ASA 8.0: Autenticación ldap de la configuración para los usuarios de WebVPN

Contenido

Introducción

Este documento demuestra cómo configurar Cisco Adaptive Security Appliance (ASA) para utilizar un servidor LDAP para la autenticación de usuarios de WebVPN. El servidor LDAP de este ejemplo es Microsoft Active Directory. Esta configuración se realiza con el Administrador de dispositivos de seguridad adaptante (ASDM) 6.0(2) en un ASA que funcione con la versión de software 8.0(2).

Nota: En este Lightweight Directory Access Protocol (LDAP) del ejemplo la autenticación se configura para los usuarios de WebVPN, pero esta configuración se puede utilizar para el resto de los tipos de clientes de acceso remoto también. Asigne simplemente al Grupo de servidores AAA al perfil de la conexión deseado (grupo de túnel), como se muestra.

prerrequisitos

Se requiere una configuración VPN básica. En este ejemplo se utiliza el WebVPN.

Antecedentes

En este ejemplo, el ASA marca con un servidor LDAP para verificar la identidad de los usuarios que autentica. Este proceso no trabaja como un Remote Authentication Dial-In User Service (RADIUS) tradicional o el Terminal Access Controller Access Control System más el intercambio (TACACS+). Estos pasos explican, en un nivel elevado, cómo el ASA utiliza a un servidor LDAP para marcar los credenciales de usuario.

1. El usuario inicia una conexión al ASA.
2. El ASA se configura para autenticar a ese usuario con el servidor del Microsoft Active Directory (AD) /LDAP.
3. El ASA ata al servidor LDAP con las credenciales configuradas en el ASA (admin en este caso), y mira para arriba el nombre de usuario proporcionado. **El Usuario administrador** también obtiene las credenciales apropiadas para enumerar el contenido dentro del Active Directory. Refiera a http://support.microsoft.com/?id=320528 para más información sobre cómo conceder los privilegios de la interrogación LDAP.**Nota:** El sitio Web de Microsoft en http://support.microsoft.com/?id=320528 es manejado por un proveedor del otro vendedor. Cisco no es responsable por su contenido.
4. Si se encuentra el nombre de usuario, el ASA intenta atar al servidor LDAP con las credenciales a que el usuario proporcionó en el login.
5. Si el segundo lazo es acertado, la autenticación tiene éxito y el ASA procesa los atributos del usuario.**Nota:** En este ejemplo los atributos no se utilizan para cualquier cosa. Refiérase ASA/PIX: Asociando a los clientes VPN a las directivas del grupo VPN con el ejemplo de la Configuración LDAP para ver un ejemplo de cómo el ASA puede procesar los atributos LDAP.

