Lab 03: Authentication, Authorization & Security

**Lab Time:** 60 minutes

**Lab Overview:** This lab walks you through creating a new Publishing site but creating two authentication paths for accessing the site. This is a common scenario for content-centric Internet facing sites. Companies want the ability to have certain employees access the site using their corporate AD credentials to create, edit, review, approve and publish content. In addition, there is a need to have the same site be available to the world as an anonymous site. Some companies also have password protected areas of their site. Your IT staff will not be happy when they hear your team has decided to put every user who creates an account on the public website in the corporate Active Directory... that just is not safe, secure... or sane! At the end of this lab, you will have two paths into your site, one non-anonymous using AD for authentication and another, anonymous access with some password protected areas using Forms Based Authentication (FBA) for authentication.

Exercise 1: Creating a new Web application & provisioning a Publishing site collection

In this exercise you will create a new Web application that will be the starting point for the rest of this lab. In the previous lab, you created a new DNS entry and Web application and site collection using the Publishing Portal site template. Refer to those same instructions for the following steps.

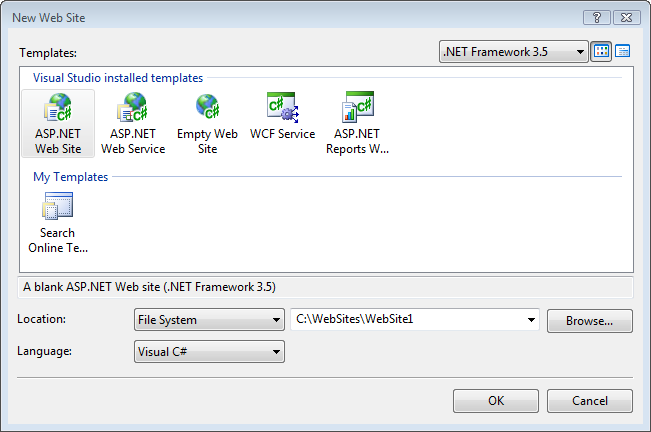
1. Create a new DNS **A** record where **Name** = **extranet** and **IP** = **192.168.150.1**.
2. Create a new Web application with the following values:
   * **IIS Web Site:** Create a new IIS web site
   * **Description:** (leave alone... this will automatically be changed as you sent the next two values)
   * **Port:** 80
   * **Host Header:** extranet.litwareinc.com
   * **Application Pool:** Use existing application pool & SharePointDefaultAppPool (Litwareinc\SP\_WorkerProcess)
   * **Database Server:** LitwareServer
   * **Database Name:** WSS\_Extranet
   * **Database Authentication:** Windows authentication (recommended)
3. Create a new site collection within the Web application created in step 2 above using the following values:
   * **Web Application:** http://extranet.litwareinc.com
   * **Title:** Litware Inc.
   * **Description:** Litware Inc. Publishing Site Web Site
   * **Address:** http://extranet.litwareinc.com
   * **Template Selection:** Publishing Portal (found under the Publishing tab)
   * **Primary Site Collection Administrator:** LITWAREINC\administrator

At this point you now have a new Web application and site collection. This site will be used as the "authoring site" where your company employees will go to edit the site content.

Exercise 2: Creating & configuring the FBA ASP.NET 2.0 database

Before you can setup an alternate access point for your authoring site for the world to see (with much more restrictive permissions). In this exercise you will create a new ASP.NET 2.0 database that will retain the users and roles used on the externally facing site (which you will create in the next exercise).

