ASA 8.0: Configurar a autenticação LDAP para usuários WebVPN

Índice

Introdução

Este documento demonstra como configurar a Cisco Adaptive Security Appliance (ASA) para usar um servidor LDAP para autenticação de usuários da WebVPN. O servidor LDAP neste exemplo é o Microsoft Active Directory. Esta configuração é executada com o Security Device Manager adaptável (ASDM) 6.0(2) em um ASA que execute a versão de software 8.0(2).

Nota: Neste Lightweight Directory Access Protocol (LDAP) do exemplo a autenticação é configurada para usuários WebVPN, mas esta configuração pode ser usada para todos tipos restantes de clientes de acesso remoto também. Atribua simplesmente o Grupo de servidores AAA ao perfil de conexão desejado (grupo de túneis), como mostrado.

Pré-requisitos

Uma configuração de VPN básica é exigida. Neste exemplo o WebVPN é usado.

Informações de Apoio

Neste exemplo, o ASA verifica com um servidor ldap a fim verificar a identidade dos usuários que autentica. Este processo não trabalha como uma troca tradicional do Remote Authentication Dial-In User Service (RADIUS) ou do protocolo tacacs+ (TACACS+). Estas etapas explicam, em um nível alto, como o ASA usa um servidor ldap a fim verificar credenciais do usuário.

1. O usuário inicia uma conexão ao ASA.

2. O ASA é configurado para autenticar esse usuário com o server do microsoft ative directory (AD) /LDAP.
3. O ASA liga ao servidor ldap com as credenciais configuradas no ASA (admin neste caso), e olha acima o username fornecido. **O usuário admin** igualmente obtém as credenciais apropriadas para alistar índices dentro do diretório ativo. Refira http://support.microsoft.com/?id=320528 para obter mais informações sobre de como conceder privilégios da pergunta LDAP.**Nota:** A site do microsoft em http://support.microsoft.com/?id=320528 é controlada por um fornecedor da terceira parte. Cisco não é responsável para seu índice.
4. Se o username é encontrado, o ASA tenta ligar ao servidor ldap com as credenciais que o usuário forneceu no início de uma sessão.
5. Se o segundo ligamento é bem sucedido, a autenticação sucede e o o ASA processa os atributos do usuário.**Nota:** Neste exemplo os atributos não são usados para qualquer coisa. Refira ASA/PIX: Traçando clientes VPN às políticas do grupo de VPN com o exemplo da configuração ldap a fim ver um exemplo de como o ASA pode processar atributos LDAP.