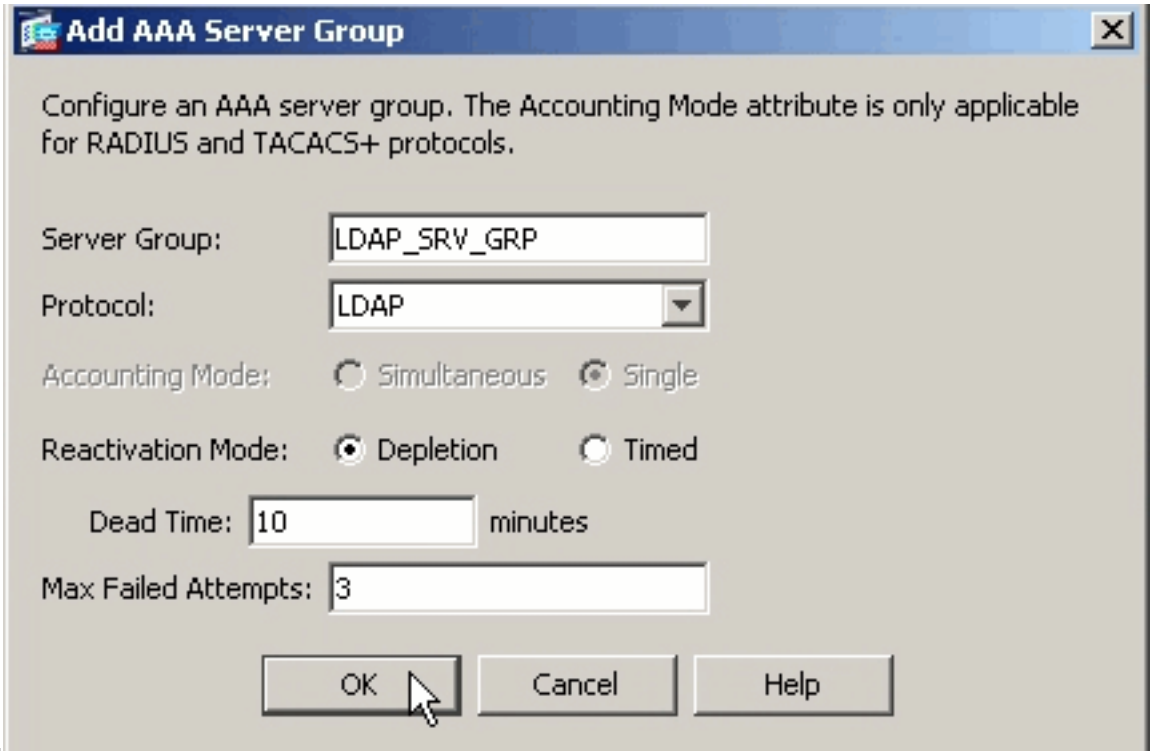
Autenticación ldap de la configuración

En esta sección, le presentan con la información para configurar el ASA para utilizar a un servidor LDAP para la autenticación de los clientes del WebVPN.