1. First, you need to create the ASP.NET 2.0 database that will contain the users and roles before you configure any providers or create users/roles. Run the utility provided by Microsoft to launch the ASP.NET SQL Server Setup Wizard... the utility can be found here: **c:\Windows\Microsoft.NET\Framework\v2.0.5027\aspnet\_regsql.exe**. When prompted, use the following values:
   * **Server:** LitwareServer
   * **Windows Authentication**
   * **Database:** LitwareFBA
2. With the database created, you need to grant a user access to the database. This will be the user account your SharePoint site will access the database as. To get this user account, check the identity of the application pool containing Web application created in exercise 1 previously. To save time, the application pool you used is the **SharePointDefaultAppPool** which is configured to execute using the **LITWAREINC\SP\_WorkerProcess** account. Using **SQL Server Management Studio** (available from **Start » All Programs » Microsoft SQL Server 2005 » SQL Server Management Studio**), add the **LITWAREINC\SP\_WorkerProcess** account to the **LitwareFBA** database and grant it the following roles: **db\_datareader** & **db\_datawriter**.
3. The next step involves creating the necessary membership & role providers, as well as creating a few users and roles in the database. Microsoft has included a simple web application to assist in managing the database, however it is only accessible when launched via Visual Studio. It's not so bad as it also gives you a good place to test your providers without adding the complexity of SharePoint.
4. Open Visual Studio and create a new **Visual C#**, **ASP.NET Web Site** on the **File System** in the following location: **c:\Student\Labs\03\_AuthenticationAuthorization\Lab\LitwareFbaWebSite**. Refer to the following image for more information:



1. The first step is to establish a connection to the FBA database. Replace the existing **<connectionStrings />** XML element with the following:

<connectionStrings>

<add name="LitwareFba"

connectionString="server=LitwareServer; database=LitwareFBA; Integrated Security=SSPI;"

providerName="System.Data.SqlClient" />

</connectionStrings>

1. Next, add the following XML within the **<system.web>** elements to define the membership and role providers:

<!-- membership provider -->

<membership defaultProvider="LitwareFbaSqlMembershipProvider">

<providers>

<add name="LitwareFbaSqlMembershipProvider"

type="System.Web.Security.SqlMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"

connectionStringName="LitwareFba"

enablePasswordRetrieval="false"

enablePasswordReset="true"

requiresQuestionAndAnswer="false"

applicationName="/"

requiresUniqueEmail="false"

passwordFormat="Hashed"

maxInvalidPasswordAttempts="5"

minRequiredPasswordLength="1"

minRequiredNonalphanumericCharacters="0"

passwordAttemptWindow="10"

passwordStrengthRegularExpression="" />

</providers>

</membership>

<!-- role provider -->

<roleManager enabled="true" defaultProvider="LitwareFbaSqlRoleProvider">

<providers>

<add name="LitwareFbaSqlRoleProvider"

type="System.Web.Security.SqlRoleProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"

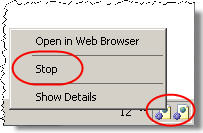
connectionStringName="LitwareFba"

applicationName="/" />

</providers>

</roleManager>

1. With the connection string and providers configured, you can now use Visual Studio to launch the Web application you can use to manage the database. Within Visual Studio, select **Website » ASP.NET Configuration**. The first thing you need to do is switch the site from **Integrated Authentication** to **Forms Authentication** by selecting the **Security** link and then **Select Authentication Type** in the **Users** container. Make sure the option **From The Internet** is selected... this is another way to say "Forms Based Authentication." Finally click **Done**.
2. With the security all configured, test the providers. Select the **Provider** tab, then click **Select a different provider for each feature (advanced)** and click the **Test** link next to the two providers defined the **web.config**: **LitwareFbaSqlMembershipProvider** & **LitwareFbaSqlRoleProvider**. If either test reports an error, go back and double check the web.config. Make sure you close the browser and stop the local running instances of ASP.NET (found in the system tray... refer to the following image) every time you rerun the test:



1. Now add two new users to the database. If it is not already active, select the **Security** tab and then **Create user** within the **Users** container.
2. On the **Create User** page, enter the following information for the new user, make sure the **Active User** checkbox is **checked** and click **Create User**:
   * **User Name:** brian.perry
   * **Password & Confirm Password:** pass@word1
   * **E-mail:** brian.perry@litwareinc.com
3. Repeat the step above for a second user which will be the administrator account on the anonymous access/FBA site:
   * **User Name:** FbaAdministrator
   * **Password & Confirm Password:** pass@word1
   * **E-mail:** fba.admin@litwareinc.com

At this point you have now confirmed you have a valid connection string, membership and role provider definitions. You also have created a database that contains a single user account which you will use later to test the site.

Exercise 3: Extending a new Web application with different authentication & enabling anonymous access

In this exercise you will create a second Web application that will provide a second link into the site collection created in exercise 1. It is this second Web application that you will configure to use the alternate authentication mechanism.

