

ASA 8.0 : Configurer l'authentification LDAP pour les utilisateurs WebVPN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Informations générales](#)

[Configurez l'authentification LDAP](#)

[ASDM](#)

[Interface de ligne de commande](#)

[Exécutez les recherches de Multi-domaine \(facultatifs\)](#)

[Vérifiez](#)

[Test avec l'ASDM](#)

[Test avec le CLI](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique comment configurer le dispositif de sécurité adaptatif Cisco (ASA) pour utiliser un serveur LDAP pour l'authentification des utilisateurs WebVPN. Le serveur LDAP dans cet exemple est Microsoft Active Directory. Cette configuration est exécutée avec Adaptive Security Device Manager (ASDM) 6.0(2) sur une ASA qui exécute la version de logiciel 8.0(2).

Remarque: Dans ce Protocole LDAP (Lightweight Directory Access Protocol) d'exemple l'authentification est configurée pour des utilisateurs WebVPN, mais cette configuration peut être aussi bien utilisée pour tous autres types de clients d'Accès à distance. Affectez simplement le Groupe de serveurs AAA au profil désiré de connexion (groupe de tunnel), comme affiché.

[Conditions préalables](#)

Une configuration du VPN de base est exigée. Dans cet exemple le webvpn est utilisé.

[Informations générales](#)

Dans cet exemple, l'ASA vérifie avec un serveur LDAP afin de vérifier l'identité des utilisateurs qu'elle authentifie. Ce processus ne fonctionne pas comme un échange traditionnel de Service RADIUS (Remote Authentication Dial-In User Service) ou de Terminal Access Controller Access Control System Plus (TACACS+). Ces étapes expliquent, à un haut niveau, comment l'ASA utilise un serveur LDAP afin de vérifier des identifiants utilisateurs.

1. L'utilisateur initie une connexion à l'ASA.
2. L'ASA est configurée pour authentifier cet utilisateur avec le serveur de Microsoft Active Directory (AD) /LDAP.
3. L'ASA lie au serveur LDAP avec les qualifications configurées sur l'ASA (admin dans ce cas), et aux consultations le nom d'utilisateur fourni. L'utilisateur d'**admin** obtient également les qualifications appropriées pour répertorier le contenu dans le Répertoire actif. Référez-vous à <http://support.microsoft.com/?id=320528> pour plus d'informations sur la façon d'accorder des privilèges de requête de LDAP. **Remarque:** Le site Web de Microsoft chez <http://support.microsoft.com/?id=320528> est géré par un fournisseur de tiers. [Cisco n'est pas responsable de son contenu.](#)
4. Si le nom d'utilisateur est trouvé, les tentatives ASA de lier au serveur LDAP avec les qualifications que l'utilisateur a fournies à la procédure de connexion.
5. Si le deuxième grippage est réussi, l'authentification réussit et la l'ASA traite les attributs de l'utilisateur. **Remarque:** Dans cet exemple les attributs ne sont pas utilisés pour n'importe quoi. Reportez-vous à la section [ASA/PIX : Traçant des clients vpn aux stratégies de groupe VPN par l'exemple de configuration de LDAP](#) afin de voir un exemple de la façon dont l'ASA peut traiter des attributs de LDAP.

