

Como usar o LDAP aceite a pergunta para validar os receptores de mensagens de entrada usando o microsoft active directory (LDAP)?

Índice

[Pergunta:](#)

Pergunta:

Como usar o LDAP aceite a pergunta para validar os receptores de mensagens de entrada usando o microsoft active directory (LDAP)?

Nota: O exemplo seguinte integra com um desenvolvimento padrão do microsoft active directory, embora os princípios possam ser aplicados a muitos tipos de aplicações LDAP.

Você criará primeiramente uma entrada do servidor ldap, que no ponto você deve especificar seu servidor de diretório assim como a pergunta que a ferramenta de segurança do email executará. A pergunta então é permitida ou aplicada em seu novo ouvinte (público). Estes ajustes do servidor ldap podem ser compartilhados por ouvintes diferentes e outras partes da configuração tais como a quarentena do utilizador final alcançam.

Para facilitar a configuração das perguntas LDAP em seu dispositivo de IronPort, nós recomendamos que você usa um navegador LDAP, que permita que você tome olhar em seu esquema assim como todos os atributos em cima de que você pode perguntar contra.

Para Microsoft Windows, você pode usar-se:

Para Linux ou UNIX, você pode usar o comando do `ldapsearch`.

Primeiramente, você precisa de definir o servidor ldap para perguntar. Neste exemplo, a alcunha de "PublicLDAP" é dada para o servidor ldap de *myldapservers.example.com*. As perguntas são dirigidas à porta TCP 389 (o padrão).

NOTA: Se sua aplicação do diretório ativo contém subdomínios, você não poderá perguntar para usuários em um domínio secundário usando a base DN do domínio da raiz. Contudo, ao usar o diretório ativo, você pode igualmente perguntar o LDAP contra o server global do catálogo (GC) na porta TCP 3268. O GC contém a informação parcial para objetos do *all* na floresta do diretório ativo e fornece referências ao subdomínio na pergunta quando a informação adicional é exigida. Se você não pode "encontrar" usuários em seus subdomínios, deixe a base DN na raiz e

ajuste o IronPort para usar a porta do GC.

GUI:

1. Crie um perfil novo do servidor ldap com os valores situados previamente de seu servidor de diretório (a administração do sistema > LDAP). Por exemplo: Nome do perfil de servidor: *PublicLDAP* Nome de host: *myldapserver.example.com* Método de autenticação: *Senha do uso: Habilitado* Nome de usuário: *cn=ESA, cn=Users, dc=example, dc=com* Senha: *senha* Tipo de servidor: *Diretório ativo* Porta: *3268* BaseDN: *dc=example, dc=com* Certifique-se usar do “o botão dos server teste” para verificar seus ajustes antes de continuar. A saída bem sucedida deve olhar como:

```
Connecting to myldapserver.example.com at port 3268
Bound successfully with DN CN=ESA,CN=Users,DC=example,DC=com
Result: succeeded
```

2. Use a mesma tela para definir o LDAP aceite a pergunta. O exemplo seguinte verifica o endereço destinatário contra os atributos mais comuns, “correio” OU “proxyAddresses”: Nome: *PublicLDAP*. *acceptQueryString: ((mail= {a}) (proxyAddresses=smtp: {a}))* Você pode usar do “o botão da pergunta teste” para verificar seus resultados dos retornos da pergunta da busca para uma conta válida. A saída bem sucedida que procura pelo endereço “esa.admin@example.com” da conta de serviço deve olhar como:

```
Query results for host:myldapserver.example.com
Query (mail=esa.admin@example.com) >to server PublicLDAP (myldapserver.example.com:3268)
Query (mail=esa.admin@example.com) lookup success, (myldapserver.example.com:3268) returned
1 results
Success: Action: Pass
```

3. Aplique este novo aceite a pergunta ao ouvinte de entrada (rede > ouvintes). Expanda as perguntas das opções LDAP > aceite, e escolhem sua pergunta *PublicLDAP.accept*.
4. Finalmente, comprometa as mudanças para permitir estes ajustes.

CLI:

1. Primeiramente, você usa o comando do *ldapconfig* definir um servidor ldap para que o dispositivo ligue a, e as perguntas para a aceitação destinatária (subcommand do *ldapaccept*), distribuindo (subcommand *ldaprouting*), e masquerading (subcommand do *disfarce*) são configuradas.

```
mail3.example.com> ldapconfig
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
[ ]> new
Please create a name for this server configuration (Ex: "PublicLDAP"):
```

```

[ ]> PublicLDAP
Please enter the hostname:
[ ]> myldapserver.example.com
Use SSL to connect to the LDAP server? [N]> n
Please enter the port number:
[389]> 389
Please enter the base:
[dc=example,dc=com]>dc=example,dc=com
Select the authentication method to use for this server configuration:
1. Anonymous
2. Password based
[1]> 2
Please enter the bind username:
[cn=Anonymous]>cn=ESA,cn=Users,dc=example,dc=com
Please enter the bind password:
[ ]> password
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com

```

2. Em segundo, você precisa de definir a pergunta para executar contra o servidor ldap que você apenas configurou.

```

Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing. - MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
[ ]> ldapaccept
Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept
Enter the LDAP query string:
[(mailLocalAddress= {a})]>(|(mail={a})(proxyAddresses=smtp:{a}))
Please enter the cache TTL in seconds:
[900]>
Please enter the maximum number of cache entries to retain:
[10000]>
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept

```

3. Uma vez que você configurou a pergunta LDAP, você precisa de aplicar a política de LDAPaccept a seu ouvinte de entrada.

```

example.com> listenerconfig
Currently configured listeners:
1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[ ]> edit
Enter the name or number of the listener you wish to edit.
[ ]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:

```

```
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS >- Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be
accepted or bounced/dropped.
- LDAPROUTING - Configure an LDAP query to reroute messages.
[> ldapaccept Available Recipient Acceptance Queries
1. None
2. PublicLDAP.ldapaccept
[1]> 2
Should the recipient acceptance query drop recipients or bounce them?
NOTE: Directory Harvest Attack Prevention may cause recipients to be
dropped regardless of this setting.
1. bounce
2. drop
[2]> 2
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: ldapaccept (PublicLDAP.ldapaccept)
```

4. Para ativar as mudanças feitas ao ouvinte, comprometa suas mudanças.