Tapestry5HowToSecureWithAcegiAndLDAP

This article describes how you can easily integrate Tapestry5 with Acegi using LDAP for storing your users and roles.

Setting up

The only additional dependency you'll need is the tapestry-acegi integration module that you can find here. At the time of this writing, you'll need to use the 1.1.1-SNAPSHOT release of the module as the final 1.1.1 version hasn't been released yet. If your using maven you can get this version by adding the following to your POM:

```
<dependency>
   <groupId>nu.localhost.tapestry</groupId>
   <artifactId>tapestry5-acegi</artifactId>
   <version>1.1.1-SNAPSHOT</version>
</dependency>

...and...

<repository>
   <id>localhost.nu</id>
   <url>http://www.localhost.nu/java/mvn-snapshot</url>
</repository>
```

Configuring your application

First you'll need to add something to the Tapestry filter mapping in your *web.xml* file. This is because by default when you specify a filter mapping the filter will actually only be invoked when actual request are made to the configured URL, but not when the RequestDispatcher forwards a request to that URL. Acegi uses FORWARD so you'll have to make you filter mapping look something like this:

```
<filter-mapping>
   <filter-name>app</filter-name>
   <url-pattern>/*</url-pattern>
   <dispatcher>FORWARD</dispatcher>
   <dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

Now you'll need to configure your security services. As every configuration in Tapestry, this is done you the application module. I usually create and SecurityModule submodule so that i don't get my main module filled with security stuff, but you can place the following code in any module you want.

```
public class SecurityModule
{
  public static UserDetailsService buildLdapUserDetailsService(final @Inject LdapUserSearch ldapUserSearch,
final Logger logger)
  {
    return new UserDetailsService()
    {
      /**
       * Finds user details by the username.
       *
       * @param username the username to look for.
       * @return the user details or <code>null</code> if no user is found with the given username.
       */
      public UserDetails loadUserByUsername(String username)
      {
        try
        {
          return ldapUserSearch.searchForUser(username);
        } catch (UsernameNotFoundException ex)
        {
          logger.info("Couldn't find user with username \"" + username + "\".");

          return null;
        }
      }
    };
  }
```

```
  public static InitialDirContextFactory buildInitialDirContextFactory(@Inject @Value("${ldap-provider-url}")
String providerUrl,
                                                                       @Inject @Value("${ldap-manager-dn}")
String managerDn,
                                                                       @Inject @Value("${ldap-manager-
password}") String managerPassword)
  {
    assert providerUrl != null;

    assert managerDn != null;

    assert managerPassword != null;

    // Initialize the context factory
    DefaultInitialDirContextFactory factory = new DefaultInitialDirContextFactory(providerUrl);
    factory.setManagerDn(managerDn);
    factory.setManagerPassword(managerPassword);

    // Sets the referral property of the Context (http://java.sun.com/j2se/1.5.0/docs/api/javax/naming/Context.
html#REFERRAL)
    Map<String, String> extraEnvVars = new HashMap<String, String>();
    extraEnvVars.put("java.naming.referral", "follow");
    factory.setExtraEnvVars(extraEnvVars);

    return factory;
  }

  public static LdapUserSearch buildFilterBasedLdapUserSearch(InitialDirContextFactory factory,
                                                               @Inject @Value("${ldap-users-search-base}")
String usersSearchBase)
  {
    FilterBasedLdapUserSearch userSearch = new FilterBasedLdapUserSearch(usersSearchBase, "(cn={0})", factory);

    // search in subtrees
    userSearch.setSearchSubtree(true);

    userSearch.setDerefLinkFlag(true);

    return userSearch;
  }

  public static AuthenticationProvider buildLdapAuthenticationProvider(InitialDirContextFactory factory,
@Inject LdapUserSearch ldapUserSearch,
                                                                       @Inject @Value("${ldap-roles-search-
base}") String rolesSearchBase)
          throws Exception
  {
    BindAuthenticator authenticator = new BindAuthenticator(factory);
    authenticator.setUserSearch(ldapUserSearch);
    authenticator.afterPropertiesSet();

    DefaultLdapAuthoritiesPopulator populator = new DefaultLdapAuthoritiesPopulator(factory, rolesSearchBase);
    populator.setGroupRoleAttribute("cn");
    populator.setGroupSearchFilter("member={0}");
    populator.setDefaultRole("ROLE_ANONYMOUS");
    populator.setConvertToUpperCase(true);
    populator.setSearchSubtree(true);
    populator.setRolePrefix("ROLE_");

    return new LdapAuthenticationProvider(authenticator, populator);
  }

  public static void contributeProviderManager(OrderedConfiguration<AuthenticationProvider> configuration,
                                               @InjectService("LdapAuthenticationProvider")
AuthenticationProvider ldapAuthenticationProvider)
  {
    configuration.add("ldapAuthenticationProvider", ldapAuthenticationProvider);
  }

  public static void contributeApplicationDefaults(MappedConfiguration<String, String> configuration)
```

```
  {
    // Url redirected to when trying to use a secured class and/or method.
    configuration.add("acegi.loginform.url", "/login");

    // Url redirected to when fails to login.
    configuration.add("acegi.failure.url", "/login/failed");

    // If set to other than empty, the request dispatcher will "forward" to this specified error page view.
From Acegi documentation: The error page to use.
    // Must begin with a "/" and is interpreted relative to the current context root.
    configuration.add("acegi.accessDenied.url", "/accessdenied");

    // Change the default password encoder. Must implement org.acegisecurity.providers.encoding.PasswordEncoder.
    configuration.add("acegi.password.encoder", "org.acegisecurity.providers.encoding.Md5PasswordEncoder");

    // Page redirected to after a successful logout.
    configuration.add("acegi.afterlogout.page", "Index");
  }
}
```

I think most of is self explanatory. As you can see there are a lot inject symbols, this is because i wanted to keep this solution as generic as possible so it could be used in other projects without changing any code. You'll find more information on some of the configurations made here.

Lets use it

Using this couldn't be simpler. Secure your application the way its described here. Just add the @Secured annotation on your page classes and methods and it's done.