Come utilizzare LDAP Accept Query per convalidare i destinatari dei messaggi in ingresso utilizzando Microsoft Active Directory (LDAP)?

Sommario

Domanda:

Come utilizzare LDAP Accept Query per convalidare i destinatari dei messaggi in ingresso utilizzando Microsoft Active Directory (LDAP)?

Nota: Nell'esempio seguente viene eseguita l'integrazione con una distribuzione standard di Microsoft Active Directory, sebbene i principi possano essere applicati a molti tipi di implementazioni LDAP.

Verrà innanzitutto creata una voce relativa al server LDAP. A questo punto sarà necessario specificare il server di elenchi in linea e la query che verrà eseguita da Email Security Appliance. La query viene quindi abilitata o applicata al listener in ingresso (pubblico). Queste impostazioni del server LDAP possono essere condivise da diversi listener e da altre parti della configurazione, ad esempio l'accesso dell'utente finale in quarantena.

Per facilitare la configurazione delle query LDAP sull'accessorio IronPort, è consigliabile utilizzare un browser LDAP, che consente di esaminare lo schema e tutti gli attributi su cui è possibile eseguire query.

Per Microsoft Windows è possibile utilizzare:

Per Linux o UNIX, è possibile utilizzare `ldapsearch`

Innanzitutto, è necessario definire il server LDAP su cui eseguire la query. In questo esempio, il soprannome "PublicLDAP" è dato per il server LDAP *myldapserver.example.com*. Le query vengono indirizzate alla porta TCP 389 (impostazione predefinita).

NOTA: Se l'implementazione di Active Directory contiene sottodomini, non sarà possibile eseguire query per gli utenti in un sottodominio utilizzando il DN di base del dominio radice. Tuttavia, quando si utilizza Active Directory, è possibile eseguire una query su LDAP per il server di catalogo globale (GC) sulla porta TCP 3268. Il catalogo globale contiene informazioni parziali per *tutti* gli oggetti nella foresta di Active Directory e fornisce riferimenti al sottodominio in questione

quando sono necessarie ulteriori informazioni. Se non è possibile "trovare" gli utenti nei sottodomini, lasciare il DN di base nella radice e impostare IronPort per utilizzare la porta GC.

GUI:

1. Creare un nuovo profilo del server LDAP con i valori presenti in precedenza nel server delle directory (Amministrazione sistema > LDAP). Ad esempio: Nome profilo server: *LDAP pubblico*Nome host: *myldapserver.example.com*Metodo di autenticazione: *Password: Attivato*Nome utente:*cn=ESA,cn=Users,dc=esempio,dc=com*Password: *password*Tipo server: *Active Directory*Port: *3268*BaseDN:*dc=esempio,dc=com*Prima di continuare, utilizzare il pulsante "Test server(s)" per verificare le impostazioni. L'output corretto dovrebbe avere il seguente aspetto:

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

2. Utilizzare la stessa schermata per definire la query di accettazione LDAP. Nell'esempio seguente l'indirizzo del destinatario viene confrontato con gli attributi più comuni, ovvero "mail" O "proxyAddresses":Nome: *LDAPpubblico.accetta*StringaQuery:*(|(mail={a})(proxyAddresses=smtp:{a}))*Èpossibile utilizzare il pulsante "Test query" per verificare che la query di ricerca restituisca risultati per un account valido. L'output della ricerca dell'indirizzo dell'account del servizio "esa.admin@example.com" dovrebbe essere simile al seguente:

```
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. Applica questa nuova query di accettazione al listener in entrata (Rete > Listener). Espandere le opzioni LDAP Query > Accetta e scegliere la query PublicLDAP.accept.

4. Eseguire infine il commit delle modifiche per abilitare queste impostazioni.

CLI:

1. **Innanzitutto, è necessario utilizzare il comando *ldapconfig* per definire un server LDAP a cui l'accessorio deve collegarsi e configurare le query per l'accettazione del destinatario (sottocomando ldapaccept), il routing (sottocomando ldaprouting) e il mascheramento (sottocomando masquerade).**

```
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. In secondo luogo, è necessario definire la query da eseguire sul server LDAP appena configurato.

```
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. Dopo aver configurato la query LDAP, è necessario applicare il criterio LDAPaccept al listener in entrata.

```
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. Per attivare le modifiche apportate al listener, eseguire il commit delle modifiche.