind qui est l'emplacement de l'utilisateur admin du WLC qui sera utilisé pour accéder au serveur LDAP et à son mot de passeDans le champ User Base DN, entrez le nom distinctif (DN) du sous-arbre dans le serveur LDAP qui contient une liste de tous les utilisateurs. Par exemple, ou=unité organisationnelle, .ou=unité organisationnelle suivante et o=corporation.com. Si l'arborescence qui contient les utilisateurs est le DN de base, entrez o=corporation.com ou dc=corporation, dc=com.Dans cet exemple, l'utilisateur se trouve sous l'unité d'organisation (OU) LDAP-USERS, qui, à son tour, est créé dans le cadre du domaine lab.wireless.Le DN de base d'utilisateur doit pointer vers le chemin complet où se trouvent les informations d'utilisateur (informations d'identification d'utilisateur selon la méthode d'authentification EAP-FAST). Dans cet exemple, l'utilisateur se trouve sous le DN de base OU=LDAP-USERS,

DC=CISCOSYSTEMS, DC=local.Dans le champ User Attribute, entrez le nom de l'attribut dans l'enregistrement utilisateur contenant le nom d'utilisateur.Dans le champ User Object Type, entrez la valeur de l'attribut LDAP objectType qui identifie l'enregistrement comme utilisateur. Souvent, les enregistrements utilisateur ont plusieurs valeurs pour l'attribut objectType, certains étant propres à l'utilisateur et certains étant partagés avec d'autres types d'objetVous pouvez obtenir la valeur de ces deux champs à partir de votre serveur d'annuaire à l'aide de l'utilitaire de navigateur LDAP fourni avec les outils de support de Windows 2012. Cet outil de navigateur LDAP Microsoft est appelé LDP. À l'aide de cet outil, vous pouvez connaître les champs DN de base utilisateur, Attribut utilisateur et Type d'objet utilisateur de cet utilisateur particulier. Des informations détaillées sur la façon d'utiliser le protocole LDP pour connaître ces attributs spécifiques à l'utilisateur sont présentées dans la section *Utilisation du protocole LDP pour identifier les attributs* de l'*utilisateur* de ce document.Dans le champ Server Timeout, saisissez le nombre de secondes entre les retransmissions. La plage valide s'étend de 2 à 30 secondes, et la valeur par défaut est de 2 secondes.Cochez la case **Enable Server Status pour activer ce serveur LDAP ou décochez-la pour le désactiver.** Par défaut, cette option est désactivée.Cliquez sur Apply pour valider les modifications. Voici un exemple déjà configuré avec ces informations
:

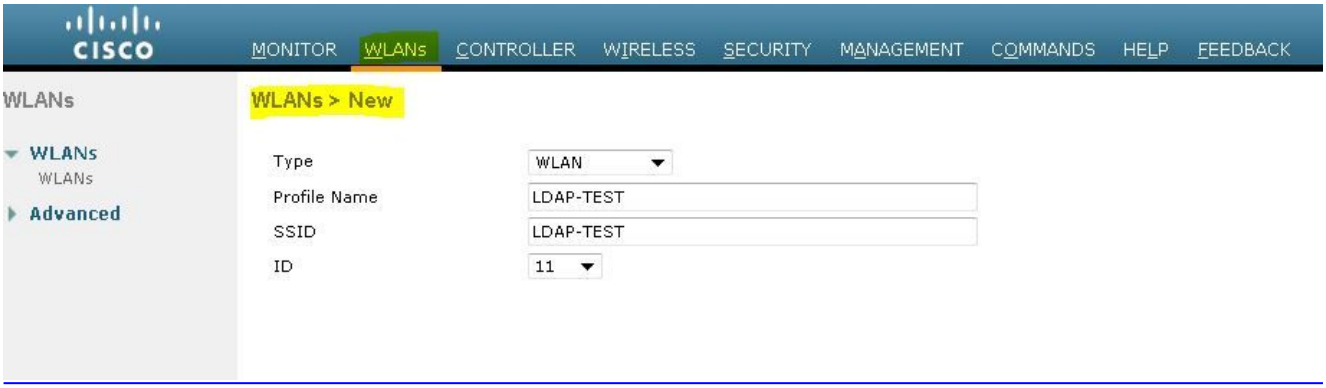


3. Maintenant que les détails sur le serveur LDAP sont configurés sur le WLC, l'étape suivante consiste à configurer un WLAN pour l'authentification Web.