ASDM

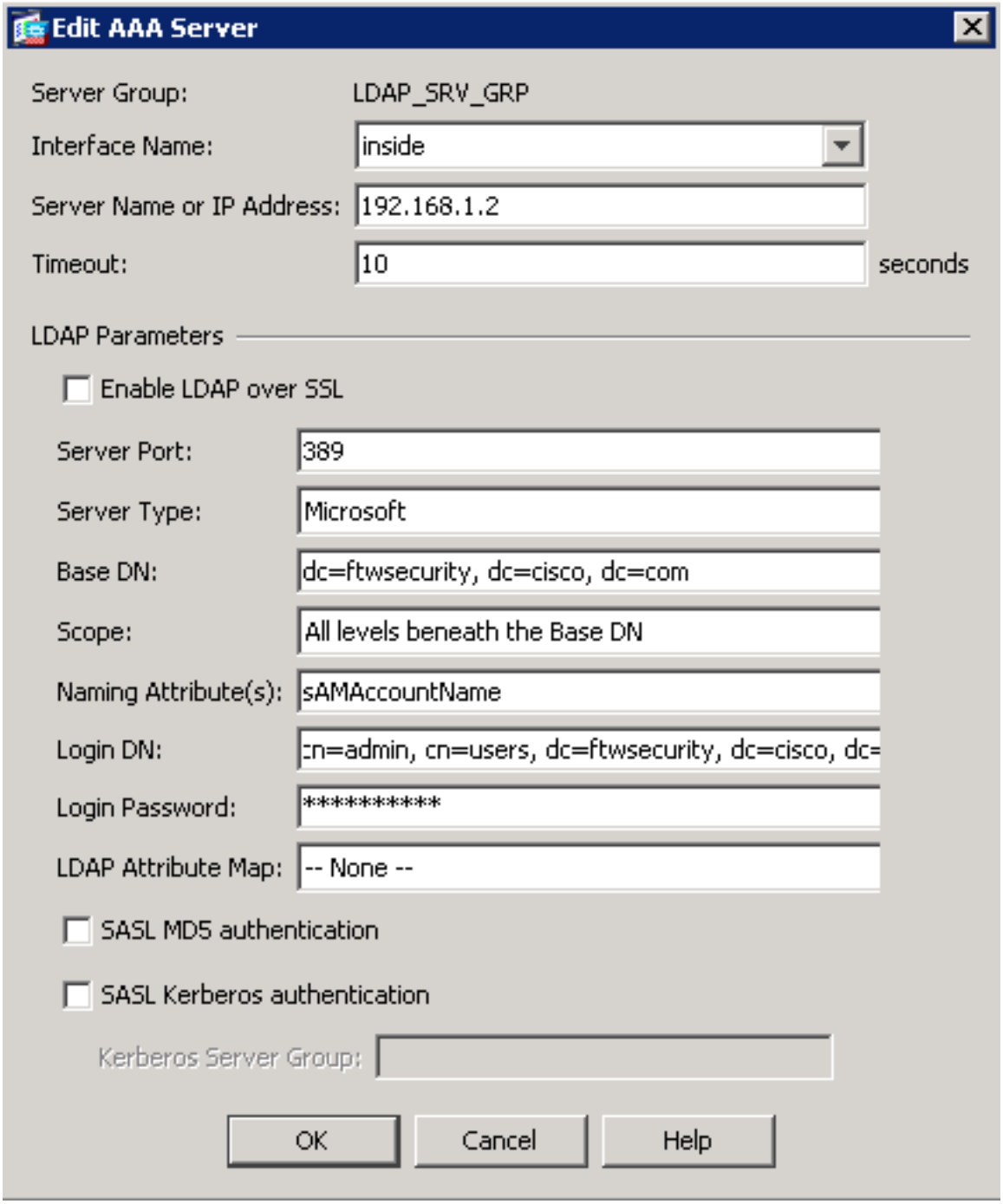
Complete estos pasos en el ASDM para configurar el ASA para comunicar con el servidor LDAP y para autenticar a los clientes del WebVPN.

