Admissões IP ISR e LDAP para a reorientação da Web a ScanSafe/a exemplo da configuração de segurança Web da nuvem

Índice

Introdução

Este documento descreve como configurar o Roteadores dos Serviços integrados do G2 Series de Cisco (ISR). Quando a configuração da admissão e do Lightweight Directory Access Protocol (LDAP) IP puder ser usada simplesmente para o Proxy de autenticação no ISR, está usada tipicamente conjuntamente com os recursos de redirecionamento da Segurança da Web da nuvem de Cisco (CWs). Como tal, este documento é pretendido ser uma referência a fim suplementar a configuração da reorientação CWs e a documentação do Troubleshooting em ISR.

Pré-requisitos

Requisitos

Cisco recomenda que sua reunião do sistema estas exigências antes que você tente as configurações que estão descritas neste documento:

- O ISR deve executar a versão de código 15.2(1)T1 ou mais tarde.
- Seu sistema deve ter as imagens com a licença (SEC) ajustada recursos de segurança que estão disponíveis no ® do Cisco IOS (universal).
- A estação de trabalho cliente no domínio do diretório ativo (AD) deve ter a capacidade de executar a autenticação ativa através de um navegador da Web.
- Você deve ter uma assinatura CWs.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Internet explorer, Google Chrome, Mozilla Firefox (exige a configuração adicional para a autenticação transparente do gerenciador de LAN de NT (NTLM))
- Cisco G2 800, 1900, 2900, e 3900 Series ISR.
- Controlador de domínio de Microsoft Windows AD (ADDC)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

> Nota: Cisco G1 1800, 2800, e 3800 Series Router não é apoiado.

Informações de Apoio

Muitos administradores que instalam o G2 Series ISR de Cisco que não tem as ferramentas de segurança adaptáveis de Cisco (ASA) em suas redes escolhem utilizar a funcionalidade da reorientação ISR CWs (anteriormente ScanSafe) a fim aproveitar-se da solução CWs para a filtração da Web. Como parte dessa solução, a maioria de administradores igualmente querem utilizar a infraestrutura atual AD a fim enviar a informação de identidade do usuário às torres CWs para fins do reforço de política do usuário ou grupo-baseado para as políticas de filtragem da Web no portal CWs.

O conceito total é similar à integração entre o ASA e o agente de diretório do contexto (CDA), com algumas diferenças. A maioria de diferença notável é que o ISR não mantém realmente um base de dados passivo do mapeamento USER-à-IP, assim que os usuários devem passar através de algum tipo de autenticação a fim transitar pelo ISR e enviar a informação do usuário ou do grupo ao portal CWs.

> Dica: Refira a seção dos **métodos de autenticação d**este documento para obter mais informações sobre das diferenças entre os vários métodos de autenticação que estão disponíveis.

Quando a parcela da reorientação CWs da configuração que está descrita neste documento for relativamente direta, alguns administradores puderam encontrar a dificuldade com tentativas de configurar a parcela da autenticação. Esta parcela trabalha com o comando da **admissão IP** que provê as instruções de autenticação dos servidores ldap e do Authentication, Authorization, and Accounting (AAA) que devem igualmente ser configuradas. A finalidade deste documento é fornecer operadores de rede uma fonte de referência detalhada a fim configurar ou pesquisar defeitos as admissões IP e parcelas LDAP desta configuração no G2 Series ISR de Cisco.

Configurar

Use a informação que é descrita nesta seção a fim configurar Cisco ISR.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Configurar o LDAP

Termine estas etapas a fim configurar as propriedades LDAP dos server AAA:

1. Configurar um mapa do atributo LDAP a fim forçar o username que é incorporado pelo usuário para combinar a propriedade do **sAMAccountName no** AD:
   ```
   C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
    username
   C-881(config-attr-map)#map type sAMAccountName username
   ```
   Nota: Esta configuração é exigida porque o atributo do **sAMAccountName** é um valor exclusivo no AD, ao contrário do atributo do Common Name (CN), que é usado de outra maneira a fim combinar à revelia. Por exemplo, pode haver umas múltiplas instâncias de *John Smith no* AD, mas pode somente haver um usuário com o **sAMAccountName do** *jsmith*, que é igualmente o fazer logon da conta de usuário. Outras contas de *John Smith* têm **sAMAccountNames** tais como *jsmith1* ou *jsmith2*.
   O comando dos **atributos do ldap da mostra** pode igualmente ser usado a fim ver uma lista dos atributos LDAP e dos atributos associados AAA.