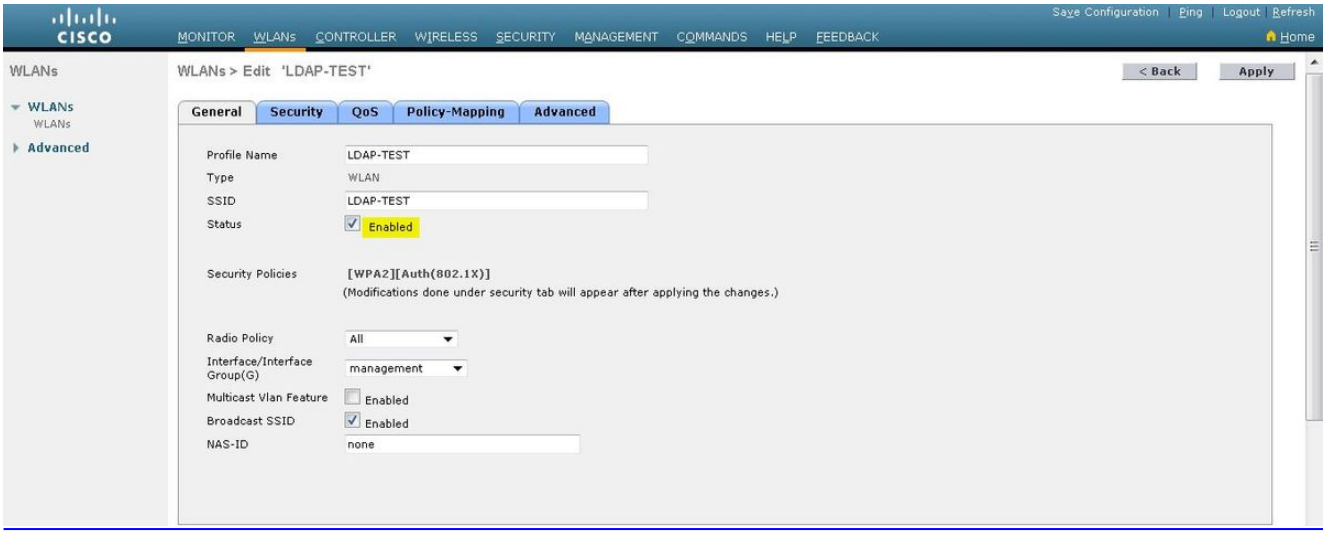
Configurer le WLAN pour l'authentification Web

La première étape consiste à créer un réseau local sans fil pour les utilisateurs. Procédez comme suit :

1. Cliquez sur **WLANs depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.**La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New pour configurer un nouveau WLAN.**Dans cet exemple, le WLAN est nommé Web-
Auth.



