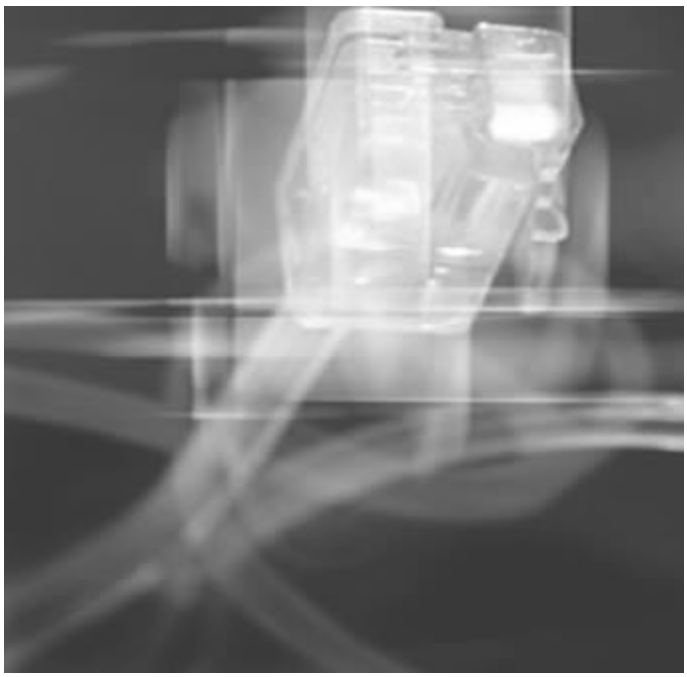
Configuring SSL for LDAP

MICROSOFT ACTIVE DIRECTORY (AD)

Revision 1.0-EN



DIGITALIS 2003

João Carlos Galaio da Silva
Rodrigo Gonçalves

Created:
22nd January 2007

INDEX

Revision history

v.1.0	22nd January 2007	João Silva	Document creation
v.1.0-EN	30th April 2008	Rodrigo Gonçalves	Translation

Before you start

The following requirements must be met prior to configure the connection:

1. Active Directory instance running on Windows 2000 or 2003
2. Java Virtual Machine(JVM) >= 1.5 installed on the server that will run the LDAP client application. The environment variable **JAVA_HOME** must point to the JVM install folder. The **$PATH** environment variable must contain the **JAVA_HOME/bin** entry.
3. Certificate Authority Web Enrollment tool must be configured on the AD server. The following link points to a page that shows how to configure this:
   http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx

Configuring the SSL connection

- Assuming all the requirements described on the previous section are fulfilled and that the AD server belongs to the domain "server.domain.com", the administrator should do the following:
  - From the server that will run the LDAP client application, access via browser to http://computador.dominio.pt/certsrv/certcarc.asp. Log in the page to Access to the Active Directory server. On the following page click on **Download a CA Certificate** leaving the **DER encoded** option selected. The file **certnew.cer** should be saved on any server's folder.
  - Open a command line shell and navigate to the folder where the **certnew.cer** file was saved and do the following:
    - The **JAVA_HOME/jre/lib/security/cacerts** file contains the **client certificate authority** for the JVM. Best practices advise password changing (the default value is **changeit**). To do it execute the following command on a shell:
      - On windows:

        keytool -storepasswd -new newpass -storepass changeit -keystore "%JAVA_HOME%/jre/lib/security/cacerts"

- On Linux:

  keytool -storepasswd -new newpass -storepass changeit -keystore $JAVA_HOME/jre/lib/security/cacerts

- The digital certificate must be imported to the **cacerts** client file. It**'s** assumed that the digital certificate was downloaded from a server with the following DNS "server.domain.com". Using this information issue the following command:
  - On Windows:

    keytool -import -alias domain -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"
  - On Linux:

    keytool -import -alias domain -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts

  Some information about the certificate will be printed on the screen and a question about the certificate's trustiness will be asked. The answer should be **yes** so cacerts can trust the AD server.
- To check the certificate's effectiveness a user can be added to the AD server through the client application.