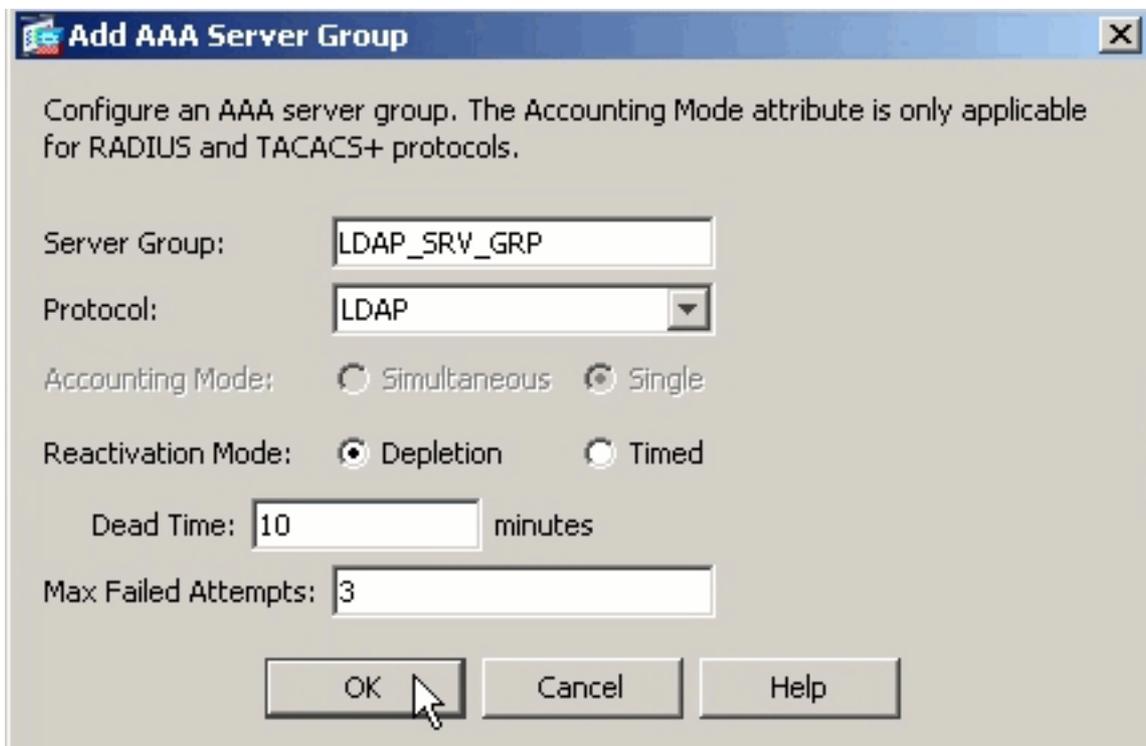
[Configurez l'authentification LDAP](#)

Dans cette section, vous êtes présenté avec les informations pour configurer l'ASA pour utiliser un serveur LDAP pour l'authentification des clients de webvpn.

[ASDM](#)

Terminez-vous ces étapes dans l'ASDM afin de configurer l'ASA pour communiquer avec le serveur LDAP et pour authentifier des clients de webvpn.

1. Naviguez vers la configuration > l'Accès à distance VPN > AAA installé > des Groupes de serveurs AAA.
2. Cliquez sur Add à côté des Groupes de serveurs AAA
3. Spécifiez un nom pour le nouveau Groupe de serveurs AAA, et choisissez le **LDAP** comme



protocole.

4. Soyez sûr que votre nouveau groupe est sélectionné dans le volet supérieur, et cliquez sur Add à côté des **serveurs** dans le volet de **groupe sélectionné**.
5. Fournissez les informations de configuration pour votre serveur LDAP. Le tir d'écran ultérieur illustre un exemple de configuration. C'est une explication de plusieurs des options de configuration :
 - Nom d'interface** — l'interface qui les utilisations ASA afin d'atteindre le serveur LDAP
 - Nom du serveur ou adresse IP** — l'adresse qui les utilisations ASA afin d'atteindre le serveur LDAP
 - Type de serveur** — le type de serveur LDAP, tel que Microsoft
 - DN de base** — l'emplacement dans la hiérarchie de LDAP où le serveur doit commencer au
 - rechercher
 - Portée** — l'ampleur de la recherche dans la hiérarchie de LDAP que le serveur doit faire
 - Nommant l'attribut** — l'attribut de nom unique relatif (ou attributs) qu'identifie seulement une entrée sur le serveur LDAP. **le sAMAccountName** est l'attribut par défaut dans la Microsoft Active Directory. D'autres attributs utilisés généralement sont NC, UID, et userPrincipalName.
 - DN de procédure de connexion** — le DN avec assez de privilèges afin d'être de recherche capable/utilisateurs de lire/consultation dans le serveur LDAP
 - Mot de passe de connexion** — le mot de passe pour le compte de DN
 - Carte d'attribut de LDAP** — une carte d'attribut de LDAP à utiliser avec des réponses de ce serveur. Reportez-vous à la section [ASA/PIX : Traçant les clients vpn aux stratégies de groupe VPN par l'exemple de configuration de LDAP](#) pour plus d'informations sur la façon configurer le LDAP attribuent