1. Create a new DNS A record where **Name = internet** and **IP = 192.168.150.1** (refer to lab #2, exercise #1 if you need a refresher on how to do this).
2. Launch Central Administration by selecting **Start » All Programs » Microsoft Office Server » SharePoint 3.0 Central Administration**.
3. From the **Central Administration** site, select the **Application Management** tab and then select **Create or extend Web application** under the **SharePoint Web Application Management** section.
4. On the **Create or Extend Web Application** page, select **Extend an existing Web application**.
5. On the **Extend Web Application to Another IIS Web Site** page, use the following formation to extend an existing Web application by creating a new Web application:
   * **Web Application:** http://extranet.litwareinc.com
   * **Description:** (leave alone... this will automatically be changed as you sent the next two values)
   * **Port:** 80
   * **Host Header:** internet.litwareinc.com
   * **Load Balanced URL / Zone:** Internet
6. Now it is time to configure the Web applications so they can both access the FBA ASP.NET 2.0 database. To do this you will add the connection string, membership provider and role provider definitions created in the Visual Studio Web Site project previously in this lab into the web.config files for each Web application. Open the **web.config** for the **extranet.litwareinc.com** site (found in this folder: **c:\Inetpub\wwwroot\wss\VirtualDirectories\extranet.litwareinc.com80**) and add the following XML below just after the closing **</SharePoint>** element and opening **<system.web>** element:

*Tip: Save yourself some time typing and copy the XML from the* web.config *in the Visual Studio Web Site project created previously in exercise 2. This applies to all XML in this step.*

<connectionStrings>

<add name="LitwareFba"

connectionString="server=LitwareServer; database=LitwareFBA; Integrated Security=SSPI;"

providerName="System.Data.SqlClient" />

</connectionStrings>

Next, add the following XML just after the opening XML <system.web> element:

<!-- membership provider -->

<membership defaultProvider="LitwareFbaSqlMembershipProvider">

<providers>

<add name="LitwareFbaSqlMembershipProvider"

type="System.Web.Security.SqlMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"

connectionStringName="LitwareFba"

enablePasswordRetrieval="false"

enablePasswordReset="true"

requiresQuestionAndAnswer="false"

applicationName="/"

requiresUniqueEmail="false"

passwordFormat="Hashed"

maxInvalidPasswordAttempts="5"

minRequiredPasswordLength="1"

minRequiredNonalphanumericCharacters="0"

passwordAttemptWindow="10"

passwordStrengthRegularExpression="" />

</providers>

</membership>

<!-- role provider -->

<roleManager enabled="true" defaultProvider="LitwareFbaSqlRoleProvider">

<providers>

<add name="LitwareFbaSqlRoleProvider"

type="System.Web.Security.SqlRoleProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"

connectionStringName="LitwareFba"

applicationName="/" />

</providers>

</roleManager>

Save your changes. Now do the same thing to the **web.config** for the **internet.litwareinc.com** site (found in this folder: **c:\Inetpub\wwwroot\wss\VirtualDirectories\internet.litwareinc.com80**).

1. With the two sites’ Web applications configured, you now need to configure the Central Administration site because you may need to manage the security on the Web applications from within Central Administration, therefore it needs the same changes to communicate with the FBA ASP.NET 2.0 database. Repeat the previous step for the **web.config** for the **Central Administration** site (found in this folder: **c:\Inetpub\wwwroot\wss\VirtualDirectories\####**).

However there is one difference. Change the **defaultProvider** attribute on the XML **<roleManager>** element to **AspNetWindowsTokenRoleProvider**. This is necessary because Central Administration still uses Windows Authentication for the role provider.

With all the web.config modifications complete, now you can turn on FBA on the http://internet.litwareinc.com site.