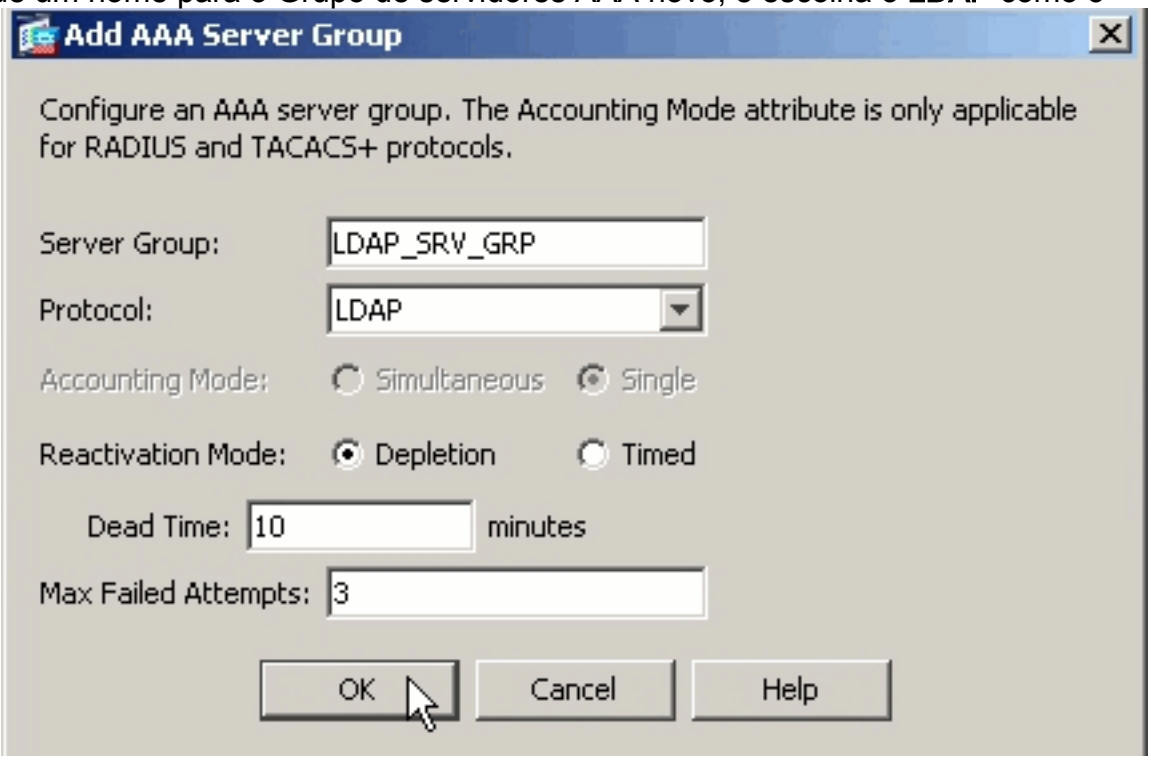
Configurar a autenticação LDAP

Nesta seção, você é presentado com a informação para configurar o ASA para usar um servidor ldap para a autenticação de clientes WebVPN.

