LDAP Accept Query를 사용하여 Microsoft LDAP(Active Directory)를 사용하여 인바운드 메시지의 수신자를 확인하는 방법

목차

질문:

LDAP Accept Query를 사용하여 Microsoft LDAP(Active Directory)를 사용하여 인바운드 메시지의 수신자를 확인하는 방법

참고:다음 예에서는 여러 유형의 LDAP 구현에 이 원칙을 적용할 수 있지만 표준 Microsoft Active Directory 배포와 통합됩니다.

먼저 LDAP 서버 엔트리를 생성합니다. 이 엔트리는 Email Security Appliance에서 수행할 쿼리와 디렉토리 서버를 지정해야 합니다. 그런 다음 수신(공용) 리스너에서 쿼리가 활성화되거나 적용됩니다.이러한 LDAP 서버 설정은 다른 리스너 및 최종 사용자 격리 액세스와 같은 컨피그레이션의 다른 부분에서 공유할 수 있습니다.

IronPort 어플라이언스에서 LDAP 쿼리를 쉽게 구성할 수 있도록 LDAP 브라우저를 사용하는 것이 좋습니다. 이 브라우저를 사용하면 스키마와 쿼리할 수 있는 모든 특성을 살펴볼 수 있습니다.

Microsoft Windows의 경우 다음을 사용할 수 있습니다.

Linux 또는 UNIX의 경우 `ldapsearch` 명령을 사용합니다.

먼저 쿼리할 LDAP 서버를 정의해야 합니다.이 예에서는 myldapserver.example.*com* LDAP 서버에 대해 "PublicLDAP"*라는* 별칭이 지정됩니다.쿼리는 TCP 포트 389(기본값)로 전달됩니다.

참고:Active Directory 구현에 하위 도메인이 포함된 경우 루트 도메인의 기본 DN을 사용하여 하위 도메인의 사용자를 쿼리할 수 없습니다.그러나 Active Directory를 사용할 때 TCP 포트 3268의 GC(Global Catalog) 서버에 대해 LDAP를 쿼리할 수도 있습니다.GC는 Active Directory 포리스트에 있는 *all* 개체에 대한 부분 정보를 포함하며 추가 정보가 필요할 때 해당 하위 도메인을 참조합니다.하위 도메인에서 사용자를 "찾을 수 없는 경우 기본 DN을 루트에 두고 IronPort에서 GC 포트를 사용하도록 설정합니다.

GUI:

1. 이전에 디렉토리 서버에서 가져온 값을 사용하여 새 LDAP 서버 프로파일을 생성합니다 (System Administration(시스템 관리) > LDAP). 예: 서버 프로필 이름:*공용 LDAP*호스트 이름 :*myldapserver.example.com*인증 방법:*암호 사용:사용*사용자 이름 :*cn=ESA,cn=Users,dc=example,dc=com*암호:*암호*서버 유형:*Active Directory*포트 :*3268*BaseDN:*dc=example,dc=com*계속하기 전에 "서버 테스트" 단추를 사용하여 설정을 확인하십시오. 성공적인 출력은 다음과 같습니다.

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

2. 동일한 화면에서 LDAP 수락 쿼리를 정의합니다. 다음 예에서는 수신자 주소를 더 일반적인 특성, "mail" 또는 "proxyAddresses"에 대해 확인합니다.이름:*공용 LDAP.accept*QueryString:*(|(mail={a})(proxyAddresses=smtp:{a}))*"Test Query(쿼리 테스트)" 버튼을 사용하여 검색 쿼리가 유효한 계정에 대한 결과를 반환하는지 확인할 수 있습니다. 서비스 어카운트의 주소 "esa.admin@example.com"을 검색한 결과는 다음과 같아야 합니다.

```
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. 이 새 수락 쿼리를 인바운드 리스너(Network(네트워크) > Listeners(리스너)에 적용합니다. LDAP Queries(LDAP 쿼리) > Accept(수락) 옵션을 확장하고 PublicLDAP.accept 쿼리를 선택합니다.

4. 마지막으로, 변경 사항을 커밋하여 이러한 설정을 활성화합니다.

CLI:

1. **먼저 ldapconfig 명령을 사용하여 어플라이언스에 바인딩할 LDAP 서버를 정의하고 수신자 수락 쿼리(ldapaccept 하위 명령), 라우팅(ldaprouting 하위 명령) 및 masquerade(masquerade 하위 명령)를 구성합니다.**

```
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. 둘째, 방금 구성한 LDAP 서버에 대해 수행할 쿼리를 정의해야 합니다.

```
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. LDAP 쿼리를 구성했으면 인바운드 리스너에 LDAPaccept 정책을 적용해야 합니다.

```
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. 리스너에 대한 변경 사항을 활성화하려면 변경 사항을 커밋합니다.