Comment utiliser le LDAP recevez la requête pour valider les destinataires des messages d'arrivée utilisant la Microsoft Active Directory (LDAP) ?

Contenu

Question :

Comment utiliser le LDAP recevez la requête pour valider les destinataires des messages d'arrivée utilisant la Microsoft Active Directory (LDAP) ?

Remarque: L'exemple suivant intègre avec un déploiement standard de Microsoft Active Directory, bien que les principes puissent être appliqués à beaucoup de types de réalisations de LDAP.

Vous créerez d'abord une entrée de serveur LDAP, laquelle au point vous devez spécifier votre serveur de répertoire aussi bien que la requête que l'appliance de sécurité du courrier électronique exécutera. La requête est alors activée ou appliquée sur votre auditeur (public) entrant. Ces configurations de serveur LDAP peuvent être partagées par différents auditeurs et d'autres parties de la configuration telles que l'accès de quarantaine d'utilisateur.

Pour faciliter la configuration des requêtes de LDAP sur votre appliance d'IronPort, nous recommandons que vous utilisiez un navigateur de LDAP, qui te permet pour prendre à un regarder votre schéma aussi bien que tous les attributs sur contre lesquels vous pouvez questionner.

Pour Microsoft Windows, vous pouvez utiliser :

Pour le Linux ou l'UNIX, vous pouvez utiliser la commande de `ldapsearch`.

D'abord, vous devez définir le serveur LDAP pour questionner. Dans cet exemple, le surnom de « PublicLDAP » est donné pour le serveur LDAP de *myldapserver.example.com*. Des requêtes sont dirigées vers le port TCP 389 (le par défaut).

REMARQUE: Si votre implémentation de Répertoire actif contient des sous-domaines, vous ne pourrez pas questionner pour des utilisateurs dans un sous domaine utilisant le DN de base du domaine de racine. Cependant, en utilisant le Répertoire actif, vous pouvez également

questionner le LDAP contre le serveur global de catalogue (CHROMATOGRAPHIE GAZEUSE) sur le port TCP 3268. La CHROMATOGRAPHIE GAZEUSE contient les informations partielles pour des objets de *all* dans la forêt de Répertoire actif et fournit des références au sous-domaine en question quand les informations supplémentaires sont exigées. Si vous ne pouvez pas « trouver » des utilisateurs dans vos sous-domaines, laissez le DN de base à la racine et placez l'IronPort pour utiliser le port de CHROMATOGRAPHIE GAZEUSE.

GUI :

1. Créez un nouveau profil de serveur LDAP avec des valeurs situées précédemment de votre serveur de répertoire (administration système > LDAP). Exemple : Nom de profil de serveur : *PublicLDAP*Nom de l´hôte : *myldapserver.example.com*Méthode d'authentification : *Mot de passe d'utilisation : Activé*Nom d'utilisateur : *cn=ESA, cn=Users, dc=example, dc=com*Mot de passe : *mot de passe*Type de serveur : *Active Directory*Port : *3268*BaseDN : *dc=example, dc=com*Veillez à utiliser le bouton « de serveurs de test » pour vérifier vos configurations avant la continuation. La sortie réussie devrait ressembler à :

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

2. Utilisez le même écran pour définir le LDAP reçoivent la requête. L'exemple suivant vérifie l'adresse réceptive contre les attributs plus communs, l'un ou l'autre « messagerie » OU « proxyAddresses » :Nom : *PublicLDAP.accept*QueryString : *(|(mail= {a}) (proxyAddresses=smtp : {a}))*Vous pouvez utiliser le bouton « de requête de test » pour vérifier vos résultats de retours de requête de recherche pour un compte valide. La sortie réussie recherchant l'adresse « esa.admin@example.com » du compte des services devrait ressembler à :

```
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. Appliquez ce nouveau reçoivent la requête à l'auditeur d'arrivée (réseau > auditeurs). Développez les requêtes de LDAP d'options > reçoivent, et choisissent votre requête PublicLDAP.accept.

4. En conclusion, commettez les modifications pour activer ces configurations.

CLI :

1. **D'abord, vous utilisez la commande de *ldapconfig* de définir un serveur LDAP pour que l'appliance lie à, et des requêtes pour l'acceptation réceptive (commande secondaire de ldapaccept), conduisant (commande secondaire ldaprouting), et déguisant (commande secondaire de mascarade) sont configurées.**

```
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 second lieu, vous devez définir la requête pour exécuter contre le serveur LDAP que vous avez juste configuré.

```
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. Une fois que vous avez configuré la requête de LDAP, vous devez s'appliquer la stratégie de LDAPaccept à votre auditeur d'arrivée.

```
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. Pour lancer les modifications apportées à l'auditeur, commettez vos modifications.