2. Configurar o grupo de servidor ldap:
   ```
   C-881(config)#aaa group server ldap LDAP_GROUP
   C-881(config-ldap-sg)#server DC01
   ```
3. Configurar os servidores ldap:
   ```
   C-881(config)#ldap server DC01
   C-881(config-ldap-server)# ipv4 10.10.10.150
   C-881(config-ldap-server)#attribute map ldap-username-map
   C-881(config-ldap-server)# bind authenticate root-dn CN=Csco_Service,CN=Users,
   DC=lab,DC=cisco,DC=com password Cisco12345!

   C-881(config-ldap-server)#base-dn DC=lab,DC=cisco,DC=com
   C-881(config-ldap-server)#search-filter user-object-type top
   C-881(config-ldap-server)#authentication bind-first
   ```

Esta configuração geralmente não exige a alteração, a menos que houver uma necessidade de executar um busca-filtro feito sob encomenda. Somente os administradores que são bem versados no LDAP e sabem entrar corretamente esta informação devem utilizar filtros feitos sob encomenda da busca. Se você é incerto sobre o filtro da busca que deve ser usado, use simplesmente o filtro descrito; encontra os usuários em um ambiente normal AD.

Uma outra parcela da configuração ldap que igualmente exige a atenção cuidadosa detalhar é os nomes destacados (DN) que são exigidos nos comandos ligamento-autenticar-raiz-**dn** e base-**dn**. Estes devem ser entrados exatamente enquanto aparecem no servidor ldap, ou as perguntas LDAP falham. Além, o comando base-**dn** deve ser o mais baixo parte da árvore LDAP, onde todos os usuários que são autenticados residem.

Considere a encenação em que o comando base-**dn na** configuração precedente é alterado como este:

```
base-dn OU=TestCompany,DC=lab,DC=cisco,DC=com
```

Neste caso, a pergunta para os usuários que são incluídos nos **cn=Users, DC=lab, dc=cisco, dc=com** não retorna nenhum resultado, desde que o servidor ldap procura somente a unidade organizacional de TestCompany (OU) e os objetos da criança dentro dele. Em consequência, a autenticação falha sempre para aqueles usuários até que estejam movidos no TestCompany OU ou em seu subtree, ou se o comando base-**dn** está alterado a fim o incluir na pergunta.

Dica: Refira a **determinação aos objetos DN no AD - ADSI editam a** seção deste documento para detalhes sobre como determinar os DN apropriados para a base e os comandos root.

Configurar o AAA

Agora que os servidores ldap são configurados, você deve provê-los nas indicações correspondentes AAA que são usadas pelo processo da admissão IP:

```
C-881(config)#aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
C-881(config)#aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

Nota: Se estes comandos não estão disponíveis, a seguir o **comando aaa new-model** pôde precisar de ser inscrito a fim permitir esta funcionalidade AAA porque não é permitida à revelia.

Configurar a admissão IP

A parcela da admissão IP provocam um processo que alerte o usuário para a autenticação (ou executa a autenticação transparente) e executam então as perguntas LDAP baseadas nas credenciais do usuário e os servidores AAA que são definidos na configuração. Se os usuários são autenticados com sucesso, a informação de identidade do usuário então está puxada pelo processo da índice-varredura e mandada às torres CWs, junto com o fluxo reorientado. O processo da admissão IP não é ativado até que o ***comando name da* admissão IP** esteja inscrito na interface de ingresso do roteador. Consequentemente, esta parcela da configuração pode ser executada sem nenhum impacto do tráfego.

```
C-881(config)#ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm
C-881(config)#ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH
```

Permita a admissão IP

Está aqui a configuração que é usada a fim permitir a admissão IP:

Nota: Isto força os usuários a ser autenticado, que causa a interrupção do fluxo de tráfego se a autenticação falha.