1. Navegue a la configuración > al VPN de acceso remoto >AAA ponen >AAA a los grupos de servidores.
2. El tecleo **agrega** al lado de los Grupos de servidores AAA
3. Especifique un nombre para el nuevo Grupo de servidores AAA, y elija el **LDAP** como el

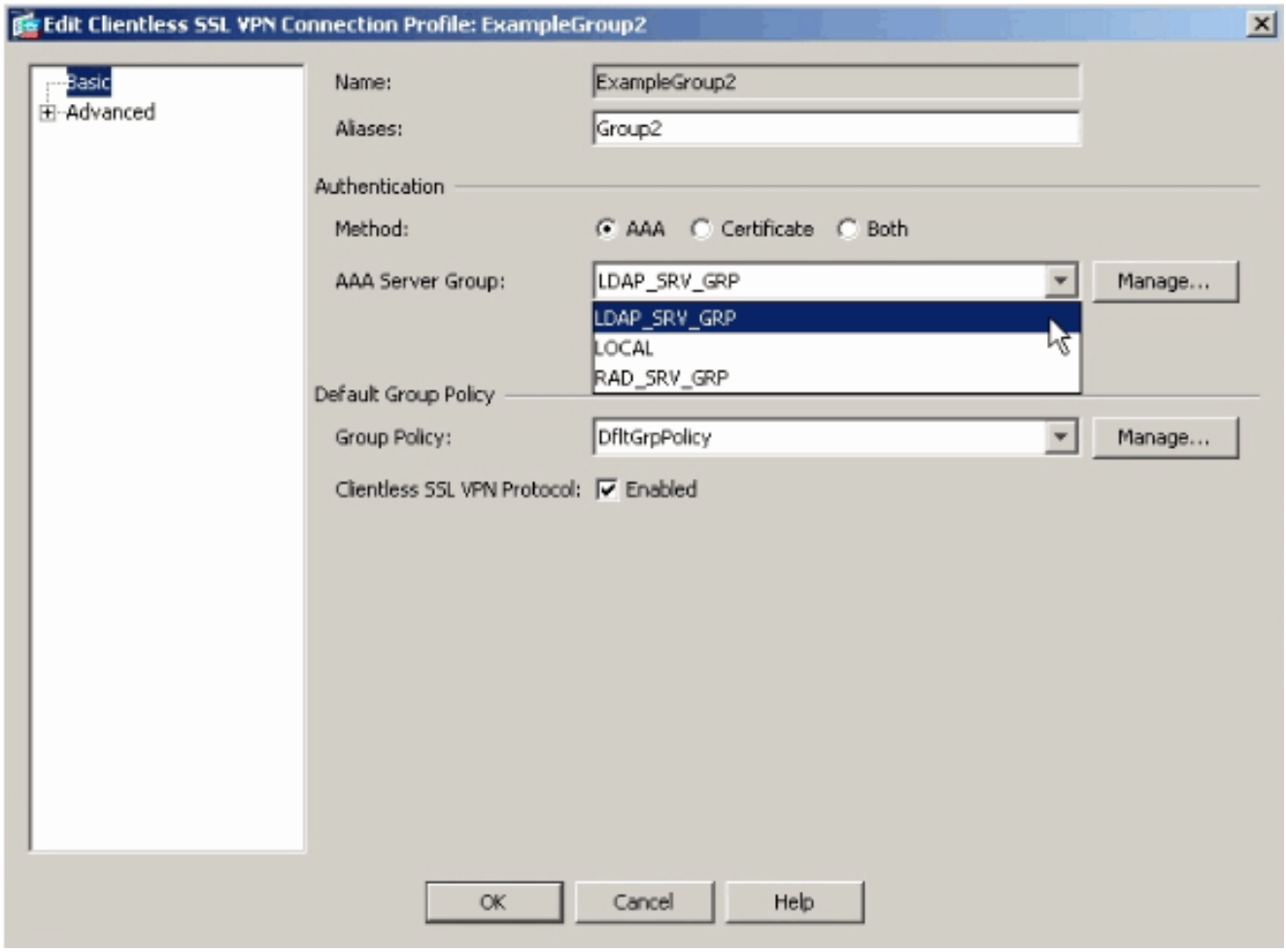


protocolo.

4. Esté seguro que seleccionan a su nuevo grupo en el cristal superior, y el tecleo **agrega** al lado de los **servidores en el** cristal **seleccionado del grupo**.
5. Proporcione la información de la configuración para su servidor LDAP. El tiro de pantalla subsiguiente ilustra un ejemplo de configuración. Ésta es una explicación de muchas de las opciones de configuración:**Nombre de la interfaz** — la interfaz que las aplicaciones ASA para alcanzar al servidor LDAP**Nombre del servidor o dirección IP** — el direccionamiento que las aplicaciones ASA para alcanzar al servidor LDAP**Tipo de servidor** — el tipo de servidor LDAP, tal como Microsoft**Base DN** — la ubicación en la jerarquía LDAP en donde el servidor debe comenzar a buscar**Alcance** — el fragmento de la búsqueda en la jerarquía LDAP que el servidor debe hacer**Atributo de nombramiento** — el atributo de nombre distintivo relativo (o atributos) que identifica únicamente una entrada en el servidor LDAP. **el sAMAccountName** es el atributo predeterminado en el Microsoft Active Directory. Otros atributos de uso general son CN, UID, y userPrincipalName.**Login DN** — el DN con bastantes privilegios para ser buscar capaz/usuarios del lread/de las operaciones de búsqueda en el servidor LDAP**Contraseña de inicio de sesión** — la contraseña para la cuenta DN**Mapa del atributo LDAP** — una correspondencia del atributo LDAP que se utilizará con las respuestas de este servidor. Refiérase [ASA/PIX: Asociando los clientes VPN a las directivas del grupo VPN con el ejemplo de la Configuración LDAP] para más información sobre cómo configurar el LDAP atribuyen las
correspondencias.



6. Una vez que usted ha configurado al Grupo de servidores AAA y ha agregado un servidor a él, es necesario configurar su perfil de la conexión (grupo de túnel) para utilizar la nueva configuración AAA. Navegue a la configuración > al VPN de acceso remoto > al acceso > a los perfiles de la conexión del clientless SSL VPN.
7. Elija el perfil de la conexión (el grupo de túnel) para quien usted quiere configurar el AAA, y el tecleo **edita**
8. Bajo **autenticación**, elija al grupo de servidor LDAP que usted creó anterior.