3. Cliquez sur **Apply**.
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.



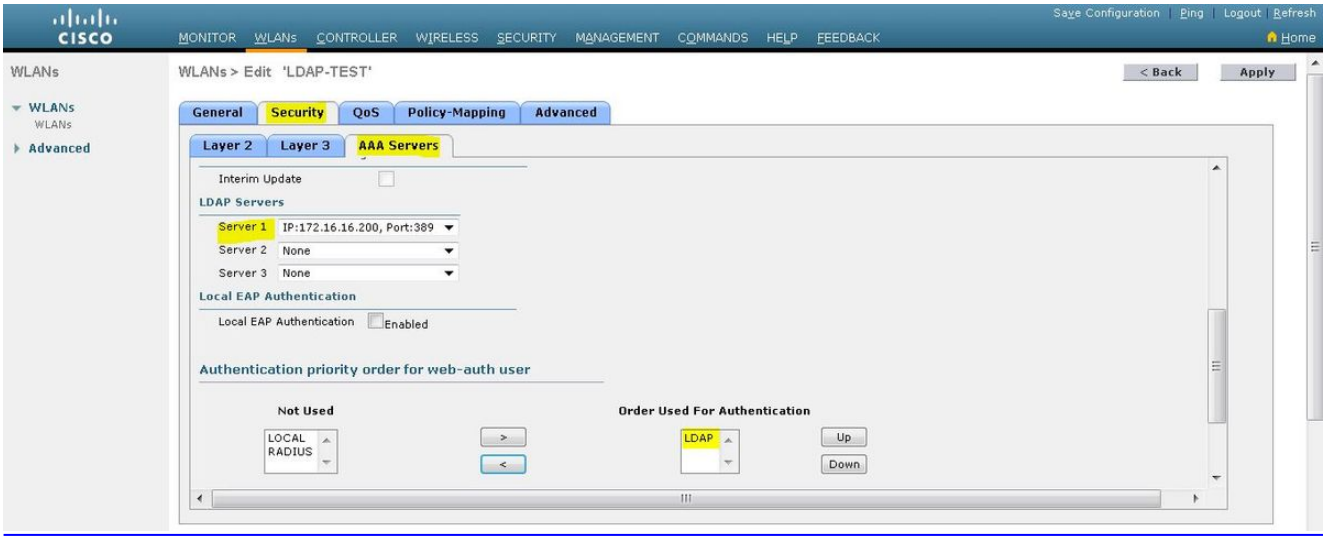
Cochez la case Status pour activer le WLAN.Pour le réseau WLAN, choisissez l'interface appropriée dans le champ Interface Name [nom de l'interface].Cet exemple montre comment mapper l'interface de gestion qui se connecte au WLAN Web-Auth.

5. Cliquez sur l'onglet **Security.** Dans le champ Layer 3 Security, cochez la case **Web Policy** et choisissez l'option **Authentication**.

Cette option est sélectionnée car l'authentification Web est utilisée pour authentifier les clients sans fil. Cochez la case **Override Global Config** pour activer la configuration de l'authentification Web WLAN. Sélectionnez le type d'authentification Web approprié dans le menu déroulant Type d'authentification Web. Cet exemple utilise l'authentification Web interne.**Remarque** : l'authentification Web n'est pas prise en charge avec l'authentification

802.1x. Cela signifie que vous ne pouvez pas choisir 802.1x ou un WPA/WPA2 avec 802.1x comme sécurité de couche 2 lorsque vous utilisez l'authentification Web. L'authentification Web est prise en charge avec tous les autres paramètres de sécurité de couche 2.

6. Cliquez sur l'onglet **AAA Servers**. Sélectionnez le serveur LDAP configuré dans le menu déroulant Serveur LDAP. Si vous utilisez une base de données locale ou un serveur RADIUS, vous pouvez définir la priorité d'authentification sous le champ *Ordre de priorité d'authentification pour l'*utilisateur *Web-auth*.



7. Cliquez sur **Apply**.**Remarque** : dans cet exemple, les méthodes de sécurité de couche 2 pour authentifier les utilisateurs ne sont pas utilisées. Par conséquent, sélectionnez **None** dans le champ Layer 2 Security.