```
C-881(config)#int vlan301 (internal LAN-facing interface)
C-881(config-if)#ip admission SCANSAFE_ADMISSION
```

Host internos isentos da autenticação

Alguns administradores puderam desejar isentar por razões diversas alguns host internos do processo de autenticação. Por exemplo, pôde ser indesejável para os servidores internos ou os dispositivos que não são capazes do NTLM ou da autenticação básica a ser afetados pelo processo das admissões IP. Nestes exemplos, um Access Control List (ACL) pode ser aplicado à configuração da admissão IP a fim impedir que o host específico IPs ou as sub-redes provoquem a admissão IP.

Neste exemplo, o host interno 10.10.10.150 é isento da exigência da autenticação, quando a autenticação for exigida ainda para todos anfitriões restantes:

```
C-881(config)#ip access-list extended NO_ADMISSION
C-881(config-ext-nacl)#deny ip host 10.10.10.150 any
C-881(config-ext-nacl)#permit ip any any
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm list NO_ADMISSION
```

Permita o Server do HTTP no ISR

Exige-se que você permite o Server do HTTP a fim interceptar as sessões de HTTP e iniciar o processo de autenticação:

```
Ip http server
Ip http secure-server
```

> Nota: O servidor seguro do HTTP de IP é precisado somente se a reorientação ao HTTPS para a autenticação é exigida.

Configurar a reorientação CWs

Está aqui uma configuração sumária básica para a reorientação CWs:

```
Ip http server
Ip http secure-server
```

Termine a configuração de exemplo

Esta seção fornece exemplos de configuração completos para as seções anterior.

LDAP

```
Ip http server
Ip http secure-server
```

AAA

```
Ip http server
Ip http secure-server
```

Admissão IP

```
Ip http server
Ip http secure-server
```

Server do HTTP

```
Ip http server
Ip http secure-server
```

Índice-varredura e CWs

```
Ip http server
Ip http secure-server
```

Determine os objetos DN no AD - ADSI editam

Se necessário, é possível consultar uma estrutura AD a fim olhar acima DN para o uso com a base do usuário ou da busca do grupo. Os administradores podem usar uma ferramenta chamada o *ADSI editam* que é construído em controladores de domínio AD. A fim abrir o ADSI edite, escolha o **Iniciar > Executar no** controlador de domínio AD e incorpore **adsiedit.msc.**

Uma vez que o ADSI Edit está aberto, clicar com o botão direito todo o objeto, tal como um OU, grupo, ou usuário, e escolha **propriedades** a fim ver o DN desse objeto. A corda DN pode então facilmente ser copiada e colado à configuração de roteador a fim evitar todos os erros tipográficos. Esta imagem ilustra o processo:

Métodos de autenticação

Há quatro tipos diferentes de métodos de autenticação disponíveis que usam a admissão IP, e são entendidos mal frequentemente, especialmente a diferença entre o NTLM transparente e passivo. As próximas seções descrevem as diferenças entre estes tipos de autenticação.

NTLM ativo

O método de autenticação de NTLM do active alerta usuários para a autenticação quando a autenticação de NTLM transparente falha. Isto é geralmente devido ao fato que o navegador cliente não apoia a autenticação integrada de Microsoft Windows ou porque o usuário registrado na estação de trabalho com credenciais locais (do NON-domínio). A autenticação de NTLM ativa executa perguntas LDAP ao controlador de domínio a fim assegurar-se de que as credenciais fornecidas estejam corretas.

> Nota: Com todos os tipos de autenticação de NTLM, as credenciais não são passadas através do texto claro. Contudo, a versão 1 NTLM (NTLMv1) tem vulnerabilidades bem documentados. O ISR é NTLMv2-capable, embora à revelia, umas versões mais velhas de Microsoft Windows possam negociar através do NTLMv1. Este comportamento é dependente das políticas de autenticação AD.

NTLM transparente

A autenticação de NTLM transparente ocorre quando um usuário é registrado na estação de trabalho com credenciais do domínio, e aquelas credenciais estão passadas transparentemente pelo navegador ao IOS Router. O IOS Router executa então uma pergunta LDAP a fim validar as credenciais do usuário. Este é geralmente o formulário de autenticação o mais desejado para esta

característica.

Autenticação básica (através do HTTP no texto claro)

Este formulário de autenticação está usado tipicamente como um mecanismo de recuo quando a autenticação de NTLM falha ou não é possível para clientes tais como Macintosh, dispositivos Linux-baseados, ou dispositivos móveis. Com este método, se o servidor seguro HTTP não é permitido, a seguir estas credenciais são passadas através do HTTP no texto claro (muito incerto).

NTLM passivo

As credenciais passivas dos pedidos da autenticação de NTLM dos usuários mas não autenticam realmente o usuário contra o controlador de domínio. Quando isto puder evitar os problemas LDAP-relacionados onde as perguntas falham contra o controlador de domínio, igualmente expõe usuários no ambiente a um risco de segurança. Se a autenticação transparente falha ou não é possível, a seguir os usuários estão alertados para credenciais. Contudo, o usuário pode incorporar todas as credenciais que escolherem, que são passadas à torre CWs. Em consequência, as políticas não puderam ser aplicadas apropriadamente.

Por exemplo, o usuário A pode usar Firefox (que à revelia não permite o NTLM transparente sem configuração adicional) e incorporar o username do usuário B com toda a senha, e as políticas para o usuário B são aplicadas ao usuário A. A exposição do risco pode ser abrandada se os usuários todos são forçados a usar os navegadores que apoiam a autenticação de NTLM transparente, mas na maioria dos casos, o uso da autenticação passiva não é recomendado.

Sequência de mensagem para a autenticação de NTLM ativa

Está aqui a sequência do mensagem completa para o método de autenticação de NTLM ativo:

```
Browser -->  ISR : GET / google.com
Browser <--  ISR : 302 Page moved http://1.1.1.1/login.html
Browser -->  ISR : GET /login.html 1.1.1.1
Browser <--  ISR : 401 Unauthorized..Authenticate using NTLM
Browser -->  ISR : GET /login.html + NTLM Type-1 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-1 msg
```

O ISR copia o tipo-1 mensagem do HTTP ao LDAP, byte-por-byte sem nenhuma alteração dos dados.

```
ISR     <--  AD  : LDAP Bind Response + NTLM Type-2 msg
Browser <--  ISR : 401 Unauthorized + NTLM Type-2 msg
```

A mensagem do Tipo 2 é copiada igualmente byte-por-byte do LDAP ao HTTP. Assim, no PCAP, parece originar de **1.1.1.1**, mas o índice real é do AD.

```
Browser -->  ISR : GET /login.html + NTLM Type-3 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-3 msg
ISR     <--  AD  : LDAP Bind response - Success
Browser <--  ISR : 200OK + redirect to google.com
```

Quando o NTLM ativo é configurado, o ISR não interfere durante a troca NTLM. Contudo, se o NTLM passivo é configurado, a seguir o ISR gerencie sua própria mensagem do Tipo 2.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Comandos show

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Você pode usar estes **comandos show** a fim pesquisar defeitos sua configuração:

- **mostre o esconderijo da admissão IP**
- **mostre o estado da admissão IP**
- **mostre estatísticas da admissão IP**
- **mostre o servidor ldap todo**

Comandos debug

> Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Estão aqui alguns comandos debug úteis que você pode usar a fim pesquisar defeitos sua configuração:

- **debugar o ldap todo** - Este comando pode ser usado a fim descobrir a razão que a autenticação falha.
- **debugar o detalhe da admissão IP** - Este comando é muito verboso e processo intensivo de cpu. Cisco recomenda que você o usa somente com únicos clientes de teste que provocam a admissão IP.
- **debugar o ntlm da admissão IP** - Este comando pode ser usado a fim descobrir a razão que o processo da admissão IP está provocado.
- **debugar o httpd da admissão IP**
- **debugar a transação do HTTP de IP**

- debugar o debug aaa authorization da autenticação aaa

Problemas comuns

Esta seção descreve alguns problemas comuns que são encontrados com a configuração descrita neste documento.

A admissão IP não intercepta pedidos do HTTP

Esta edição torna-se evidente quando você vê a saída do **comando statistics da admissão da mostra IP**. A saída não mostra a intercepção de nenhuns pedidos do HTTP:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

Soluções possíveis

Há duas soluções possíveis a esta edição. O primeiro é verificar que o **server do HTTP de IP** está permitido.

Se o Server do HTTP para o ISR não é permitido, a seguir os disparadores da admissão IP mas interceptam nunca realmente a sessão de HTTP. Consequentemente, alerta para a autenticação. Nesta situação, não há nenhuma saída para o **comando cache da admissão da mostra IP**, mas muitos retornos destas linhas são considerados na saída do **comando detail da admissão debugar IP**:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

A segunda solução a esta edição é verificar que o endereço IP de Um ou Mais Servidores Cisco ICM NT do usuário não é isento do ACL na configuração da admissão IP.

Os usuários recebem um erro *404 não encontrado*

Esta edição é observada quando os usuários são reorientados para a autenticação, e um erro **404 não encontrado** ocorre no navegador.

Solução possível

Assegure-se de que o nome no virtual-**host ISR_PROXY de 1.1.1.1 do IP virtual da admissão IP** possa com sucesso resolver com o server do Domain Name System (DNS) do cliente. Neste caso, o cliente executa uma pergunta DNS para **ISR_PROXY.lab.cisco.com** desde que **lab.cisco.com** é o nome de domínio totalmente qualificado (FQDN) do domínio a que a estação de trabalho é juntada. Se a pergunta DNS falha, o cliente envia uma pergunta da resolução de nome

do Multicast do link local (LLMNR), seguida por uma pergunta de NETBIOS que seja transmissão à sub-rede local.

Se todas estas tentativas da definição falham, a seguir uns **404 não encontrados** ou o **internet explorer não podem indicar o** erro do **Web page** estão indicados no navegador.

A autenticação de usuário falha quando alertada

Isto pode ser causado por várias razões mas é relacionado geralmente à configuração ldap no ISR, ou a uma comunicação entre o ISR e o servidor ldap. No ISR, o sintoma está observado geralmente quando os usuários estão colados no **estado de INIT a** admissão IP está provocada uma vez que:

```
C-881(config)#do show ip admi cac
Authentication Proxy Cache
Client Name N/A, Client IP 10.10.10.152, Port 56674, timeout 60,
 Time Remaining 2, state INIT
```

Causas comuns

Estas são as causas comum para esta edição:

- Um username e/ou uma senha inválidos são incorporados pelo usuário para a autenticação ativa.
- **Um base-dn** inválido é usado na configuração ldap, que conduz às buscas que não retornam nenhum resultado.
- Uma autenticação inválida raiz-**dn do** ligamento é configurada para o username ou a senha, que fazem com que o ligamento LDAP falhe.
- Uma comunicação entre o ISR e o servidor ldap falha. Verifique que o servidor ldap escuta na porta TCP especificada uma comunicação LDAP e que todos os Firewall entre os dois permitem o tráfego.
- Um filtro inválido da busca não causa nenhum resultado para a busca LDAP.

Pesquise defeitos o LDAP

A melhor maneira de determinar a razão que a autenticação falha é utilizar os comandos debug LDAP no ISR. Mantenha na mente que debuga pode ser cara e perigosa ser executado em um ISR se há umas saídas excessivas, e podem fazer com que o roteador pendure e exija um ciclo duro da potência. Isto é especialmente verdadeiro para as Plataformas mais baixo da gama.

A fim pesquisar defeitos, Cisco recomenda que você aplica um ACL à regra da admissão IP a fim sujeitar somente uma única estação de trabalho do teste na rede à autenticação. Esta maneira, debuga pode ser permitida com um risco mínimo de impacto negativo à capacidade do roteador para passar o tráfego.

Dica: Refira os **host internos isentos da** seção da **autenticação d**este documento para obter mais informações sobre do aplicativo de um ACL à configuração das admissões IP.

Quando você pesquisa defeitos problemas LDAP-relacionados, é útil compreender as etapas em que o LDAP processa pedidos do ISR.

Etapas de nível elevado para a autenticação LDAP

Estão aqui as etapas de nível elevado para a autenticação LDAP:

1. Abra a conexão ao servidor ldap na porta especificada. A porta padrão é **TCP 389**.
2. O ligamento ao servidor ldap com o ligamento autentica o usuário raiz-**dn** e a senha.
3. Execute a busca LDAP, com o uso do base-**dn** e dos busca-filtros que são definidos na configuração ldap, para o usuário que tenta autenticar.
4. Obtenha os resultados LDAP do servidor ldap e crie uma entrada de cache da admissão IP para o usuário se a autenticação é bem sucedida, ou o reprompt para credenciais no caso de uma falha de autenticação.

Análise do resultado do debug LDAP

Estes processos podem ser vistos na saída do **comando all do ldap debugar**. Esta seção fornece um exemplo do resultado do debug LDAP para uma autenticação que falhe devido a um base-**dn** inválido. Reveja o resultado do debug e os comentários associados, que descrevem as parcelas da saída que mostram onde as etapas acima mencionadas puderam encontrar a falha.