Server Group: LDAP_SRV_GRP

Interface Name: inside

Server Name or IP Address: 192.168.1.2

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: Microsoft

Base DN: dc=ftwsecurity, dc=cisco, dc=com

Scope: All levels beneath the Base DN

Naming Attribute(s): sAMAccountName

Login DN: cn=admin, cn=users, dc=ftwsecurity, dc=cisco, dc=

Login Password: *****

LDAP Attribute Map: -- None --

SASL MD5 authentication

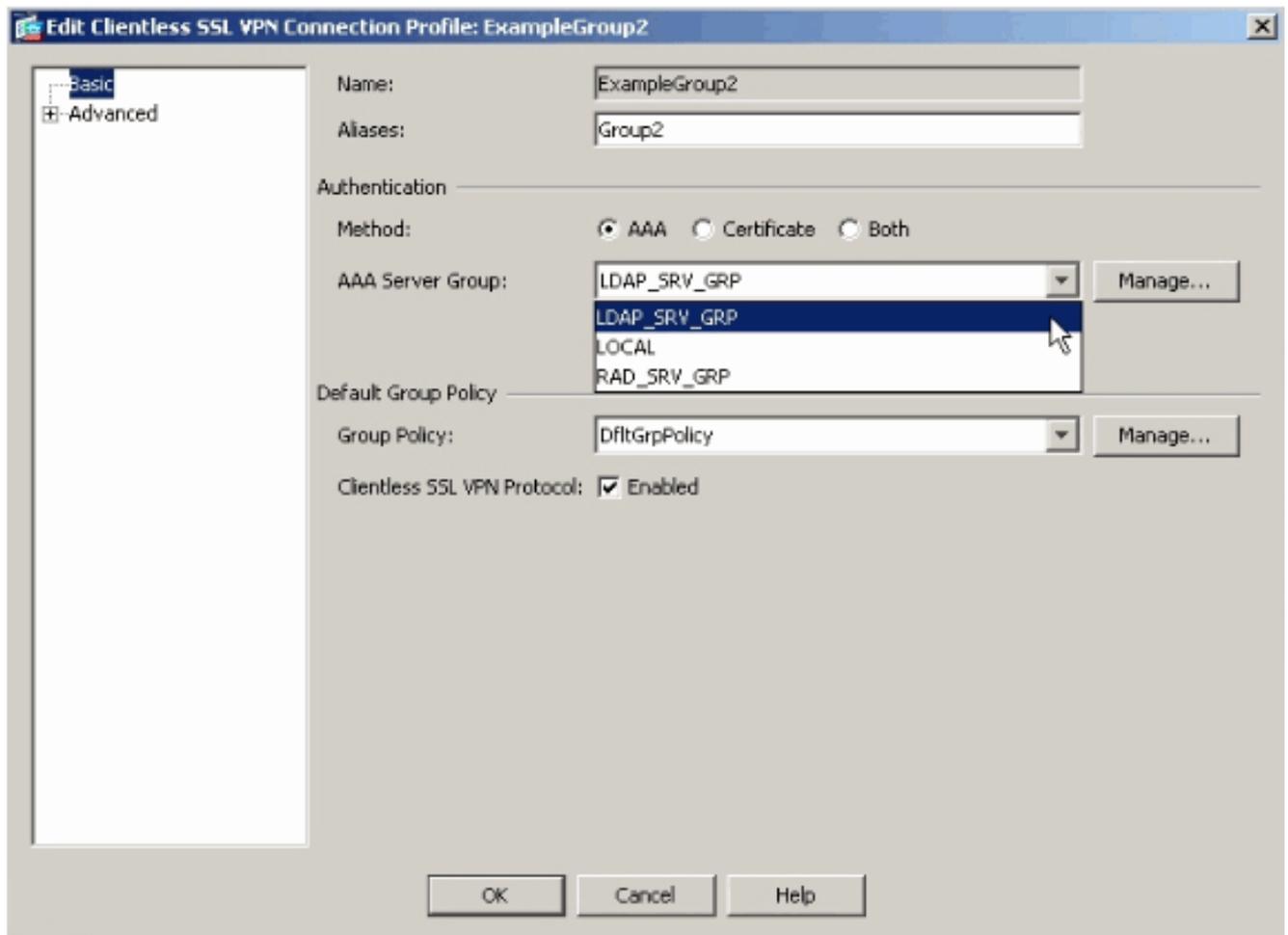
SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

des cartes.

6. Une fois que vous avez configuré le Groupe de serveurs AAA et avez ajouté un serveur à lui, il est nécessaire de configurer votre profil de connexion (groupe de tunnel) pour utiliser la nouvelle configuration d'AAA. Naviguez vers la configuration > l'Accès à distance VPN > VPN SSL sans client Access > profils de connexion.
7. Choisissez le profil de connexion (le groupe de tunnel) pour lequel vous voulez configurer l'AAA, et cliquez sur Edit
8. Sous l'**authentification**, choisissez le groupe de serveur LDAP que vous avez créé plus tôt.



[Interface de ligne de commande](#)

Terminez-vous ces étapes dans l'interface de ligne de commande (CLI) afin de configurer l'ASA pour communiquer avec le serveur LDAP et pour authentifier des clients de webvpn.

```
ciscoasa#configure terminal !--- Configure the AAA Server group. ciscoasa(config)#aaa-server
LDAP_SRV_GRP protocol ldap !--- Configure the AAA Server. ciscoasa(config-aaa-server-group)#aaa-
server LDAP_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-server-host)#ldap-base-dn
dc=ftwsecurity, dc=cisco, dc=com ciscoasa(config-aaa-server-host)#ldap-login-dn cn=admin,
cn=users, dc=ftwsecurity, dc=cisco, dc=com ciscoasa(config-aaa-server-host)#ldap-login-password
***** ciscoasa(config-aaa-server-host)#ldap-naming-attribute sAMAccountName
ciscoasa(config-aaa-server-host)#ldap-scope subtree ciscoasa(config-aaa-server-host)#server-type
microsoft ciscoasa(config-aaa-server-host)#exit !--- Configure the tunnel group to use the new
AAA setup. ciscoasa(config)#tunnel-group ExampleGroup2 general-att ciscoasa(config-tunnel-
general)#authentication-server-group LDAP_SRV_GRP
```

[Exécutez les recherches de Multi-domaine \(facultatives\)](#)

Facultatif. L'ASA actuellement ne prend en charge pas le mécanisme de référence de LDAP pour des recherches de multi-domaine (ID de bogue Cisco CSCsj32153). des recherches de Multi-domaine sont prises en charge avec l'AD en mode de serveur global de catalogue. Afin d'exécuter des recherches de multi-domaine, l'installation vers le haut du serveur d'AD pour le mode de serveur global de catalogue, habituellement avec ceux-ci introduisent des paramètres pour l'entrée de serveur LDAP dans l'ASA. La clé est d'utiliser un LDAP-nom-attribut qui doit être seul à travers l'arborescence des répertoires.

```
server-port 3268
ldap-scope subtree
ldap-naming-attribute userPrincipalName
```

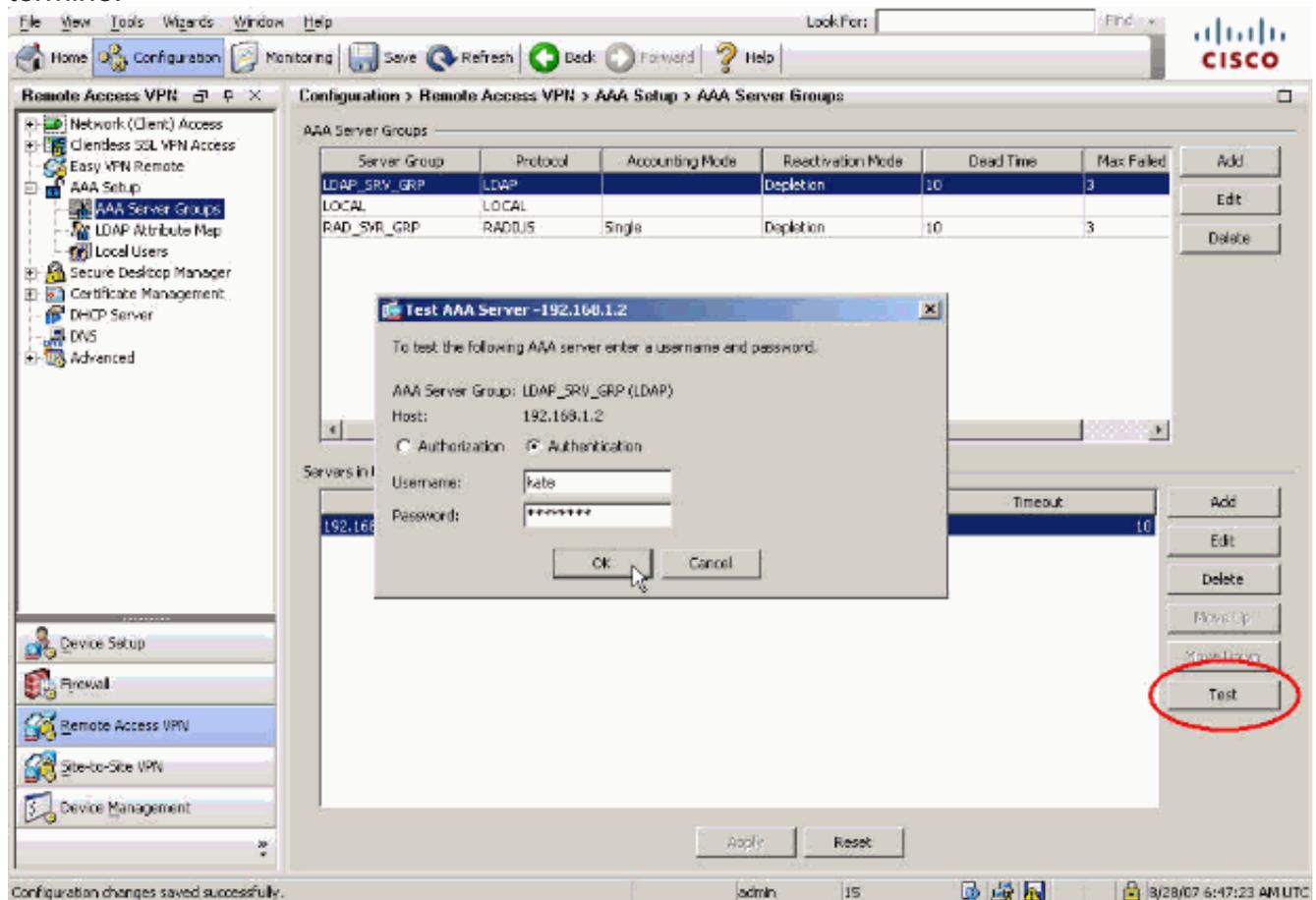
Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

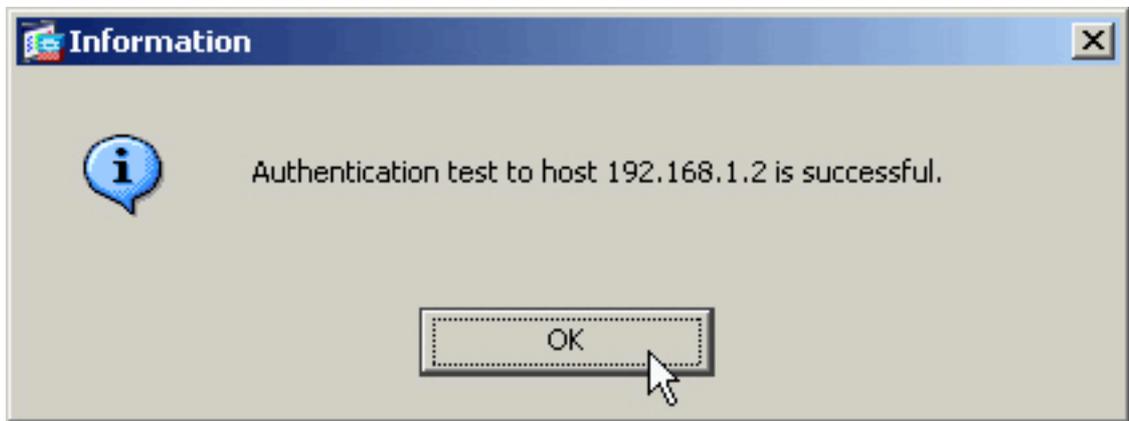
Test avec l'ASDM

Vérifiez votre configuration de LDAP avec la touche "TEST" sur l'écran de configuration de Groupes de serveurs AAA. Une fois que vous fournissez un nom d'utilisateur et mot de passe, ce bouton te permet pour envoyer une demande de test d'authentification au serveur LDAP.

1. Naviguez vers la configuration > l'Accès à distance VPN > AAA installé > des Groupes de serveurs AAA.
2. Sélectionnez votre Groupe de serveurs AAA désiré dans le volet supérieur.
3. Sélectionnez le serveur d'AAA que vous voulez examiner dans le volet inférieur.
4. Cliquez sur la touche "TEST" à la droite du volet inférieur.
5. Dans la fenêtre qui apparaît, cliquez sur la case d'option d'authentification, et fournissez les qualifications avec lesquelles vous voulez tester. Cliquez sur OK une fois terminé.



6. Après que l'ASA contacte le serveur LDAP, un message de succès ou échec



apparaît.

Test avec le CLI

Vous pouvez employer la commande de **test** sur la ligne de commande afin de tester votre installation d'AAA. Une demande de test est envoyée au serveur d'AAA, et le résultat apparaît sur la ligne de commande.

```
ciscoasa#test aaa-server authentication LDAP_SRV_GRP host 192.168.1.2 username kate password
cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

Dépannez

S'incertain de la chaîne en cours de DN à l'utiliser, vous pouvez émettre la commande de **dsquery** sur un serveur de Répertoire actif de Windows d'une invite de commande afin de vérifier la chaîne appropriée de DN d'un objet utilisateur.

```
C:\Documents and Settings\Administrator>dsquery user -samid kate !--- Queries Active Directory
for samid id "kate" "CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com"
```

La commande du **LDAP 255 de débogage** peut aider à dépanner des problèmes d'authentification dans ce scénario. Cette élimination des imperfections de LDAP de commandes enables et te permet pour observer le processus que l'ASA l'utilise pour connecter au serveur LDAP. Ceci sort l'exposition que l'ASA connectent au serveur LDAP conformément à la [section Informations générales de](#) ce document.

Ceci mettent au point des expositions une authentification réussie :