Vérifier

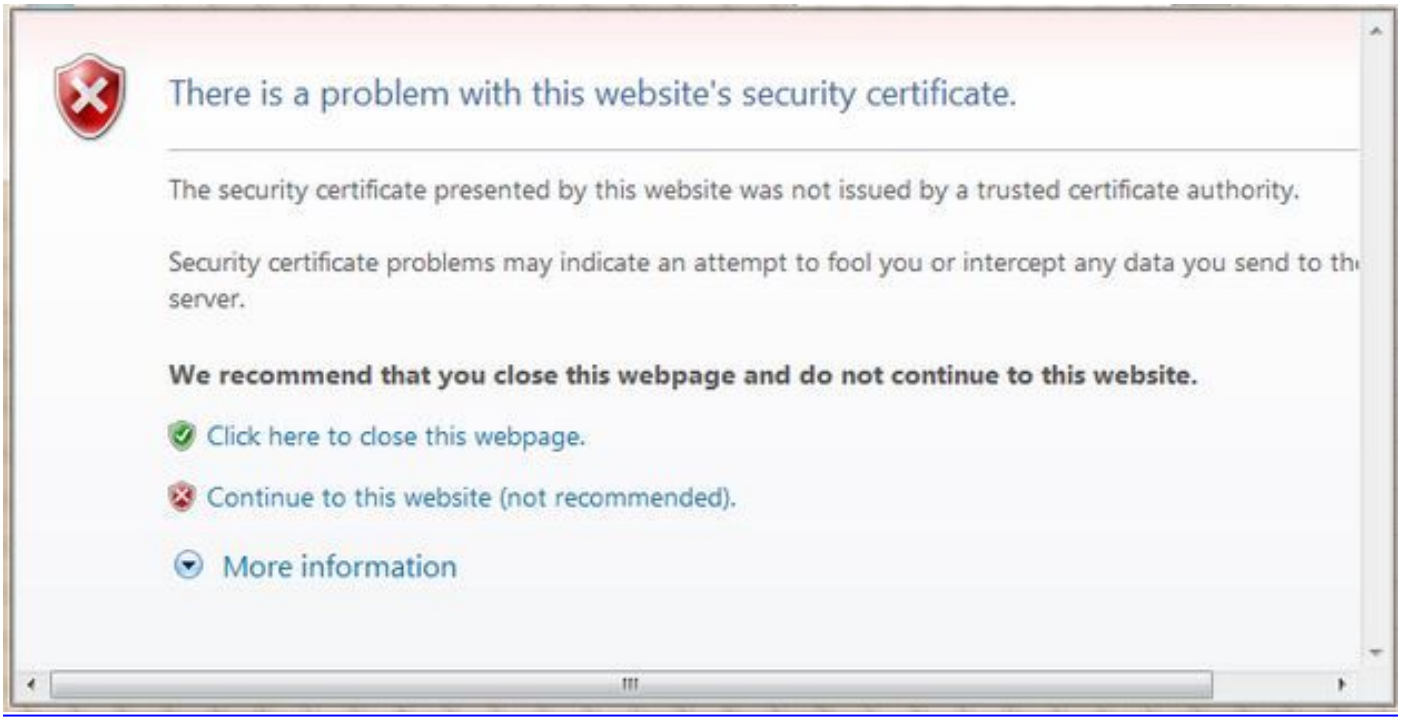
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