```
*Jan 30 20:51:50.818: LDAP: LDAP: Queuing AAA request 23 for processing
*Jan 30 20:51:50.818: LDAP: Received queue event, new AAA request
*Jan 30 20:51:50.818: LDAP: LDAP authentication request
*Jan 30 20:51:50.818: LDAP: Username sanity check failed
*Jan 30 20:51:50.818: LDAP: Invalid hash index 512, nothing to remove
*Jan 30 20:51:50.818: LDAP: New LDAP request
*Jan 30 20:51:50.818: LDAP: Attempting first next available LDAP server
*Jan 30 20:51:50.818: LDAP: Got next LDAP server :DC01
*Jan 30 20:51:50.818: LDAP: Free connection not available. Open a new one.
*Jan 30 20:51:50.818: LDAP: Opening ldap connection
( 10.10.10.150, 389 )ldap_open
```

A parcela da saída mostrada em corajoso indica que esta não é uma edição da camada de rede, desde que o a conexão é aberta com sucesso.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

O ligamento autenticar-dn está correto nesta saída. Se a configuração está incorreta para esta, a seguir as falhas do ligamento estão consideradas.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
```

```
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

A parcela da saída mostrada em corajoso indica que todas as operações do ligamento são bem sucedidas e continua procurar pelo usuário real.

```
*Jan 30 20:51:51.854: LDAP: SASL NTLM authentication done..Execute search
*Jan 30 20:51:51.854: LDAP: Next Task: Send search req
*Jan 30 20:51:51.854: LDAP: Transaction context removed from list[ldap reqid=15]
*Jan 30 20:51:51.854: LDAP: Dynamic map configured
*Jan 30 20:51:51.854: LDAP: Dynamic map found for aaa type=username
*Jan 30 20:51:51.854: LDAP: Ldap Search Req sent
ld 2293572544
base dn     dc=lab1,dc=cisco,dc=comscope       2
filter (&(objectclass=top)(sAMAccountName=testuser5))
ldap_req_encode
put_filter "(&(objectclass=top)(sAMAccountName=testuser5))"
put_filter: AND
put_filter_list "(objectclass=top)(sAMAccountName=testuser5)"
put_filter "(objectclass=top)"
put_filter: simple
put_filter "(sAMAccountName=testuser5)"
put_filter: simple
Doing socket write
*Jan 30 20:51:51.854: LDAP: lctx conn index = 2
```

A primeira linha (mostrada em corajoso) indica que o resultado do debug da busca LDAP começa. Também, observe que o controlador de domínio base-**dn** deve ser configurado para o **laboratório**, não **lab1**.

```
*Jan 30 20:51:52.374: LDAP: LDAP Messages to be processed: 1
*Jan 30 20:51:52.374: LDAP: LDAP Message type: 101
*Jan 30 20:51:52.374: LDAP: Got ldap transaction context from reqid
16ldap_parse_result
*Jan 30 20:51:52.374: LDAP: resultCode: 10 (Referral)
*Jan 30 20:51:52.374: LDAP: Received Search Response resultldap_parse_result
ldap_err2string
*Jan 30 20:51:52.374: LDAP: Ldap Result Msg: FAILED:Referral, Result code =10
*Jan 30 20:51:52.374: LDAP: LDAP Search operation result : failedldap_msgfree
*Jan 30 20:51:52.374: LDAP: Closing transaction and reporting error to AAA
*Jan 30 20:51:52.374: LDAP: Transaction context removed from list
[ldap reqid=16]
*Jan 30 20:51:52.374: LDAP: Notifying AAA: REQUEST FAILED
```

A parcela da saída mostrada em corajoso indica que a busca não retornou nenhum resultado, que é neste caso devido a um base-**dn** inválido.

RFC 4511

RFC 4511 (**Lightweight Directory Access Protocol (LDAP): O protocolo**) fornece a informação sobre as mensagens do código do resultado para o LDAP e a outra informação protocolo-relacionada LDAP, que podem ser providas através do Web site IETF.