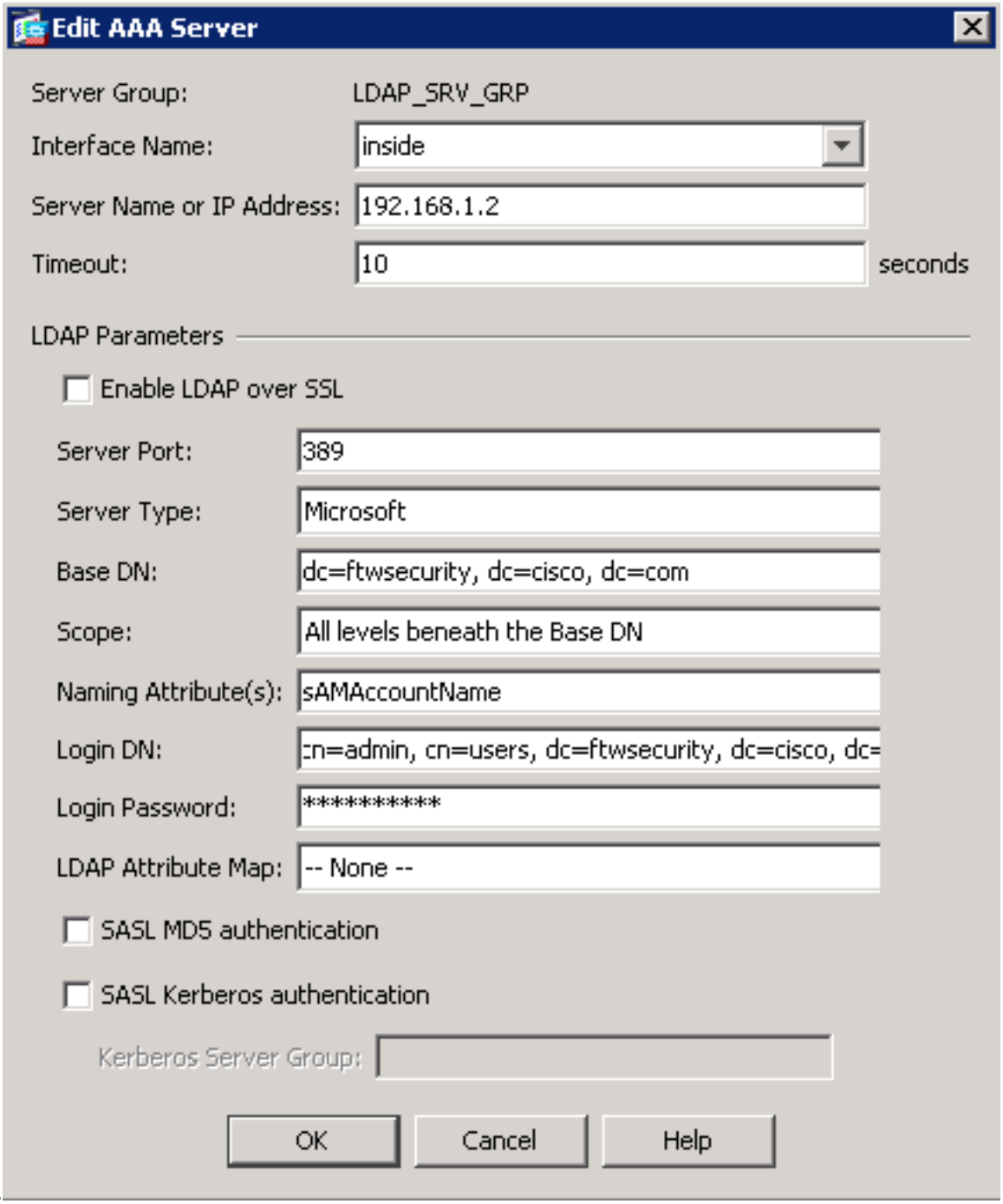
ASDM

Termine estas etapas no ASDM a fim configurar o ASA para comunicar-se com o servidor ldap e para autenticar clientes WebVPN.

1. Navegue à configuração > ao acesso remoto VPN > ao AAA Setup > Grupos de servidores AAA.
2. O clique **adiciona** ao lado dos Grupos de servidores AAA
3. Especifique um nome para o Grupo de servidores AAA novo, e escolha o **LDAP** como o protocolo.