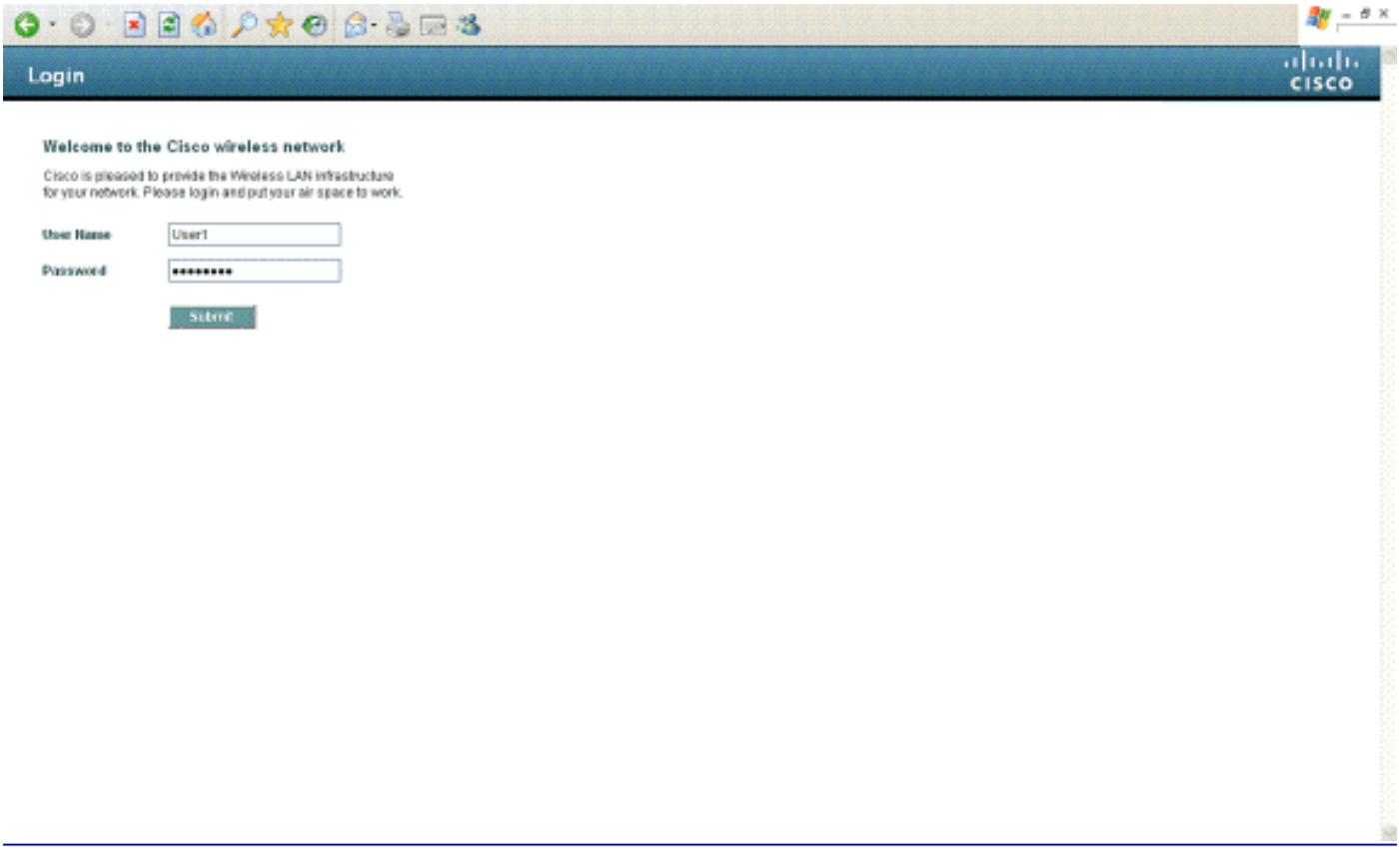
Afin de vérifier cette configuration, connectez un client sans fil et vérifiez si la configuration fonctionne comme prévu.

