ASA 8.0： WebVPN ユーザのための LDAP 認証の設定

目次

[概要](#)
[前提条件](#)
[背景説明](#)
[LDAP 認証の設定](#)
[ASDM](#)
[コマンド行インターフェイス](#)
[マルチドメイン検索の実行（オプション）](#)
[確認](#)
[ASDM でのテスト](#)
[CLI でのテスト](#)
[トラブルシューティング](#)
[関連情報](#)

概要

このドキュメントでは、WebVPN ユーザの認証に LDAP を使用するように、Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を設定する方法を示しています。 この例の LDAP サーバは、Microsoft Active Directory です。 この設定は、ソフトウェア バージョン 8.0(2) が稼働する ASA 上の Adaptive Security Device Manager（ASDM）6.0(2) で実行されます。

注: この例では、Lightweight Directory Access Protocol（LDAP）認証が WebVPN ユーザ向けに設定されていますが、この設定は他のすべてのタイプのリモート アクセス クライアントにも使用できます。 示されているように、AAA サーバ グループを対象の接続プロファイル（トンネル グループ）に割り当てるだけです。

前提条件

基本的な VPN 構成が必要です。 この例では、WebVPN が使用されます。

背景説明

この例では、認証されるユーザの ID を確認するために、ASA によって LDAP サーバがチェックされます。 このプロセスは、従来の Remote Authentication Dial-In User Service（RADIUS）や Terminal Access Controller Access-Control System Plus（TACACS+）の交換のようには動作しません。 次の手順では、ユーザのクレデンシャルをチェックするために、ASA で LDAP サーバが使用される方法の概略を説明しています。

1. ユーザが ASA への接続を開始します。
2. ASA は Microsoft Active Directory（AD）/LDAP サーバを使用してユーザを認証するように設定されています。
3. ASA は、ASA 上で設定されたクレデンシャル（この場合は admin）を使用して LDAP サーバにバインドし、指定されたユーザ名を検索します。 **admin ユーザ**も、Active Directory 内でコンテンツを一覧で表示するために適切なクレデンシャルを取得します。 http://support.microsoft.com/?id=320528 を参照して、 LDAP クエリー特権を付与する方法についての詳細を確認してください。**注:** http://support.microsoft.com/?id=320528 の Microsoft ウェブサイトは、 サード パーティのプロバイダーによって管理されます。 Cisco では、そのコンテンツに関する責任を負いません。
4. そのユーザ名が見つかった場合、ASA はユーザがログイン時に指定したクレデンシャルを使用して LDAP サーバへのバインドを試みます。
5. 2 回目のバインドに成功すると、認証が成功し、ASA によってユーザのアトリビュートが処理されます。**注:** この例では、アトリビュートはどの目的にも使用されません。 『ASA/PIX: LDAP 設定により VPN クライアントを VPN グループ ポリシーにマッピングする例』で、ASA で LDAP アトリビュートを処理できる方法についての例を参照してください。

LDAP 認証の設定

このセクションでは、WebVPN クライアントの認証に LDAP サーバを使用することを目的として、ASA を設定するための情報を提供しています。

ASDM

LDAP サーバと通信を行って WebVPN クライアントを認証するように ASA を設定するには、ASDM で次の手順を実行します。

1. [Configuration] > [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] の順に移動します。
2. AAA Server Groups の横にある **Add** をクリックします。
3. 新しい AAA サーバ グループの名前を指定し、プロトコルとして **LDAP** を選択します。
4. 新しいグループが最上部のペインで選択されていることを確認し、**Servers in the Selected Group** ペインの横にある **Add** をクリックします。
5. LDAP サーバの設定情報を入力します。 続くスクリーンショットは設定例を示しています。これは数多くある設定オプションの説明の 1 つです。**Interface Name** ：LDAP サーバに到達するために ASA によって使用されるインターフェイス。**Server Name or IP address**：LDAP サーバに到達するために ASA によって使用されるアドレス。**Server Type**：Microsoft など、LDAP サーバのタイプ。**Base DN**：サーバが検索を開始する必要がある LDAP 階層内の場所。**Scope**：サーバが作成する必要がある LDAP 階層内の検索の範囲。**Naming Attribute**：LDAP サーバ上でエントリが一意に識別される相対識別名アトリビュート（複数のアトリビュートの場合もあり）。 **sAMAccountName**は、Microsoft Active Directory 内のデフォルトのアトリビュートです。 一般的に使用される他のアトリビュートは、CN、UID、および userPrincipalName です。**Login DN**：LDAP サーバでのユーザの検索、読み取り、またはルックアップを可能にするために十分な特権を与えられた DN。**Login Password**：DN アカウントのパスワード。**LDAP Attribute Map**：このサーバからの応答で使用される LDAP アトリビュート マップ。 『ASA/PIX: LDAP アトリビュート マップを設定する方法についての詳細は、『LDAP 設定により VPN クライアントを VPN グループ ポリ