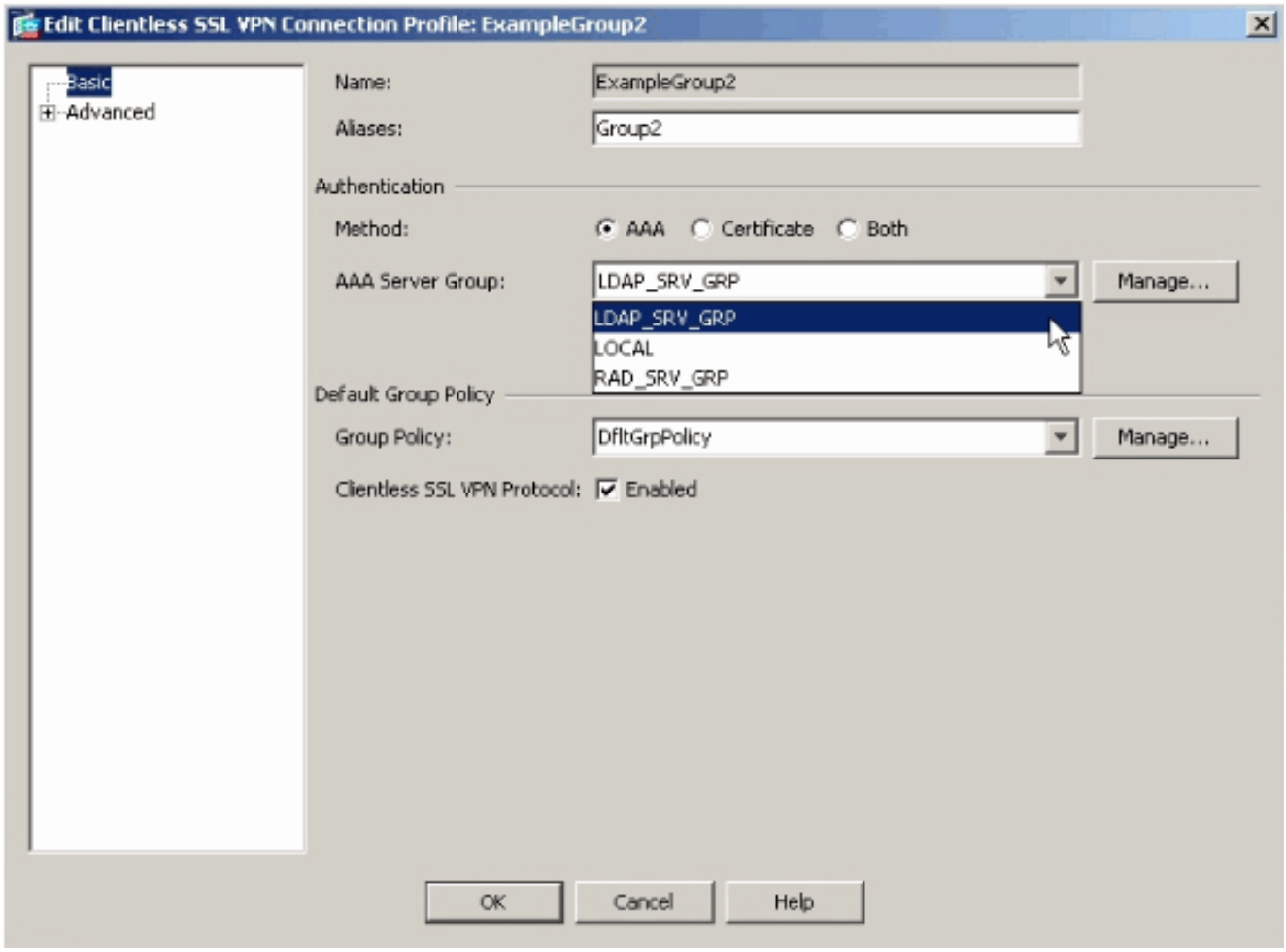


4. Seja certo que seu grupo novo está selecionado na placa superior, e o clique **adiciona** ao lado dos **server na** placa **selecionada do grupo**.
5. Forneça a informação de configuração para seu servidor ldap. O tiro de tela subsequente ilustra um exemplo de configuração. Esta é uma explicação de muitas das opções de configuração:**Nome da relação** — a relação que os usos ASA a fim alcançar o servidor ldap**Nome do servidor ou endereço IP de Um ou Mais Servidores Cisco ICM NT** — o endereço que os usos ASA a fim alcançar o servidor ldap**Tipo de servidor** — o tipo de servidor ldap, tal como Microsoft**Base DN** — o lugar na hierarquia LDAP onde o server deve começar a procurar**Espaço** — a extensão da busca na hierarquia LDAP que o server deve fazer**Atributo de nomeação** — o atributo de nome destacado relativo (ou atributos) que identifica excepcionalmente uma entrada no servidor ldap. **o sAMAccountName** é o atributo de padrão no microsoft ative directory. Outros atributos de uso geral são CN, UID, e userPrincipalName.**Início de uma sessão DN** — o DN com bastante privilégios a fim ser procurar capaz/usuários do lread/consulta no servidor ldap**Senha de login** — a senha para a conta DN**Mapa do atributo LDAP** — um mapa do atributo LDAP a ser usado com respostas deste server. Refira ASA/PIX: Traçando os clientes VPN às políticas do grupo de VPN com o exemplo da configuração ldap para obter mais informações sobre de como configurar o LDAP atribuem



mapas.

6. Uma vez que você configurou o Grupo de servidores AAA e lhe adicionou um server, é necessário configurar seu perfil de conexão (grupo de túneis) para usar a configuração de AAA nova. Navegue à configuração > ao acesso remoto VPN > ao acesso > aos perfis de conexão dos sem clientes SSL VPN.
7. Escolha o perfil de conexão (o grupo de túneis) para que você quer configurar o AAA, e o clique **edita**
8. Sob a **autenticação**, escolha o grupo de servidor ldap que você criou mais cedo.