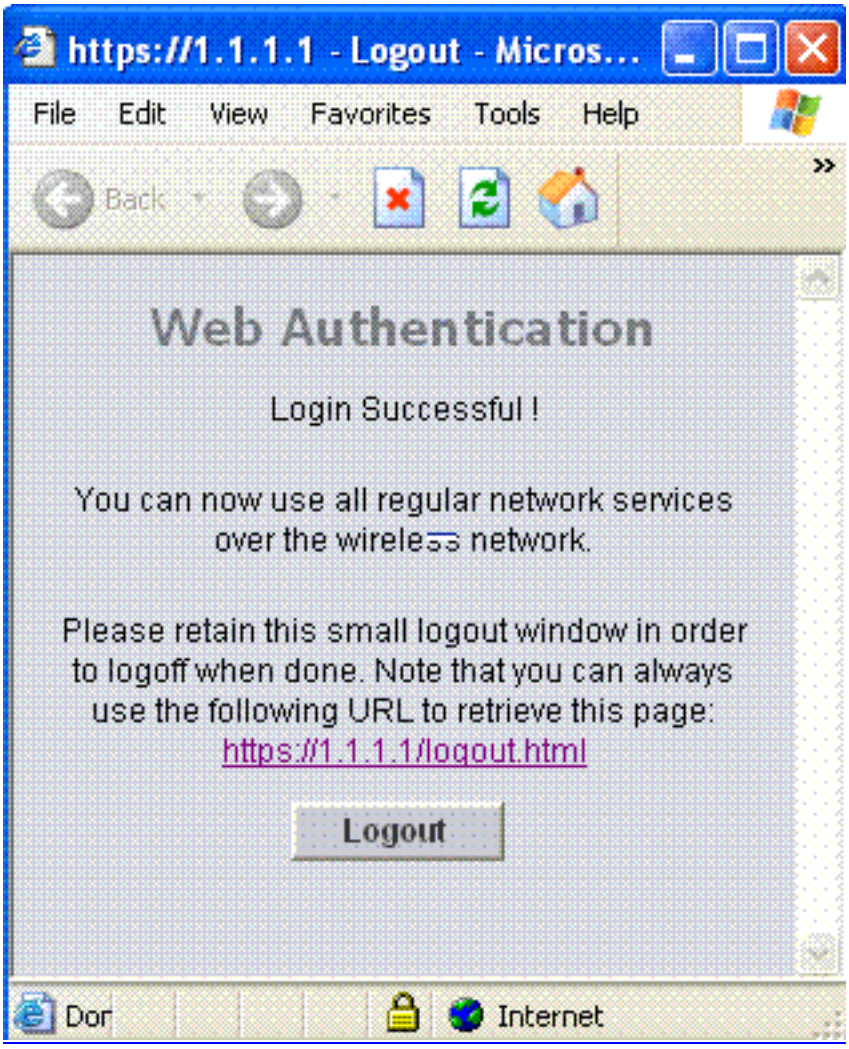
Le client sans fil s'affiche et l'utilisateur saisit l'URL, par exemple www.yahoo.com, dans le navigateur Web. Comme l'utilisateur n'a pas été authentifié, le WLC redirige l'utilisateur vers l'URL de connexion Web interne.

L'utilisateur est invité à saisir ses informations d'identification. Une fois que l'utilisateur envoie le nom d'utilisateur et le mot de passe, la page de connexion prend l'entrée d'informations d'identification de l'utilisateur et, lors de l'envoi, renvoie la demande à l'exemple action_URL, http://1.1.1.1/login.html, du serveur Web WLC. Il s'agit d'un paramètre d'entrée pour l'URL de redirection du client, où 1.1.1.1 est l'adresse d'interface virtuelle sur le commutateur.

Le WLC authentifie l'utilisateur par rapport à la base de données d'utilisateurs LDAP. Une fois l'authentification réussie, le serveur Web du WLC transfère l'utilisateur à l'URL de redirection configurée ou à l'URL avec laquelle le client a démarré, telle que www.yahoo.com.


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to th
server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information


Login
cisco
Welcome to the Cisco wireless network
Cisco is pleased to provide the Wireless LAN infrastructure
for your network. Please login and put your air space to work.
User Name
User1
Password
Submit



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Utilisez ces commandes pour dépanner votre configuration :

- **debug mac addr** <adresse-MAC-client xx:xx:xx:xx:xx:xx>
- **debug aaa all enable**
- **debug pem state enable**
- **debug pem events enable**
- **debug dhcp message enable**
- **debug dhcp packet enable**

Voici un exemple de sortie des commandes **debug mac addr cc:fa:00:f7:32:35**

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on
BSSID 00:23:eb:e5:04:1f AP AP1142-1
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP
```

```
radio

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0  cur: 1

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to
AP wlan

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking
intgrp NULL
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile,
role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2699)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2720)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy
over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central
switched to TRUE
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and
Split Acl Id = 65535
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging
override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface
Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  statusCode is 0 and
status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  ssid_done_flag is 0
finish_flag is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0
0 0 0 0 0 0 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates  statusCode is 0 and
gotSuppRatesElement is 1
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP
00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to START (0) last state WEBAUTH_REQD (8)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2:
APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing
policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to
AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name:
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change
state to WEBAUTH_REQD (8) last state L2AUTHCOMPLETE (4)