Note: The certificate expires after a year. It must be renewed before expiring. To renew the certificate do the following steps (it is advised to do it on the day before the certificate expires):

- *Navigate to the folder where the **certnew.cer** is stored and give the following command using the password defined during the certificate's installation:*
  - *On Windows:*

    keytool -delete -alias domain -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"
  - *On Linux:*

    keytool -delete -alias domain -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts
- *The certificate must be imported once again into the keytool. The **password** used on the previous step is used on this step.*
  - *On Windows:*

    keytool -import -alias domain -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"

- *On Linux:*

  keytool -import -alias domain -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts

Frequent issues

:: How can the certificate be deleted?

To delete the certificate issue the following commando: ***keytool -delete -alias domain -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts***. Remember that after the certificate has been removed some SSL-based operations will not be possible to be executed. Some of these operations include changing the password of an AD user, for example. The certificate must then be imported again.

:: A '*keytool error: java.io.IOException: Keystore was tampered with, or password was incorrect.* ' exception was raised when importing the certificate. What happened?

An incorrect password was supplied to the **cacerts** client. Remember that the password might have been changed from the default "changeit" to a user-defined password.

:: List of common stack trace of errors

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 525, v893
HEX: 0x525 - user not found
DEC: 1317 - ERROR_NO_SUCH_USER (The specified account does not exist.)
CAUSE: The supplied user is invalid.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 52e, v893
HEX: 0x52e - invalid credentials
DEC: 1326 - ERROR_LOGON_FAILURE (Logon failure: unknown user name or bad password.)
CAUSE: The supplied user is valid but the password/credential are not correct.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 530, v893
HEX: 0x530 - not permitted to logon at this time
DEC: 1328 - ERROR_INVALID_LOGON_HOURS (Logon failure: account logon time restriction violation.)
CAUSE: The user doesn't have permission to log on at the current time. LDAP servers allow definition of working time periods. Logging on outside working hours might be disabled.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893
HEX: 0x531 - not permitted to logon from this workstation
DEC: 1329 - ERROR_INVALID_WORKSTATION (Logon failure: user not allowed to log on to this computer.)
LDAP[userWorkstations: <multivalued list of workstation names>]
CAUSE: The user is not cleared to log on from the workstation where he is.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error,Documento com configuracao ldap ssl (Source) data 532, v893
HEX: 0x532 - password expired
DEC: 1330 - ERROR_PASSWORD_EXPIRED (Logon failure: the specified account password has expired.)
LDAP[userAccountControl: <bitmask=0x00800000>] - PASSWORDEXPIRED
CAUSE: The AD password has expired for the supplied user.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 533, v893
HEX: 0x533 - account disabled
DEC: 1331 - ERROR_ACCOUNT_DISABLED (Logon failure: account currently disabled.)
LDAP[userAccountControl: <bitmask=0x00000002>] - ACCOUNTDISABLE
CAUSE: The user account has been disabled on the AD server.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 701, v893
HEX: 0x701 - account expired
DEC: 1793 - ERROR_ACCOUNT_EXPIRED (The user's account has expired.)
LDAP[accountExpires: <value of -1, 0, or extemely large value indicates account will not expire>] - ACCOUNTEXPIRED
CAUSE: The user account has expired.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 773, v893
HEX: 0x773 - user must reset password
DEC: 1907 - ERROR_PASSWORD_MUST_CHANGE (The user's password must be changed before

logging on the first time.)
LDAP[pwdLastSet: <value of 0 indicates admin-required password change>] - MUST_CHANGE_PASSWD
CAUSE: The user must change the password.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 775, v893
HEX: 0x775 - account locked out
DEC: 1909 - ERROR_ACCOUNT_LOCKED_OUT (The referenced account is currently locked out and may not be logged on to.)
LDAP[userAccountControl: <bitmask=0x00000010>] - LOCKOUT
CAUSE: The user account has been locked on the AD server.

[LDAP: error code 50 - 00000005: SecErr: DSID-031A0F40, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
CAUSE: The user doesn't have permissions to perform the requested operations.