Interfaz de la línea de comandos

Complete estos pasos en el comando line interface(cli) para configurar el ASA para comunicar con el servidor LDAP y para autenticar a los clientes del 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
```

Realice las búsquedas del Multi-dominio (opcionales)

Opcional. El ASA no soporta actualmente el mecanismo de la remisión LDAP para las búsquedas del multi-dominio (Id. de bug Cisco CSCsj32153). las búsquedas del Multi-dominio se soportan con el AD en el modo de servidor de catálogo global. Para realizar las búsquedas del multi-dominio, la configuración encima del servidor AD para el modo de servidor de catálogo global, con éstos cierra generalmente los parámetros para la entrada del servidor LDAP en el ASA. La clave es utilizar un ldap-nombre-atributo que deba ser único a través del árbol de directorio.

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

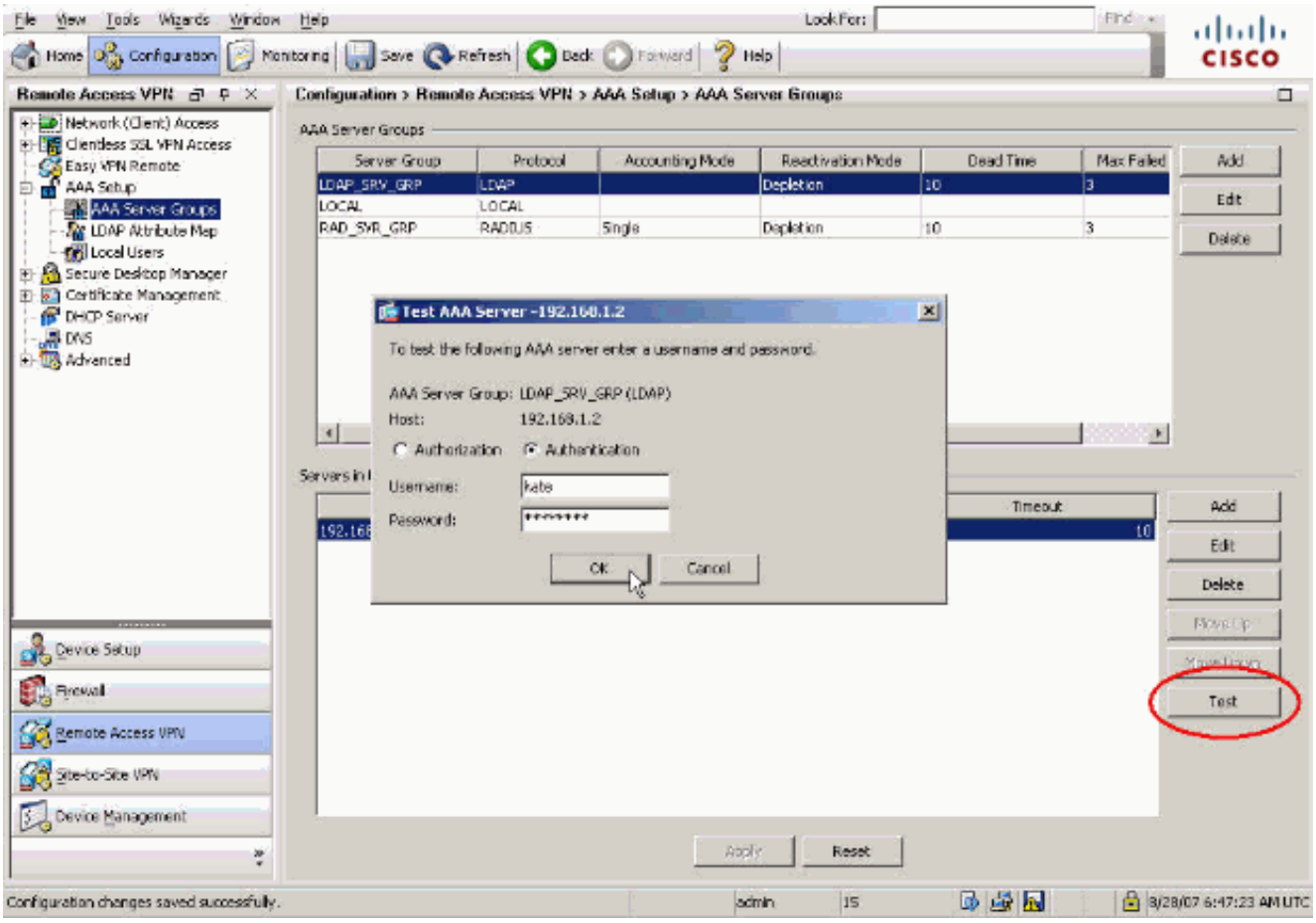
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

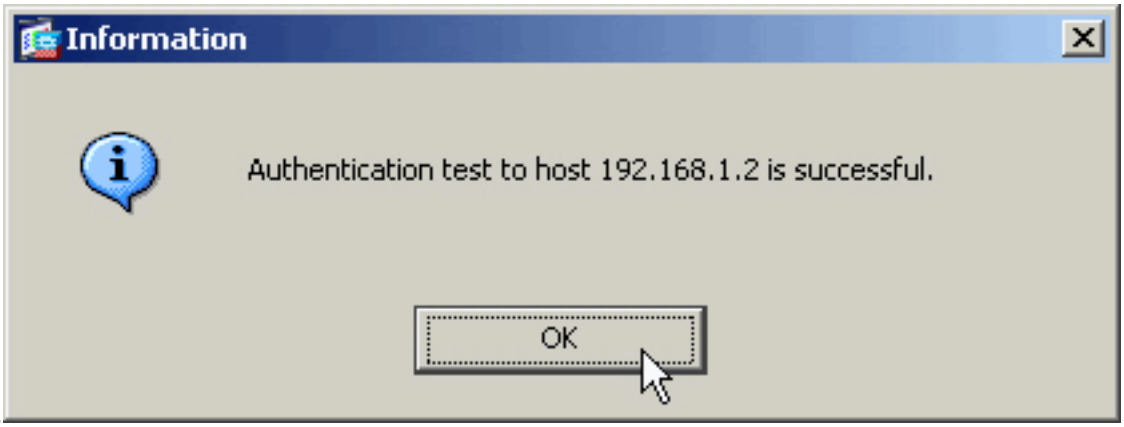
Pruebe con el ASDM

Verifique su Configuración LDAP con el **botón Test Button** en la pantalla de configuración de los Grupos de servidores AAA. Una vez que usted suministra un nombre de usuario y contraseña, este botón permite que usted envíe una petición de la prueba de la autentificación al servidor LDAP.

1. Navegue a la configuración > al VPN de acceso remoto >AAA ponen >AAA a los grupos de servidores.
2. Seleccione a su Grupo de servidores AAA deseado en el cristal superior.
3. Seleccione al servidor de AAA que usted quiere probar en el cristal más bajo.
4. Haga clic el **botón Test Button** a la derecha del cristal más bajo.
5. En la ventana que aparece, haga clic el botón de radio de la **autenticación**, y suministre las credenciales con las cuales usted quiere probar. Haga Click en OK cuando está acabado.