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3802, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding
Fast Path rule
 type = Airespace AP Client - ACL passthru
```

```
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3911, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout
forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning
flag is  1
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:
(callerId: 49) in 1800 seconds
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout =
1800, Session Timeout = 1800

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on
BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
```

```
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
322,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                        dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                        dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
334,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
```

```
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   requested ip: 172.16.16.122
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 172.16.16.25  rcvd
server id: 1.1.1.1
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK
(mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for
mobile, length = 7
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb
for mobile, length = 7
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c


*aaaQueueReader: Dec 24 03:46:01.222:   Callback.....................................0x12088c50

*aaaQueueReader: Dec 24 03:46:01.222:   protocolType.................................0x00000002

*aaaQueueReader: Dec 24 03:46:01.222:
proxyState.................................CC:FA:00:F7:32:35-00:00

*aaaQueueReader: Dec 24 03:46:01.222:   Packet contains 15 AVPs (not shown)

*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE'
(1)
*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
```

```
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated
lcapi_bind (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED
*LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP_OPT_REFERRALS

*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP_CLIENT: UID Search
(base=CN=Users,DC=CISCOSYSTEMS,DC=local, pattern=(&(objectclass=Person)(sAMAccountName=User1)))
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: ldap_search_ext_s returns 0 -5
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned 2 msgs including 0 references
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 1 type 0x64
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received 1 attributes in search entry msg
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 2 type 0x65
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : No matched DN
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : Check result error 0 rc 1013
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received no referrals in search result msg
*LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi_query
base="CN=Users,DC=CISCOSYSTEMS,DC=local" type="Person" attr="sAMAccountName" user="User1" (rc =
0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username
CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
(size 45)
*LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success
*LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc
*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14)
Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station:
(callerId: 74)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec -
starting session timer for the mobile
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached
PLUMBFASTPATH: from line 6972
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast
Path rule
 type = Airespace AP Client
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan = 16, Local
Bridging intf id = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
```

```
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0


(Cisco_Controller) >show client detail cc:fa:00:f7:32:35
Client MAC Address.............................. cc:fa:00:f7:32:35
Client Username ................................ User1
AP MAC Address.................................. 00:23:eb:e5:04:10
AP Name......................................... AP1142-1
AP radio slot Id................................ 1
Client State.................................... Associated
Client User Group............................... User1
Client NAC OOB State............................ Access
Wireless LAN Id................................. 1
Wireless LAN Network Name (SSID)................ LDAP-TEST
Wireless LAN Profile Name....................... LDAP-TEST
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:23:eb:e5:04:1f
Connected For .................................. 37 secs
Channel......................................... 36
IP Address...................................... 172.16.16.122
Gateway Address................................. 172.16.16.1
Netmask......................................... 255.255.254.0
Association Id.................................. 2
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0

--More or (q)uit current module or <ctrl-z> to abort
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
QoS Level....................................... Silver
Avg data Rate................................... 0
Burst data Rate................................. 0
Avg Real time data Rate......................... 0
Burst Real Time data Rate....................... 0
802.1P Priority Tag............................. disabled
CTS Security Group Tag.......................... Not Applicable
KTS CAC Capability.............................. No
Qos Map Capability.............................. No
WMM Support..................................... Enabled
 APSD ACs.....................................  BK  BE  VI  VO
Current Rate.................................... m7
Supported Rates................................. 12.0,18.0,24.0
Mobility State.................................. Local
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Audit Session ID................................ ac10101900000005567b69f8
AAA Role Type................................... none
Local Policy Applied............................ none
IPv4 ACL Name................................... none

--More or (q)uit current module or <ctrl-z> to abort
FlexConnect ACL Applied Status.................. Unavailable
IPv4 ACL Applied Status......................... Unavailable
IPv6 ACL Name................................... none
IPv6 ACL Applied Status......................... Unavailable
Layer2 ACL Name................................. none
Layer2 ACL Applied Status....................... Unavailable
Client Type..................................... SimpleIP
mDNS Status..................................... Enabled
mDNS Profile Name............................... default-mdns-profile
No. of mDNS Services Advertised................. 0
```