シーにマッピングする例』を参照してください。

6. AAA サーバ グループを設定して、サーバをそれに追加したら、新しい AAA 設定を使用するために接続プロファイル（トンネル グループ）を設定する必要があります。 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] の順に進みます。
7. AAA を設定する設定プロファイル（トンネル グループ）を選択し、**Edit** をクリックします。
8. [Authentication] の下で、すでに作成した LDAP サーバ グループを選択します。

コマンド行インターフェイス

LDAP サーバと通信を行って、WebVPN クライアントを認証するように ASA を設定するには、Command Line Interface（CLI; コマンドライン インターフェイス）で次の手順を実行します。

```
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
```

マルチドメイン検索の実行（オプション）

オプション。 現在、ASA ではマルチドメイン検索のための LDAP リフェラル メカニズムはサポートされていません（Cisco Bug ID CSCsj32153）。 マルチドメイン検索は、グローバル カタログ サーバ モードの AD でサポートされています。 マルチドメイン検索を実行するには、通常、ASA 内の LDAP サーバ エントリの主なパラメータを使用して、グローバル カタログ サーバ モードの AD サーバを設定します。 ディレクトリ ツリー全体で一意である必要がある ldap-name-attribute を使用することが重要です。

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

確認

このセクションでは、設定が正常に機能していることを確認します。

ASDM でのテスト

AAA サーバ グループの設定画面で **Test** ボタンを使用して、LDAP 設定を確認します。 ユーザ名とパスワードを入力すると、このボタンを使用してテスト認証要求を LDAP サーバへ送信できます。

1. [Configuration] > [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] の順に移動します。
2. 最上部のペインで対象の AAA サーバ グループを選択します。
3. 下部のペインでテストする AAA サーバを選択します。
4. 下部のペインの右側にある **Test** ボタンをクリックします。

5. 表示されるウィンドウで、[Authentication] オプション ボタンをクリックして、テスト対象のクレデンシャルを入力します。 完了したら、[OK] をクリックします。
6. ASA から LDAP サーバに通信が行われた後、成功または失敗のメッセージが表示されます。

CLI でのテスト

AAA 設定をテストするためにコマンドラインで **test** コマンドを使用できます。 テスト要求が AAA サーバに送信され、コマンド ラインに結果が表示されます。

```
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
```

トラブルシューティング

使用する現在の DN ストリングが不明な場合、コマンド プロンプトから Windows Active Driectory サーバ上で **dsquery** コマンドを発行して、ユーザ オブジェクトの適切な DN ストリングを確認できます。

```
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"
```

debug ldap 255 コマンドは、このシナリオで認証問題のトラブルシューティングに有効です。 このコマンドを使用すると、LDAP デバッグがイネーブルになり、LDAP サーバに接続するために ASA によって使用されるプロセスを監視することができます。 このドキュメントの「背景説明」セクションで概説したように、次の出力では LDAP サーバへの ASA の接続が表示されています。

次のデバッグでは、成功した認証が示されています。

```
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 = 20070815155224.0Z [7] whenChanged: value = 20070815195813.0Z [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 = 20070815195237.0Z [7] dSCorePropagationData: value = 20070815195237.0Z [7] dSCorePropagationData: value = 20070815195237.0Z [7] dSCorePropagationData: value = 16010108151056.0Z [7] Fiber exit Tx=685 bytes Rx=2690 bytes, status=1 [7] Session End

次のデバッグでは、誤ったパスワードが原因で失敗する認証が示されています。

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

次のデバッグでは、LDAP サーバでユーザを検索できないために失敗する認証が示されています。

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

デバッグは、ASA と LDAP 認証サーバ間の接続が機能しない場合にこのエラー メッセージを表示します。

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: (utrcd01) auth error.
```

関連情報

- テクニカルサポートとドキュメント - Cisco Systems