Interface da linha de comando

Termine estas etapas no comando line interface(cli) a fim configurar o ASA para comunicar-se com o servidor ldap e para autenticar clientes 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
```

Execute as buscas do Multi-domínio (opcionais)

Opcional. O ASA atualmente não apoia o mecanismo da referência LDAP para buscas do multi-domínio (identificação de bug Cisco CSCsj32153). as buscas do Multi-domínio são apoiadas com o AD no modo de servidor global catalog. A fim executar buscas do multi-domínio, a instalação acima do server AD para o modo de servidor global catalog, geralmente com estes fecha parâmetros para a entrada do servidor ldap no ASA. A chave é usar um LDAP-nome-atributo que deva ser original através da árvore de diretório.

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

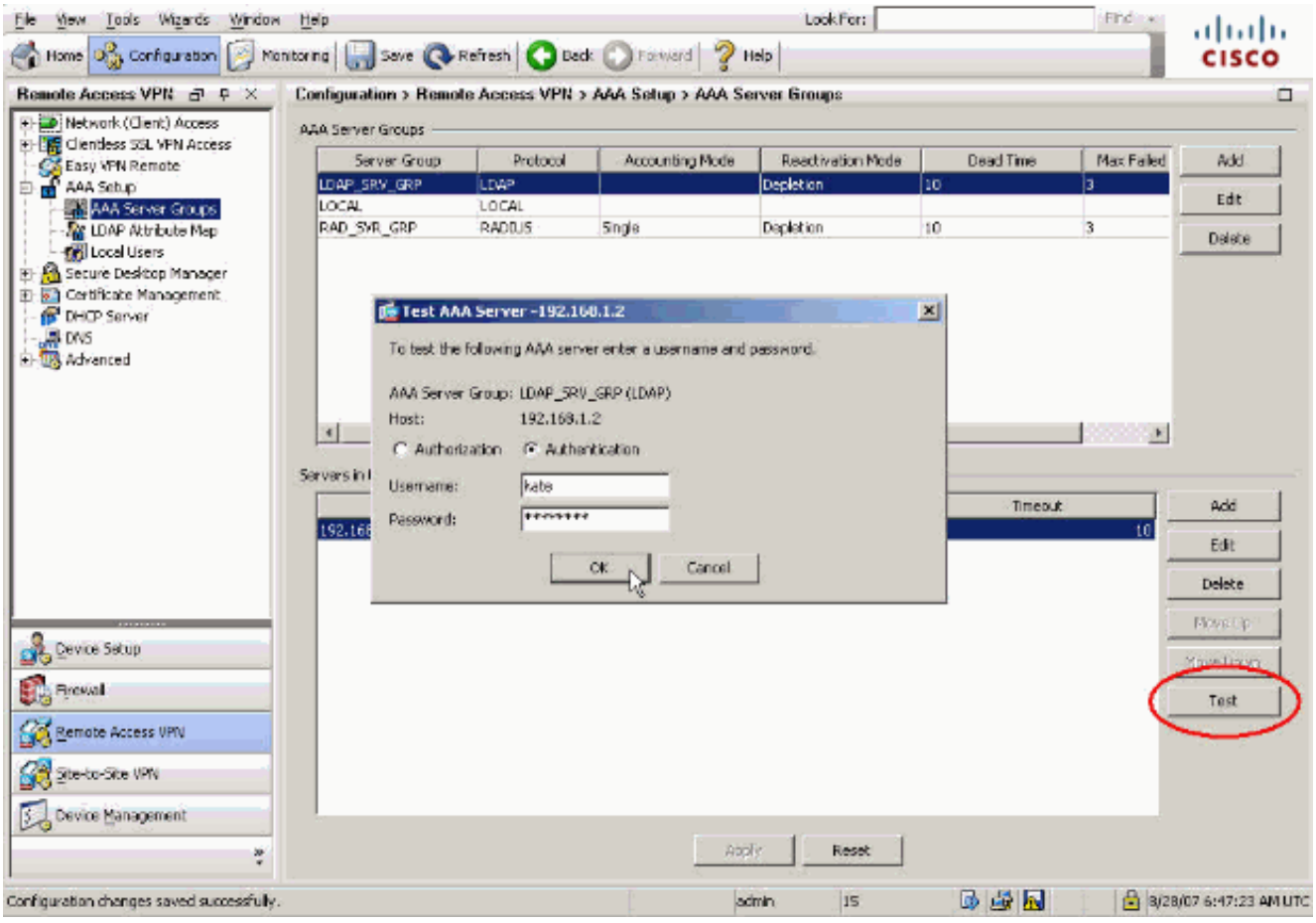
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

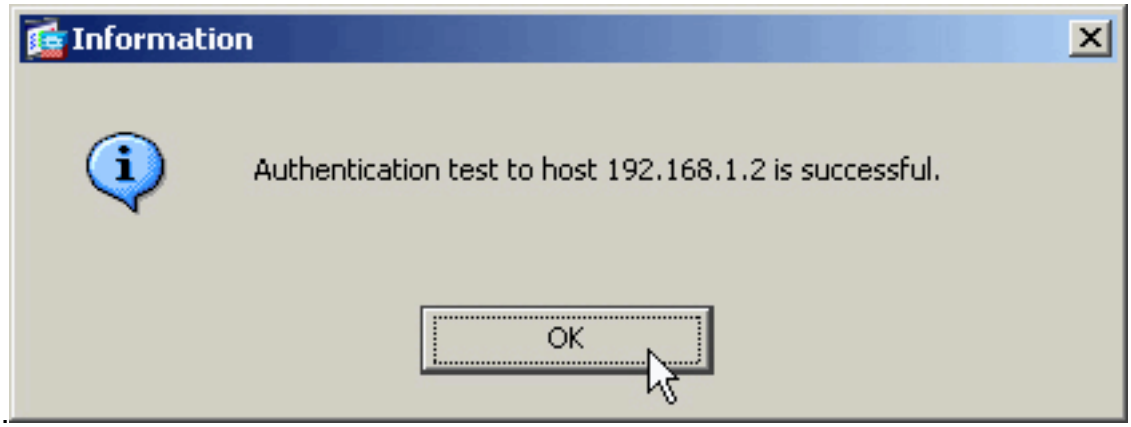
Teste com ASDM

Verifique sua configuração ldap com o **botão Test Button na** tela de configuração dos Grupos de servidores AAA. Uma vez que você fornece um nome de usuário e senha, este botão permite que você envie um pedido da autenticação de teste ao servidor ldap.

1. Navegue à configuração > ao acesso remoto VPN > ao AAA Setup > Grupos de servidores AAA.
2. Selecione seu Grupo de servidores AAA desejado na placa superior.
3. Selecione o servidor AAA que você quer testar na placa mais baixa.
4. Clique o **botão Test Button** à direita da placa mais baixa.
5. No indicador que aparece, clique o botão de rádio da **autenticação**, e forneça as credenciais com que você quer testar. Clique a **APROVAÇÃO** quando terminado.