```
ciscoasa#debug ldap 255 [7] Session Start [7] New request Session, context 0xd4b11730, reqType =
1 [7] Fiber started [7] Creating LDAP context with uri=ldap://192.168.1.2:389 [7] Connect to
LDAP server: ldap://192.168.1.2:389, status = Successful [7] defaultNamingContext: value =
DC=ftwsecurity,DC=cisco,DC=com [7] supportedLDAPVersion: value = 3 [7] supportedLDAPVersion:
value = 2 [7] supportedSASLMechanisms: value = GSSAPI [7] supportedSASLMechanisms: value = GSS-
SPNEGO [7] supportedSASLMechanisms: value = EXTERNAL [7] supportedSASLMechanisms: value =
DIGEST-MD5 !--- The ASA connects to the LDAP server as admin to search for kate. [7] Binding as
administrator [7] Performing Simple authentication for admin to 192.168.1.2 [7] LDAP Search:
Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=kate] Scope = [SUBTREE]
[7] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [7] Talking to Active
Directory server 192.168.1.2 [7] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
DC=ftwsecurity,DC=cisco,DC=com [7] Read bad password count 1 !--- The ASA binds to the LDAP
server as kate to test the password. [7] Binding as user [7] Performing Simple authentication
for kate to 192.168.1.2 [7] Checking password policy for user kate [7] Binding as administrator
[7] Performing Simple authentication for admin to 192.168.1.2 [7] Authentication successful for
kate to 192.168.1.2 [7] Retrieving user attributes from server 192.168.1.2 [7] Retrieved
Attributes: [7] objectClass: value = top [7] objectClass: value = person [7] objectClass: value
= organizationalPerson [7] objectClass: value = user [7] cn: value = Kate Austen [7] sn: value =
```

```
Austen [7] givenName: value = Kate [7] distinguishedName: value = CN=Kate
Austen,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [7] instanceType: value = 4 [7] whenCreated:
value = 20070815155224.OZ [7] whenChanged: value = 20070815195813.OZ [7] displayName: value =
Kate Austen [7] uSNCreated: value = 16430 [7] memberOf: value =
CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] memberOf: value =
CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] uSNChanged: value = 20500 [7] name:
value = Kate Austen [7] objectGUID: value = ..z...yC.q0.... [7] userAccountControl: value =
66048 [7] badPwdCount: value = 1 [7] codePage: value = 0 [7] countryCode: value = 0 [7]
badPasswordTime: value = 128321799570937500 [7] lastLogoff: value = 0 [7] lastLogon: value =
128321798130468750 [7] pwdLastSet: value = 128316667442656250 [7] primaryGroupID: value = 513
[7] objectSid: value = .....Q..p..*p?E.Z... [7] accountExpires: value =
9223372036854775807 [7] logonCount: value = 0 [7] sAMAccountName: value = kate [7]
sAMAccountType: value = 805306368 [7] userPrincipalName: value = kate@ftwsecurity.cisco.com [7]
objectCategory: value = CN=Person,CN=Schema,CN=Configuration, DC=ftwsecurity,DC=cisco,DC=com [7]
dSCorePropagationData: value = 20070815195237.OZ [7] dSCorePropagationData: value =
20070815195237.OZ [7] dSCorePropagationData: value = 20070815195237.OZ [7]
dSCorePropagationData: value = 16010108151056.OZ [7] Fiber exit Tx=685 bytes Rx=2690 bytes,
status=1 [7] Session End
```

Ceci mettent au point des expositions une authentification qui échoue en raison d'un mot de passe incorrect :

