Securing LDAP

* Identify server
  1. nslookup -type=srv \_ldap.\_tcp.DOMAINNAME (DOMAINNAME is your domain name)
* List OUs in ldap (linux)

$name = "username";

$pass = "password";

$adServer = "127.0.0.1";

$ldapconn = ldap\_connect($adServer) or die("Could not connect to LDAP server.");

ldap\_set\_option($ad, LDAP\_OPT\_PROTOCOL\_VERSION, 3) or die ("Could not set ldap protocol");

ldap\_set\_option($ad, LDAP\_OPT\_REFERRALS, 0) or die ("Could not set option referrals");

$account = $name;

$password = $pass;

$ldaprdn = $account."@foobar.com";

$ldappass = $password;

if ($ldapconn) {

$ldapbind = ldap\_bind($ldapconn, $ldaprdn, $ldappass) or die("Couldn't bind to AD!");

}

$dn = "ou=Agencies,dc=foobar,dc=com";

$filter="(objectClass=organizationalunit)";

$justthese = array("dn", "ou");

$sr=ldap\_search($ldapconn, $dn, $filter, $justthese);

$info = ldap\_get\_entries($ldapconn, $sr);

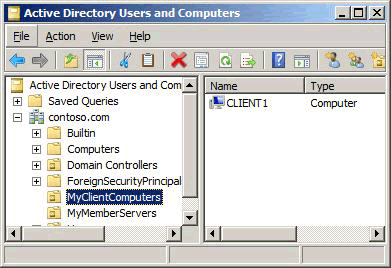
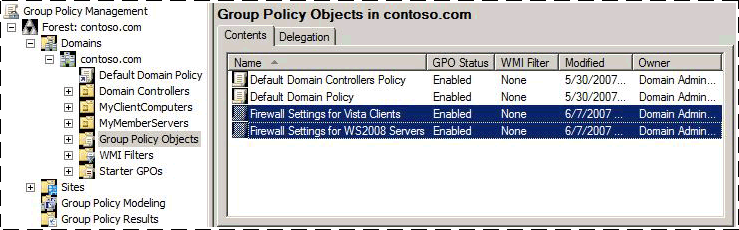
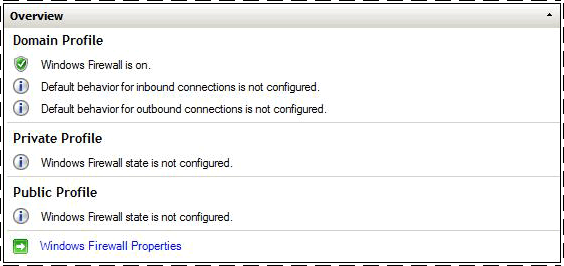
for ($i=0; $i < $info["count"]; $i++) {

echo $info[$i]["dn"]."<br>";

}

ldap\_free\_result($sr);

ldap\_unbind($ldapconn);

* List OUs (windows)
  1. Get-ADOrganizationalUnit -Filter <string> [-ResultPageSize <int>] [-ResultSetSize <System.Nullable[System.Int32]>] [-SearchBase <string>] [-SearchScope {<Base> | <OneLevel> | <Subtree>}] [-AuthType {<Negotiate> | <Basic>}] [-Credential <PSCredential>] [-Partition <string>] [-Properties <string[]>] [-Server <string>] [<CommonParameters>]
* Change root passwords
  1. Slappasswd
  2. New password: [enter new password]
  3. Re-enter new password: [re enter new password]
  4. Password will print, highlight and copy
  5. Vim chrotpw.ldif [new password in “olcRootPW” section]
  6. dn: olcDatabase={0}config,cn=config
  7. Changetype: modify
  8. Add: olcRootPW
  9. olcRootPW: [paste new password you copied]
  10. Ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.lfdif
* Change directory manager password
  1. Same as a-d in previous section
  2. Vim chdomain.lfdif
  3. Dn: olcDatabase={1}monitor,cn=config
  4. Changetype: modify
  5. Replace: olcAccess
  6. olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=srv,dc=world" read by \* none
  7. dn: olcDatabase={2}bdb,cn=config
  8. changetype: modify
  9. replace: olcSuffix
  10. olcSuffix: dc=srv,dc=world
  11. dn: olcDatabase={2}bdb,cn=config
  12. changetype: modify
  13. replace: olcRootDN
  14. olcRootDN: cn=Manager,dc=srv,dc=world
  15. dn: olcDatabase={2}bdb,cn=config
  16. changetype: modify
  17. add: olcRootPW
  18. olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
  19. dn: olcDatabase={2}bdb,cn=config
  20. changetype: modify
  21. add: olcAccess
  22. olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=Manager,dc=srv,dc=world" write by anonymous auth by self write by \* none
  23. olcAccess: {1}to dn.base="" by \* read olcAccess: {2}to \* by dn="cn=Manager,dc=srv,dc=world" write by \* read
  24. Ldapmodofy -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
* Configure LDAP to use SSL (Windows)
  1. \*LDAP sends unsecured traffic and TLS over port 389 and SSL over 636
  2. \*need to install certificate and store it on the Local computer personal certificate directory (specify your own for linux, MY certificate store for windows)
     + Certificate must contain Server Authentication OID 1.3.6.1.5.5.7.3.1
  3. Open MMC
  4. File > Add/Remove Snap-In
  5. Select **Certificates,** click Add
  6. In Certs snap in, select **Computer Account**, click Next
  7. In select computer, select **Local**, click **Ok,** then Finish
  8. Click Ok in Add or Remove Snap-Ins
  9. In console tree, expand certificates, right click **Certificates,** select **All Tasks** [if unsuccessful, you are connected to a remote DC]
  10. In **Certificate Enrollment,** click **Next**
  11. In the Select Certificate Enrollment Policy, choose **Active Directory Enrollment Policy** (default) and click Next.
  12. Select a certificate that allows for server authentication. You may want to use a custom certificate as described in Publishing a Certificate that Supports Server Authentication. Now go ahead and click Enroll
  13. The process may take a few seconds to complete. Click Finish in the Certificate Enrollment dialog box
  14. Click the **Details** tab. In the Field column, go ahead and select **Enhanced Key Usage**. You’ll want to confirm that the Server Authentication (1.3.6.1.5.5.7.3.1) is listed
  15. \*To test if LDAP over TLS works properly, use the **ldp.exe** tool.
  16. Open a command prompt and type **ldp**. Click **Enter**. The LDP application window appears.
  17. Select **Connection**, then **Connect**. The Connect dialog box appears.
  18. In the Server text box, type the name of your AD server. For this example, type the fully qualified domain name (FQDN) of the DC, just as it appears in the Subject Alternative Name (SAN) of the Digital Certificate.
  19. In the Port text box, type **636**.
  20. Check the box for **SSL**.
  21. Click OK. Now, without the above procedure you will not be able to connect.
  22. Select the Connection menu, click **Bind**, and then click **OK**.
      + The command output should display the username and domain name that you used for binding, if LDAPS is configured properly. You can start browsing through the AD tree.
* Configure SSL connections (Linux)
  1. Sudo apt-get install openssh-server
  2. sudo mkdir -v /etc/ldap/ssl
  3. pushd /etc/ldap/ssl
  4. sudo openssl req -newkey rsa:1024 -x509 -nodes -out slapd.pem -keyout slapd.pem -days 3650
     + # Make this readable to openldap only ..
  5. sudo chown -v openldap:openldap /etc/ldap/ssl/slapd.pem
  6. sudo chmod -v 400 /etc/ldap/ssl/slapd.pem
  7. Popd
* Set server LDAP signing requirement
  1. Click **Start**, click **Run**, type mmc.exe, and then click **OK**.
  2. On the **File** menu, click **Add/Remove Snap-in**.
  3. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Management Editor**, and then click **Add**.
  4. In the **Select Group Policy Object** dialog box, click **Browse**.
  5. In the **Browse for a Group Policy Object** dialog box, click **Default Domain Policy** under the **Domains, OUs and linked Group Policy Objects** area, and then click **OK**.
  6. Click **Finish**.
  7. Click **OK**.
  8. Expand **Default Domain Controller Policy**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
  9. Right-click **Domain controller: LDAP server signing requirements**, and then click **Properties**.
  10. In the **Domain controller: LDAP server signing requirements Properties** dialog box, enable **Define this policy setting**, click to select **Require signing** in the **Define this policy setting** drop-down list, and then click **OK**.
  11. In the **Confirm Setting Change** dialog box, click **Yes**.
* Set Client LDAP signing requirement through local computer policy (windows)
  1. Click **Start**, click **Run**, type mmc.exe, and then click **OK**.
  2. On the **File** menu, click **Add/Remove Snap-in**.
  3. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**.
  4. Click **Finish**.
  5. Click **OK**.
  6. Expand **Local Computer Policy**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
  7. Right-click **Network security: LDAP client signing requirements**, and then click **Properties**.
  8. In the **Network security: LDAP client signing requirements Properties** dialog box, click to select **Require signing** in the drop-down list, and then click **OK**.
  9. In the **Confirm Setting Change** dialog box, click **Yes**.
* Set the client LDAP signing requirement through a domain group policy object (windows)
  1. Click **Start**, click **Run**, type **mmc.exe**, and then click **OK**.
  2. On the **File** menu, click **Add/Remove Snap-in**.
  3. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**.
  4. Click **Browse**, and then select **Default Domain Policy** (or the Group Policy Object for which you want to enable client LDAP signing).
  5. Click **OK**.
  6. Click **Finish**.
  7. Click **Close**.
  8. Click **OK**.
  9. Expand **Default Domain Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
  10. In the **Network security: LDAP client signing requirements Properties** dialog box, click to select **Require signing** in the drop-down list, and then click **OK**.
  11. In the **Confirm Setting Change** dialog box, click **Yes**.
* Create OUs and put computer accounts into them (windows servers up to 2008)
  1. On DC1, click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**. Alternatively, you can use Server Manager. Expand **Roles**, expand **Active Directory Domain Services**, and then expand **Active Directory Users and Computers [DC1.contoso.com]**.
  2. n the navigation pane, right-click **contoso.com**, click **New**, and then click **Organizational Unit**.
  3. In the **Name** box, type **MyMemberServers**, and then click **OK**.
  4. Right-click **contoso.com** again, and then click **New**, and then click **Organizational Unit**.
  5. In the **Name** box, type **MyClientComputers**, and then click **OK**.
  6. In the navigation pane, click **Computers**.
  7. In the results pane, right-click **CLIENT1**, and then click **Move**.
  8. In the **Move** dialog box, click **MyClientComputers**, and then click **OK**.
  9. In the results pane, right-click **MBRSVR1**, and then click **Move**.
  10. In the **Move** dialog box, click **MyMemberServers**, and then click **OK**.
  11. When you have finished, your display resembles the following figure.
  12. 
  13. Close the **Active Directory Users and Computers** snap-in.
* Create new Group Policy Object (windows)
  1. On MBRSVR1, click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
  2. Alternatively, if you use Server Manager, expand **Features**, and then expand **Group Policy Management**.
  3. In the navigation pane, expand **Forest: contoso.com**, expand **Domains**, and then expand **contoso.com**.
  4. In the navigation pane, right-click **Group Policy Objects**, and then click **New**.
  5. In the **Name** box, type **Firewall Settings for Windows Servers**, and then click **OK**.
  6. In the navigation pane, right-click **Group Policy Objects**, and then click **New**.
  7. In the **Name** box, type **Firewall Settings for Windows Clients**, and then click **OK**.
  8. Select the **Group Policy Objects** node, and your display resembles the following figure.
  9. 
* Add GPO setting to enable firewall on member client computers
  1. On MBRSVR1, in **Group Policy Management**, click **Group Policy Objects**, right-click **Firewall Settings for Windows Clients**, and then click **Edit**.
  2. In **Group Policy Management Editor**, right-click the top node **Firewall Settings for Windows Clients [DC1.contoso.com] Policy**, and then click **Properties**.
  3. Select the **Disable User Configuration settings** check box.
  4. In the **Confirm Disable** dialog box, click **Yes**, and then click **OK**.
  5. Under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Windows Firewall with Advanced Security**.
  6. Click the node **Windows Firewall with Advanced Security - LDAP://cn={***GUID***},cn=policies,cn=system,DC=contoso,DC=com**, where *GUID* is a unique number assigned to your domain.
  7. In the results pane, under **Overview**, notice that for each network location profile **Windows Firewall state is not configured**, and then click **Windows Firewall Properties**.
  8. On the **Domain Profile** tab, click the drop-down list next to **Firewall state**, and then click **On (recommended)**.
  9. Click **OK** to save your changes. Note in the results pane that **Domain Profile** now shows **Windows Firewall is on**.
  10. 
  11. Close **Group Policy Management Editor**.
* Deploy initial GPO with test firewall settings
  1. On MBRSVR1, in **Group Policy Management**, in the navigation pane, right-click **MyClientComputers**, and then click **Link an Existing GPO**.
  2. In the **Group Policy objects** list, click **Firewall Settings for Windows Clients**, and then click **OK**.
* Confirm receipt and application of GPO policies
  1. On CLIENT1, open an administrator command prompt.
  2. At the command prompt window, type **gpupdate /force**, and then press ENTER. Wait until the command finishes before moving to the next step.
  3. To validate that the GPO was correctly applied, run **gpresult /r /scope computer**. In the output, look for the section **Applied Group Policy Objects**. Confirm that it contains entries for both **Firewall Settings for Windows Clients** and the **Default Domain Policy**.
  4. Open the Windows Firewall with Advanced Security snap-in.
  5. Right-click the top node **Windows Firewall with Advanced Security on Local Computer**, and then click **Properties**.
  6. Note that the **Firewall State** setting is **On (recommended)**, and that the list control is disabled. It is now controlled by Group Policy and cannot be changed locally, even by an administrator.
  7. Close the **Properties** dialog box, and the Windows Firewall with Advanced Security snap-in
* Prevent computer from using rules and settings defined by local admin
  1. On MBRSVR1, in **Group Policy Management**, click **Group Policy Objects**, right-click **Firewall Settings for Windows Clients**, and then click **Edit**.
  2. In **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Windows Firewall with Advanced Security**.
  3. Right-click **Windows Firewall with Advanced Security - LDAP://cn={***GUID***},cn=policies,cn=system,DC=contoso,DC=com**, and then click **Properties**.
  4. On the **Domain Profile** tab, in the **Settings** section, click **Customize**.
  5. Change the **Display a notification** setting to **No**. This prevents Windows from displaying a notification to the user whenever a program is blocked.
  6. In the **Rule merging** section, change the **Apply local firewall rules** list to **No**.
  7. In the **Rule merging** section, change the **Apply local connection security rules** list to **No**.
  8. Click **OK** two times to return to **Group Policy Management Editor**.
* Test new restrictions
  1. On CLIENT1, in **Administrator: Command Prompt**, run **gpupdate /force**. Wait until the command finishes.
  2. In the **Windows Firewall with Advanced Security** snap-in, in the list of **Outbound Rules**, right-click **A Test Rule**, and then click **Enable Rule**.
  3. In **Administrator: Command Prompt**, run **ping dc1**.
  4. The ping command works even though **A Test Rule** appears to be enabled. The rule is listed as enabled on the local computer, but when you set the **Apply local firewall rules** to **No** on the GPO in the previous procedure, you blocked the merging of local rules with the rules delivered in the GPO.
  5. In the navigation pane of the **Windows Firewall with Advanced Security** snap-in, expand **Monitoring**, and then click **Firewall** to see the list of rules active on the local computer.
  6. No rules are listed. You have not yet created any rules applied by GPO, and no local rules are active because of the settings that you included in the GPO.
  7. Before proceeding, delete your rule. On CLIENT1, in the navigation pane, click **Outbound Rules**. In the results pane, right-click **A Test Rule**, click **Delete**, and then click **Yes** on the confirmation dialog box.
  8. Leave both **Administrator: Command Prompt** and the **Windows Firewall with Advanced Security** snap-in open.