¿Cómo utilizar el LDAP valide la interrogación para validar a los beneficiarios de los mensajes entrantes usando el Microsoft Active Directory (LDAP)?

Contenido

Pregunta:

¿Cómo utilizar el LDAP valide la interrogación para validar a los beneficiarios de los mensajes entrantes usando el Microsoft Active Directory (LDAP)?

Nota: El siguiente ejemplo integra con un despliegue estándar del Microsoft Active Directory, aunque los principios se puedan aplicar a muchos tipos de implementaciones LDAP.

Usted primero creará una entrada del servidor LDAP, momento en el cual que usted debe especificar su Servidor del directorio así como la interrogación que el dispositivo de seguridad del correo electrónico realice. La interrogación después se habilita o se aplica en su módulo de escucha (público) entrante. Estas configuraciones del servidor LDAP se pueden compartir por diversos módulos de escucha y otras partes de la configuración tal como acceso de la cuarentena del usuario final.

Para facilitar la configuración de las interrogaciones LDAP en su dispositivo de IronPort, recomendamos que usted utiliza a un navegador LDAP, que permite que usted tome una mirada en su esquema así como todos los atributos sobre contra los cuales usted pueda preguntar.

Para Microsoft Windows, usted puede utilizar:

Para Linux o UNIX, usted puede utilizar el comando del `ldapsearch`.

Primero, usted necesita definir al servidor LDAP para preguntar. En este ejemplo, el apodo de “PublicLDAP” se da para el servidor LDAP de *myldapserver.example.com*. Las interrogaciones se dirigen al puerto TCP 389 (el valor por defecto).

NOTA: Si su aplicación del Active Directory contiene el subdomains, usted no podrá preguntar para los usuarios en un dominio sub usando la base DN del dominio de la raíz. Sin embargo, al usar el Active Directory, usted puede también preguntar el LDAP contra el servidor global del

catálogo (CROMATOGRAFÍA GASEOSA) en el puerto TCP 3268. La CROMATOGRAFÍA GASEOSA contiene la información parcial para los objetos del *all* en el bosque del Active Directory y proporciona las remisiones al subdomain en la pregunta cuando se requiere la Más información. Si usted no puede “encontrar” a los usuarios en su subdomains, deje la base DN en la raíz y fije el IronPort para utilizar el puerto de la CROMATOGRAFÍA GASEOSA.

GUI:

1. Cree un nuevo perfil del servidor LDAP con los valores situados previamente de su Servidor del directorio (administración del sistema > LDAP). Por ejemplo: Nombre del perfil del servidor: *PublicLDAP*Nombre del host: *myldapserver.example.com*Método de autentificación: *Contraseña del uso: Habilitado*Nombre de usuario: *cn=ESA, cn=Users, dc=example, dc=com*Contraseña *contraseña*Tipo de servidor: *Active Directory*Puerto: *3268*BaseDN: *dc=example, dc=com*Aseegurese utilizar “el botón de los servidores de la prueba” para verificar sus configuraciones antes de continuar. La salida acertada debe parecer:

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

2. Utilice la misma pantalla para definir el LDAP validan la interrogación. El siguiente ejemplo marca el direccionamiento receptor contra los atributos mas comunes, “correo” O los “proxyAddresses”:Nombre: *PublicLDAP.accept*QueryString: *(|(mail= {a}) (proxyAddresses=smtp: {a}))*Usted puede utilizar “el botón de la interrogación de la prueba” para verificar sus resultados de las devoluciones de la interrogación de la búsqueda para una cuenta válida. La salida acertada que busca para el direccionamiento “esa.admin@example.com” de la Cuenta de servicio debe parecer:

```
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 nuevo validan la interrogación al módulo de escucha entrante (red > módulos de escucha). Amplíe las interrogaciones de las opciones LDAP > validan, y eligen su interrogación PublicLDAP.accept.

4. Finalmente, confíe los cambios para habilitar estas configuraciones.

CLI:

1. **Primero, usted utiliza el comando del *ldapconfig* de definir a un servidor LDAP para que el dispositivo ate a, y las interrogaciones para la aceptación receptora (submandato del ldapaccept), ruteando (submandato ldaprouting), y disfrazándose (submandato de la mascarada) se configuran.**

```
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. En segundo lugar, usted necesita definir la interrogación para realizarse contra el servidor LDAP que usted acaba de configurar.

```
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. Una vez que usted ha configurado la interrogación LDAP, usted necesita aplicar la directiva de LDAPaccept a su módulo de escucha entrante.

```
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 activar los cambios realizados al módulo de escucha, confíe sus cambios.