|  |
| --- |
| **OVERVIEW:** |
| This Standard Operating Procedure (SOP) describes how to connect LDAP Clients to Enterprise Directory using SSL. |
| **APPROVALS/PRECONDITIONS** |
| List any approvals required or conditions under which this SOP can be performed:   * User must have an LDAP certificate * The CIS standard is for applications to connect using encrypted protocol (SSL); clients must use SSL * The open port (389) is not available in TDE |
| **PREPARATION: ROLES AND ACCESS REQUIRED** |
| Any application user can perform this action. |
| **PROCEDURE:** |
| 1. **Environment Summary:** Use the below hostnames to connect to the desired environment. It is always recommended to use the virtual hostname to connect to the LDAP infrastructure:    1. **DEV** dev-corpldap.it.statestr.com PORT SSL 636 (linked to test Active Directory Forests)    2. **UAT** uat-corpldap.statestr.com PORT SSL 636 (linked to production Active Directory Forests)    3. **PRD** corpldap.statestr.com PORT SSL 636 (linked to production Active Directory Forests)   **NOTE:** Any applications developed in house must begin by connecting to the development environment; vendor applications can begin by connecting to the UAT environment. Also, an application team may not have 3 separate instances for DEV, UAT and PROD.   1. **Configuration:** When prompted, provide the Base DN and User Location for the view needed. 2. To see a view of the CORP Active Directory only, enter the values below:  * Base DN : ou=internal,ou=users,dc=statestreet,dc=com * User Location : ou=internal,ou=users,dc=statestreet,dc=com  1. To see a view of all Active Directory Domains (CORP, SSGA,IFS, IMS-West, Princeton, IBT), enter the values below:  * Base DN : ou=users,dc=statestreet,dc=com * User Location :  ou=users,dc=statestreet,dc=com  1. **LDAP Clients using Java:** Use the steps below to change the default DNS Cache Behavior:    1. networkaddress.cache.ttl (default: -1): Indicates the caching policy for successful name lookups from the name service. The value is specified as integer to indicate the number of seconds to cache the successful lookup. A value of -1 indicates "cache forever".    2. networkaddress.cache.negative.ttl (default: 10): Indicates the caching policy for un-successful name lookups from the name service. The value is specified as integer to indicate the number of seconds to cache the failure for un-successful lookups. A value of 0 indicates "never cache". A value of -1 indicates "cache forever".    3. Specifically, you must specify Java Network Property "networkaddress.cache.ttl=5"   The default DNS cache behavior for Java 1.4 and Java 1.5 was taken from API documentation: <http://java.sun.com/j2se/1.4.2/docs/guide/net/properties.html>   1. **SSL Setup:** Depending on whether the application uses Mozilla or JAVA, follow the appropriate steps below: 2. Mozilla Truststore SSL Preparation: This sample command assumes Solaris 10 OS. If a different OS is being used, certutil will need to be located.    * /usr/sfw/bin/certutil -A -n " VerisignClass3PrimaryG5CA " -t "C,," -a -i ./ VerisignClass3PrimaryG5CA.cer –d    * /usr/sfw/bin/certutil -A -n " VerisignClass3SecondaryCA" -t "C,," -a -i ./ VerisignClass3SecondaryCA.cer –d 3. JAVA default Truststore SSL Preparation: The default keystore is located at {your jre}/lib/security/cacerts; the VERISIGN Root must be added to this store.    * cd {your jre}/bin      + sudo ./keytool -import -trustcacerts -alias VerisignClass3PrimaryG5CA. -file {your jre}/lib/security/VerisignClass3PrimaryG5CA.cer -keystore {your jre}/lib/security/cacerts      + sudo ./keytool -import -trustcacerts -alias VerisignClass3SecondaryCA -file {your jre}/lib/security/VerisignClass3SecondaryCA.cer -keystore {your jre}/lib/security/cacerts    * JNDI Coding – This JAVA code will be furnished upon request 4. **Settings:** To ensure proper performance, these settings must be completed during initial connection:    1. Accounts – Every employee, contractor and temp has an account in UAT & PROD (it is the LAN Account and LAN Password). Most employees have an account in DEV, although the password is different. Contact LDAP, CORP concerning the DEV account; these accounts are commonly referenced as “uatcorp” accounts.    2. Attributes – Any authenticated account has LIMITED-READOnly access by default, which allows the viewing of commonly available identity data (email, phone number, title). There are capacity restrictions on this default access to limit un-authorized server demand.   Process IDs are given no capacity restrictions by default and also have LIMITED\_READOnly access.  Enhanced access is available and must be authorized by Security Architecture and Engineering (SAE). Enterprise Directory Attributes for Internal Users   * 1. Failover – The hosts referenced in Step 1 are all high availability (HA) URLs managed by corporate F5 network hardware. If the product supports client failover options, the product support team should add the additional servers to their configuration (IP addresses for high availability URLs – obtained via nslookups); this will allow the client to find the HA service despite any disruptions in name server resolution.   2. Pooling - Clients are encouraged to use pooling. The current versions of JNDI support pooling directly in the package. Enable pooling and set the parameters using command line property settings for the JVM. For most clients, a pool size of 1 is adequate. If the client is a heavy user of LDAP services the LDAP Engineering team should be engaged to construct the ideal pooling parameters. When using pooled connections, the timeout setting must be used to cleanup idle connections.   3. Idle timeout – There are many infrastructure components used while connecting to the LDAP server (i.e., load balancers, proxies and firewalls), and each of these components may have an idletimeout configured for persistent connections. The standard is to utilize a 5 minute idletimeout on any LDAP Client. For example, java clients using JNDI would set the timeout value to (300000) milliseconds to achieve a 5 minute timeout: com.sun.jndi.ldap.connect.pool.timeout=300000 |
| **REFERENCES:** |
|  |