1. From the **Central Administration** site, select the **Application Management** tab and then select **Authentication providers** under the **Application Security** section.
2. On the **Authentication Providers** page, if it is not selected already, change the **Web Application** to **http://extranet.litwareinc.com**. Then select the **Internet** zone link.
3. On the **Edit Authentication** page, use the following information to complete the form and click **Save**:
   * **Authentication Type:** Forms
   * Check **Enable Anonymous Access**
   * **Membership Provider Name:** LitwareFbaSqlMembershipProvider
   * **Role Manager Name:** LitwareFbaSqlRoleProvider
4. Now you need to add users to the site. Browse to the **http://extranet.litwareinc.com** site and select **Site Actions » Site Settings » People And Groups** and then select **New** button.
5. On the **Add Users: Litware Inc.** page, use the following information to complete the form and then click **OK**:
   * **Add Users:** brian.perry (press [CRTL]+[K] or select the icon C:\Development\Writing\Courses\WCM401\trunk\Student Download\Labs\03_AuthenticationAuthorization\Figures\CheckNames.jpg to validate the name)
   * Give Permission / Add users to a SharePoint group: Litware Inc. Visitors [Read]
6. See if everything is working correctly. Browse to **http://extranet.litwareinc.com**... you should be able to open the site with no problem. Next, browse to **http://internet.litwareinc.com**... you should be prompted to sign in. Use the credentials for the **brian.perry** account.
7. The final touch is to configure the http://internet.litwareinc.com site to allow for anonymous users to access the site... not prompting them to login to the site. In a previous step, the Web application was configured for anonymous access... but that does not mean SharePoint is allowing it. To configure the site for anonymous access, you need to login as a user who has administrative level rights. No user has those rights on the http://internet.litwareinc.com site yet though... so you're caught in a catch-22. No fear... SharePoint now includes a way to grant rights to an entire web application without having rights to that Web application (note, this is ~only~ a farm administration level setting). To do this, open **Central Administration**, select the **Application Management** tab and then select **Policy for Web application** in the **Application Security** section. Verify you have the correct Web application selected (in this case, **http://extranet.litwareinc.com**).
8. On the **Policy for Web Application** page, select **Add Users**.
9. On the **Add Users** page, make sure the **http://extranet.litwareinc.com** Web application is selected, select the **Internet** zone and click **Next**. Then, enter the user **FbaAdministrator** and press **[CTRL]+[K]** or select the icon C:\Development\Writing\Courses\WCM401\trunk\Student Download\Labs\03_AuthenticationAuthorization\Figures\CheckNames.jpg to validate the name. Then check **Full Control** for the permission and click **Finish**. The FbaAdministrator account now has full unrestricted access to the http://internet.litwareinc.com site, the Internet zone for http://extranet.litwareinc.com.
10. Now browse to **http://internet.litwareinc.com** site, login as the **FbaAdministrator** and select **Site Actions » Site Settings**, then select **Modify All Site Settings**.
11. On the **Site Settings** page, select **Advanced Permissions**.
12. On the **Advanced Permissions** page, select **Settings » Anonymous Access**.
13. On the **Change Anonymous Access Settings: Litware Inc.** page, select **Entire Web Site** and click **OK**.
14. Now open a new browser, browse to **http://internet.litwareinc.com** and you should not have to login to the site.

At this point you have now completed setting up two authentication paths into your site. One path allows your corporate employees to access the site using their corporate AD credentials and the other allows for anonymous access and FBA authentication for certain protected areas.

Exercise 4: Configuring a password protected area of the anonymous access site

In this exercise, you will configure a subsite within the http://internet.litwareinc.com site to require authentication before browsing to that site. If the user does not have permission or is not logged in, they will not see the subsite.

1. Configure the **Press Releases** site so that it is not available to anonymous users. Browse to **http://internet.litwareinc.com/PressReleases** and login using the **FbaAdministrator** account. Then select **Site Actions » Site Settings » Modify All Site Settings** and then select **Advanced Permissions**.
2. On the **Permissions: Press Releases** page, select **Actions » Edit Permissions** to break permission inheritance in order to enable anonymous access.
3. On the **Permissions: Press Releases** page, select **Settings » Anonymous Access**.

*Note: If you do not see an option for anonymous access, you may need to break permission inheritance from the Press Releases site from its parent site.*

1. On the **Change Anonymous Access Settings** page, select **Nothing** and click **OK**.
2. Open a new browser and navigate to the **http://internet.litwareinc.com**. Notice how the Press Releases section no longer appears? Now login as one of the users you added to the site and notice how it comes back.