6. Después de que el ASA entre en contacto al servidor LDAP, un éxito o un mensaje de error

aparece. 

Pruebe con el CLI

Usted puede utilizar el **comando test** en la línea de comando para probar su configuración AAA. Una petición de la prueba se envía al servidor de AAA, y el resultado aparece en la línea de comando.

```
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
```

Troubleshooting

Si es inseguro de la cadena actual DN a utilizar, usted puede publicar el comando del **dsquery** en un servidor Active Directory de Windows de un comando prompt para verificar la cadena apropiada DN de un objeto de usuario.

```
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"
```

El comando del **ldap 255 del debug** puede ayudar a resolver problemas los problemas de autenticación en este escenario. Este comando habilita el debugging LDAP y permite que usted mire el proceso que el ASA utiliza para conectar con el servidor LDAP. Esto hace salir la demostración que el ASA conecta con el servidor LDAP de acuerdo con la sección de información previa de este documento.

Este debug muestra una autenticación satisfactoria:

```
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
```

Este debug muestra una autenticación que falle debido a una contraseña incorrecta:

```
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
```

Este debug muestra una autenticación que falle porque el usuario no puede ser encontrado en el servidor 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
```

Los debugs muestran este mensaje de error cuando la Conectividad entre el ASA y el servidor de la autenticación ldap no trabaja:

```
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.
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems