Wie werden LDAP Accept Query (LDAP Accept-Abfrage) verwendet, um die Empfänger eingehender Nachrichten mithilfe von Microsoft Active Directory (LDAP) zu validieren?

Inhalt

Frage:

Wie werden LDAP Accept Query (LDAP Accept-Abfrage) verwendet, um die Empfänger eingehender Nachrichten mithilfe von Microsoft Active Directory (LDAP) zu validieren?

Hinweis: Das folgende Beispiel kann in eine Microsoft Active Directory-Standardbereitstellung integriert werden, obwohl die Prinzipien auf viele Arten von LDAP-Implementierungen angewendet werden können.

Sie erstellen zunächst einen LDAP-Servereintrag, an dem Sie Ihren Verzeichnisserver sowie die Abfrage angeben müssen, die die E-Mail-Security-Appliance ausführen soll. Die Abfrage wird dann aktiviert oder auf den eingehenden (öffentlichen) Listener angewendet. Diese LDAP-Servereinstellungen können von verschiedenen Listenern und anderen Teilen der Konfiguration, z. B. dem Quarantänezugriff für Endbenutzer, gemeinsam genutzt werden.

Um die Konfiguration der LDAP-Abfragen auf Ihrer IronPort-Appliance zu vereinfachen, empfehlen wir die Verwendung eines LDAP-Browsers, mit dem Sie das Schema sowie alle Attribute überprüfen können, auf die Sie abfragen können.

Für Microsoft Windows können Sie Folgendes verwenden:

Für Linux oder UNIX können Sie die `ldapsearch` Befehl.

Zunächst müssen Sie den LDAP-Server für die Abfrage definieren. In diesem Beispiel wird der Spitzname "PublicLDAP" für den *myldapserver.example.com* LDAP-Server angegeben. Abfragen werden an den TCP-Port 389 (der Standardwert) weitergeleitet.

HINWEIS: Wenn Ihre Active Directory-Implementierung Subdomänen enthält, können Sie mit der Basis-DN der Stammdomäne keine Benutzer in einer Subdomäne abfragen. Bei Verwendung von Active Directory können Sie jedoch auch LDAP für den Global Catalog Server (GC) am TCP-Port

3268 abfragen. Der GC enthält partielle Informationen für *alle* Objekte im Active Directory-Wald und bietet Empfehlungen für die betreffende Subdomäne, wenn weitere Informationen erforderlich sind. Wenn Sie in Ihren Subdomänen keine Benutzer "finden" können, belassen Sie die Basis-DN im Root, und legen Sie den IronPort so fest, dass er den GC-Port verwendet.

Benutzeroberfläche:

1. Erstellen Sie ein neues LDAP-Serverprofil mit Werten, die sich zuvor auf Ihrem Verzeichnisserver befinden (Systemverwaltung > LDAP). Beispiel: Serverprofilname: *PublicLDAP*Hostname: *myldapserver.example.com*Authentifizierungsmethode: *Kennwort verwenden: Aktiviert*Benutzername:*cn=ESA,cn=Benutzer,dc=beispiel,dc=com*Kennwort: *Kennwort*Servertyp: *Active Directory*Port: *3268*BaseDN:*dc=beispiel,dc=com*Stellen Sie sicher, dass Sie die Schaltfläche "Test Server(s)" verwenden, um Ihre Einstellungen zu überprüfen, bevor Sie fortfahren. Die erfolgreiche Ausgabe sollte wie folgt aussehen:

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

2. Verwenden Sie den gleichen Bildschirm, um die LDAP Accept-Abfrage zu definieren. Im folgenden Beispiel wird die Empfängeradresse mit den gebräuchlicheren Attributen "mail" ODER "proxyAddresses" verglichen:Name: *PublicLDAP.accept*QueryString:*(|(mail={a})(proxyAddresses=smtp:{a}))*Sie können die Schaltfläche "Testabfrage" verwenden, um die Ergebnisse der Suchabfrage für ein gültiges Konto zu überprüfen. Erfolgreiche Ausgaben für die Suche nach der Adresse des Dienstkontos "esa.admin@example.com" sollten wie folgt aussehen:

```
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. Wenden Sie diese neue Accept-Abfrage auf den eingehenden Listener an (Netzwerk > Listener). Erweitern Sie die Optionen LDAP-Abfragen > Akzeptieren, und wählen Sie Ihre Abfrage PublicLDAP.accept aus.

4. Bestätigen Sie abschließend die Änderungen, um diese Einstellungen zu aktivieren.

CLI:

1. **Zuerst verwenden Sie den Befehl *ldapconfig*, um einen LDAP-Server für die Appliance zu definieren, an die eine Bindung hergestellt werden soll, und es werden Abfragen für die Annahme des Empfängers (ldapaccept-Unterbefehl), Routing (ldaprouting-Unterbefehl) und Masquerading (Masquerade-Unterbefehl) konfiguriert.**

```
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. Zweitens müssen Sie die Abfrage definieren, die für den LDAP-Server ausgeführt werden soll, den Sie gerade konfiguriert haben.

```
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. Nachdem Sie die LDAP-Abfrage konfiguriert haben, müssen Sie die LDAP Accept-Richtlinie auf den eingehenden Listener anwenden.

```
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. Bestätigen Sie Ihre Änderungen, um die am Listener vorgenommenen Änderungen zu aktivieren.