

JNDI Ldap Password Expiration Controls

Source: <http://coding.derkeiler.com/Archive/Java/comp.lang.java.programmer/2004-03/2341.html>

From: John W. (jwagenleitner_at_yahoo.com)

Date: 03/17/04

Date: 16 Mar 2004 17:58:00 -0800

We have implemented a password policy for our directory server. If I use the code below and pass it a user's DN and password to whom the policy is applied I get the Control[] back and can determine if the account is expired or when it will expire.

Is there a way to get this information by logging in with a directory admin account? In other words, I want to be able to bind to the directory as "cn=JoeAdmin" and be able to determine if "uid=joeuser,ou=..." account is expired or the date it will expire. I've run across the ProxiedAuthorizationControl control, but not sure it will allow me to proxy a user's bind and get controls back.

The reason for those that care...we have an off-the-self Java web application that receives the user login/password at signin. We can customize the product with add-in classes, but by the time the request object gets to my classes password has already hashed so I can't use to supply credentials to the context. I am hoping I can log in as admin and there is some means of doing a SwitchUser that would then tell me that the account I'm trying to switch to is expired. Or if I perform a search for an user's entry it will send back the controls related to password expiration for that user entry.

Thanks in advance.

John

```
-----  
public class PSLdap {  
  
    private Hashtable env = null;  
  
    public PSLdap() {  
        // Need to register a security provider for JSSE for LDAPS  
        java.security.Security.addProvider( new  
com.sun.net.ssl.internal.ssl.Provider() );  
        // Env to pass to context to establish connection  
        env = new Hashtable();  
    }  
}
```

```

public static void main ( String[] args ) {
    /*
     * For debug only
     */
    PSLdap psl = new PSLdap();
    psl.isExpired("user-id", "phonypassword");
}

public boolean isExpired(String dn, String creds) {
    Hashtable env = new Hashtable();
    env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
    env.put(Context.PROVIDER_URL, "ldap://...");
    env.put(Context.SECURITY_PRINCIPAL, dn);
    env.put(Context.SECURITY_CREDENTIALS, creds);
    env.put(Context.SECURITY_PROTOCOL, "ssl");

    try {
        LdapContext ctx = new InitialLdapContext(env, null);

        // If we received controls in the response...
        Control[] respControls;
        if ((respControls = ctx.getResponseControls()) != null) {
            // Loop through the results...
            long secPwdExpire = 0L;
            for (int i = 0; i < respControls.length; i++) {
                // Until we locate the password expired control...
                if (respControls[i] instanceof
PasswordExpiringResponseControl) {
                    // Password is set to expire, set error
                    message...
                    secPwdExpire =
((PasswordExpiringResponseControl) respControls[i]).timeRemaining();
                    System.out.println("Password expires in " +
secPwdExpire + " seconds.");
                    secPwdExpire = ( new Date().getTime() +
(secPwdExpire * 1000));
                    System.out.println("Date password expires is "
+ new Date(secPwdExpire));
                }
                if (respControls[i] instanceof
PasswordExpiredResponseControl) {
                    // Password expired, return...
                    System.out.println("Password Expired.");
                    return true;
                }
            }
        }

        ctx.close();
    }
}

```

```
    } catch (Exception ex) {  
        ex.printStackTrace();  
    }  
    return false;  
}  
  
}
```