```
Policy Type..................................... N/A
Encryption Cipher............................... None
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type........................................ Unknown
FlexConnect Data Switching...................... Central
FlexConnect Dhcp Status......................... Central
FlexConnect Vlan Based Central Switching........ No
FlexConnect Authentication...................... Central
FlexConnect Central Association................. No
Interface....................................... management
VLAN............................................ 16
Quarantine VLAN................................. 0

--More or (q)uit current module or <ctrl-z> to abort
Access VLAN..................................... 16
Local Bridging VLAN............................. 16
Client Capabilities:
     CF Pollable................................ Not implemented
     CF Poll Request............................ Not implemented
     Short Preamble............................. Not implemented
     PBCC....................................... Not implemented
     Channel Agility............................ Not implemented
     Listen Interval............................ 10
     Fast BSS Transition........................ Not implemented
     11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
     WFD capable................................ No
     Manged WFD capable......................... No
     Cross Connection Capable................... No
     Support Concurrent Operation............... No
Fast BSS Transition Details:
Client Statistics:
     Number of Bytes Received................... 16853
     Number of Bytes Sent....................... 31839
     Total Number of Bytes Sent................. 31839
     Total Number of Bytes Recv................. 16853
     Number of Bytes Sent (last 90s)............ 31839

--More or (q)uit current module or <ctrl-z> to abort
     Number of Bytes Recv (last 90s)............ 16853
     Number of Packets Received................. 146
     Number of Packets Sent..................... 92
     Number of Interim-Update Sent.............. 0
     Number of EAP Id Request Msg Timeouts...... 0
     Number of EAP Id Request Msg Failures...... 0
     Number of EAP Request Msg Timeouts......... 0
     Number of EAP Request Msg Failures......... 0
     Number of EAP Key Msg Timeouts............. 0
     Number of EAP Key Msg Failures............. 0
     Number of Data Retries..................... 2
     Number of RTS Retries...................... 0
     Number of Duplicate Received Packets....... 0
     Number of Decrypt Failed Packets........... 0
     Number of Mic Failured Packets............. 0
     Number of Mic Missing Packets.............. 0
     Number of RA Packets Dropped............... 0
     Number of Policy Errors.................... 0
     Radio Signal Strength Indicator............ -48 dBm
     Signal to Noise Ratio...................... 41 dB
Client Rate Limiting Statistics:
     Number of Data Packets Received............ 0
     Number of Data Rx Packets Dropped.......... 0
```

```
--More or (q)uit current module or <ctrl-z> to abort
     Number of Data Bytes Received.............. 0
     Number of Data Rx Bytes Dropped............ 0
     Number of Realtime Packets Received........ 0
     Number of Realtime Rx Packets Dropped...... 0
     Number of Realtime Bytes Received.......... 0
     Number of Realtime Rx Bytes Dropped........ 0
     Number of Data Packets Sent................ 0
     Number of Data Tx Packets Dropped.......... 0
     Number of Data Bytes Sent.................. 0
     Number of Data Tx Bytes Dropped............ 0
     Number of Realtime Packets Sent............ 0
     Number of Realtime Tx Packets Dropped...... 0
     Number of Realtime Bytes Sent.............. 0
     Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
     AP1142-1(slot 0)
       antenna0: 25 secs ago..................... -37 dBm
       antenna1: 25 secs ago..................... -37 dBm
     AP1142-1(slot 1)
       antenna0: 25 secs ago..................... -44 dBm
       antenna1: 25 secs ago..................... -57 dBm
DNS Server details:
     DNS server IP ............................. 0.0.0.0

--More or (q)uit current module or <ctrl-z> to abort
     DNS server IP ............................. 0.0.0.0
Assisted Roaming Prediction List details:


Client Dhcp Required:     False
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.