```
ciscoasa#debug ldap 255 [8] Session Start [8] New request Session, context 0xd4b11730, reqType =
1 [8] Fiber started [8] Creating LDAP context with uri=ldap://192.168.1.2:389 [8] Connect to
LDAP server: ldap://192.168.1.2:389, status = Successful [8] defaultNamingContext: value =
DC=ftwsecurity,DC=cisco,DC=com [8] supportedLDAPVersion: value = 3 [8] supportedLDAPVersion:
value = 2 [8] supportedSASLMechanisms: value = GSSAPI [8] supportedSASLMechanisms: value = GSS-
SPNEGO [8] supportedSASLMechanisms: value = EXTERNAL [8] supportedSASLMechanisms: value =
DIGEST-MD5 !--- The ASA connects to the LDAP server as admin to search for kate. [8] Binding as
administrator [8] Performing Simple authentication for admin to 192.168.1.2 [8] LDAP Search:
Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=kate] Scope = [SUBTREE]
[8] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [8] Talking to Active
Directory server 192.168.1.2 [8] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
DC=ftwsecurity,DC=cisco,DC=com [8] Read bad password count 1 !--- The ASA attempts to bind as
kate, but the password is incorrect. [8] Binding as user [8] Performing Simple authentication
for kate to 192.168.1.2 [8] Simple authentication for kate returned code (49) Invalid
credentials [8] Binding as administrator [8] Performing Simple authentication for admin to
192.168.1.2 [8] Reading bad password count for kate, dn: CN=Kate Austen,CN=Users,
DC=ftwsecurity,DC=cisco,DC=com [8] Received badPwdCount=1 for user kate [8] badPwdCount=1
before, badPwdCount=1 after for kate [8] now: Tue, 28 Aug 2007 15:33:05 GMT, lastset: Wed, 15
Aug 2007 15:52:24 GMT, delta=1122041, maxage=3710851 secs [8] Invalid password for kate [8]
Fiber exit Tx=788 bytes Rx=2904 bytes, status=-1 [8] Session End
```

Ceci mettent au point des expositions une authentification qui échoue parce que l'utilisateur ne peut pas être trouvé sur le serveur LDAP :

```
ciscoasa#debug ldap 255 [9] Session Start [9] New request Session, context 0xd4b11730, reqType =
1 [9] Fiber started [9] Creating LDAP context with uri=ldap://192.168.1.2:389 [9] Connect to
LDAP server: ldap://192.168.1.2:389, status = Successful [9] defaultNamingContext: value =
DC=ftwsecurity,DC=cisco,DC=com [9] supportedLDAPVersion: value = 3 [9] supportedLDAPVersion:
value = 2 [9] supportedSASLMechanisms: value = GSSAPI [9] supportedSASLMechanisms: value = GSS-
SPNEGO [9] supportedSASLMechanisms: value = EXTERNAL [9] supportedSASLMechanisms: value =
DIGEST-MD5 !--- The user mikhail is not found. [9] Binding as administrator [9] Performing
Simple authentication for admin to 192.168.1.2 [9] LDAP Search: Base DN = [dc=ftwsecurity,
dc=cisco, dc=com] Filter = [sAMAccountName=mikhail] Scope = [SUBTREE] [9] Requested attributes
not found [9] Fiber exit Tx=256 bytes Rx=607 bytes, status=-1 [9] Session End
```

Met au point l'exposition ce message d'erreur quand la Connectivité entre l'ASA et le serveur d'authentification LDAP ne fonctionne pas :

```
ciscoasa# debug webvpn 255
INFO: debug webvpn enabled at level 255.
ciscoasa# webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
ewaFormSubmit_webvpn_login: tgCookie = NULL
```

```
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
...not resuming [2587]
webvpn_portal.c:http_webvpn_kill_cookie[787]
webvpn_auth.c:http_webvpn_pre_authentication[2327]
WebVPN: calling AAA with ewsContext (-847917520) and nh (-851696992)!
webvpn_auth.c:webvpn_add_auth_handle[5118]
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[5158] WebVPN: AAA status = (ERROR)
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162] ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1 ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL ...resuming [2564]
webvpn_auth.c:http_webvpn_post_authentication[1506] WebVPN: user: (utrzd01) auth error.
```

[Informations connexes](#)

- [Support et documentation techniques - Cisco Systems](#)