6. Depois que o ASA contacta o servidor ldap, um sucesso ou um mensagem de falha

aparecem. 

Teste com CLI

Você pode usar o **comando test na** linha de comando a fim testar sua instalação AAA. Um pedido do teste é enviado ao servidor AAA, e o resultado aparece na linha 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

Se incerto da corda atual DN a usar-se, você pode emitir o comando do **dsquery em um** servidor ative directory de Windows de um comando prompt a fim verificar a corda apropriada DN de um objeto do usuário.

```
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"
```

O comando do **ldap 255 debugar** pode ajudar a pesquisar defeitos problemas de autenticação nesta encenação. Este comando permite a eliminação de erros LDAP e permite que você olhe o processo que o ASA se usa para conectar ao servidor ldap. Isto outputs a mostra que o ASA conecta ao servidor ldap de acordo com a seção de informações de fundo deste documento.

Isto debuga mostras uma autenticação bem sucedida:

```
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
```

Isto debuga mostras uma autenticação que falhe devido a uma senha incorreta:

```
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
```

Isto debuga mostras uma autenticação que falhe porque o usuário não pode ser encontrado no 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
```

Debuga a mostra este Mensagem de Erro quando a Conectividade entre o ASA e o server da autenticação LDAP não trabalha:

```
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.
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems