Windows Enterprise
OU Administrator Tips
Using LDAPS on the Windows Enterprise Domain

November 29, 2007
Updated: May 9, 2008

LDAP Simple Binds Should be Converted to LDAPS

ITS is in the process of shutting down "LDAP simple binds" to the four Windows Enterprise domain controllers (WINDC1-4). An "LDAP simple bind" is an extremely insecure method of authenticating to an LDAP server using "clear text" passwords.

There are secure alternatives to the LDAP authentication process. LDAP connections are done by Windows domain-member systems using Kerberos-5 credentials (via SASL on port 389). Non-domain-member systems (or other Windows 3rd party software vendors) can use LDAPS (using a digital certificate on port 636).

ITS has installed LDAPS digital certificates from Thawte on all four Windows Enterprise domain controllers. ITS is currently monitoring all systems currently using "LDAP simple binds" and will assist in the transition of LDAP to LDAPS. At a date in the future (yet to be determined) LDAP simple binds will be disabled on the Windows Enterprise Domain. LDAP simple binds will not be disabled until an attempt had been made to contact and convert software on existing systems using LDAP simple binds.

What You Need to Do If You Know You Are Using "LDAP Simple Binds"

If you know you have installed 3rd party software which performs authenticated binds to the Windows Enterprise domain controllers you need to start on the following immediately:

1. Review your systems and determine what process(es) running on the machine may be performing an "LDAP simple bind".
2. Determine how the process can successfully use "LDAPS" for SSL-TLS LDAP communications.

Feedback on specific packages follows.

Configuring Apache to use LDAPS against Active Directory

[Thanks to Darin Dugan (C EXT) for providing these tips]

Works only on Apache 2.1 or later. Tested using Apache 2.2.3 on RedHat Enterprise 5

1. Create an unprivileged account in AD that will be used to bind and search

2. You can download the Thawte root certificates from www.thawte.com/roots/. Get the Thawte CA cert in base 64 format (ThawtePremiumServerCA_b64.txt)
3. Add the following lines to the main httpd.conf:
   LDAPTrustedMode SSL
   LDAPTrustedGlobalCert CA_BASE64
   /etc/httpd/conf/ThawtePremiumServerCA_b64.txt
   (adjusting this path as appropriate)

4. Add the following lines to any Directory section or .htaccess file:

   AuthType basic
   AuthName "Credentials Required"
   AuthBasicProvider ldap
   AuthLDAPURL "ldaps://windc<n>.iastate.edu windc<n>.iastate.edu
   Windc<n>.iastate.edu
   windc<n>.iastate.edu/DC=iastate,DC=edu?sAMAccountName"
   AuthLDAPBindDN "CN=SomeUser,OU=SomeOU,DC=iastate,DC=edu"
   AuthLDAPBindPassword XXXXXXXXXXXXXXX
   Require ldap-group CN=SomeGroupName,OU=SomeOU,DC=iastate,DC=edu

Important: When configuring the order of which the Windows Enterprise domain controllers are listed in the "AuthLDAPURL" line, administrators should "randomize" the WINDC1-4 hostnames in the "AuthLDAPURL" line (space separated) on each server. In the above "AuthLDAPURL" line, the "windc<n>" numbers should be 1-4 in a randomly chosen order (not "1" "2" '3" "4" on all systems). Since the first system in the list is tried first, this will spread the connection load across all domain controllers.

This allows access for any AD user that is a member of the group specified.

Configuring Moodle to Use LDAPS Against Active Directory

[Thanks to Darin Dugan (C EXT) for providing these tips]

These instructions apply to Windows, but are comparable on Linux.

1. PHP uses php_ldap.dll and php_openssl.dll to provide LDAP and LDAPS support. Ensure both are enabled.
2. php_ldap.dll is built from OpenLDAP and expects to find a configuration file in C:\OpenLDAP\sysconf\ldap.conf.
3. Specify the path to the root CA certificate in base64 format in ldap.conf:

   TLS_CACERT C:\\OpenSSL\\certs\\ThawtePremiumServerCA_b64.txt

4. You can download the Thawte root certificates from www.thawte.com/roots/. Extract ThawtePremiumServerCA_b64.txt and place in the appropriate folder.

5. You may need to restart the web server to ensure changes take effect.

Moodle itself supports LDAP or LDAPS simply by changing from "ldap://windc<n>.iastate.edu" to 'ldaps://windc<n>.iastate.edu', assuming the above is done so that PHP can verify the certificate.

Important: When configuring the order of which the Windows Enterprise domain controllers are listed in the LDAP server settings Host URL, administrators should "randomize" the WINDC1-4 hostnames (semicolon separated) on each server. The "ldaps://windc<n>.iastate.edu" hostnames should be 1-4 in a randomly chosen order (not "1" "2" '3" "4" on all systems). Since the first system in the list is tried first, this will spread the connection load across all domain controllers.

Configuring SAMBA to Use LDAPS Against Active Directory

The ISU RHEL site has good starting instructions for integrating Samba with the ISU Enterprise Active Directory domain:

http://www.linux.iastate.edu/documentation/articles/server-configuration/integrating-samba-with-the-isu-active-directory/

[NOTE: The LDAP configuration information at this site needs to be updated from LDAP to LDAPS]

If you already have a Samba server authenticating against AD using simple binds, the fix is simple.

1. Edit ldap.conf to remove or comment out the HOST line and change the URI line from ldap://xxxxxxxxx to ldaps://xxxxxxxx
2. Stop the winbind service
3. Start the windbind service

Here is an example ldap.conf file:

****
comment out the HOST line or delete it as HOST is deprecated in favor
of URI
HOST windc1.iastate.edu
BASE DC=iastate,DC=edu
URI line takes space separated entries
put windc1-4 in random order on this line
URI ldaps://windc2.iastate.edu/ ldaps://windc4.iastate.edu
ldaps://windc1.iastate.edu ldaps://windc3.iastate.edu
ldap_version 3
binddn some_account@IASTATE.EDU

```
bindpw the_some_account_password
scope sub
nss_map_objectclass posixAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute cn sAMAccountName
pam_login_attribute sAMAccountName
nss_map_attribute userPassword msSFUPassword
nss_map_attribute homeDirectory msSFUHomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute uniqueMember member
pam_filter objectclass=user
pam_password ad
**********
```