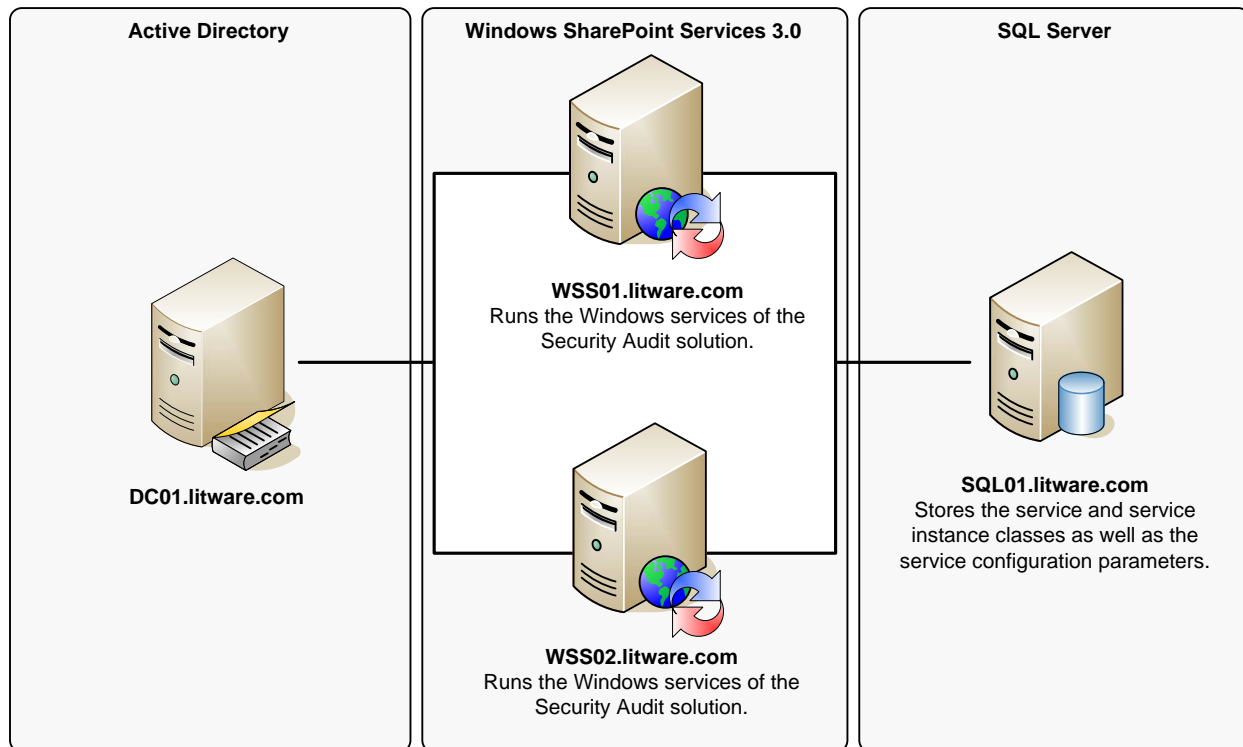


Deploying the Final Integrated Security Audit Solution

The following procedures describe step by step how to deploy the final version of the Security Audit solution in a SharePoint farm test environment with two front-end servers and a separate computer SQL Server. For a complete security monitoring solution, you must install and provision the Security Audit solution on all front-end servers.



Prerequisites:

- You have completed the step-by-step instructions to install and configure a SharePoint development environment, as outlined in the worksheet "*Deploying a WSS 3.0 Farm in a Test Environment*" that you can find in the companion material.

To deploy the SharePoint solution package in the farm environment:

1. Log on to WSS01 as Litware\Administrator and copy the **Step6** folder from the companion material to the server's **C:** drive.
2. Click **Start** and then click **Command Prompt**.
3. Type **cd /D "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Bin"** and press Enter to change into the SharePoint Bin directory.
4. Type **Stsadm.exe -o addsolution -filename C:\Step6\SPSecAudit.wsp** and press Enter to add the custom solution to SharePoint.
5. Type **Stsadm.exe -o deploysolution -immediate -allowgacdeployment -name SPSecAudit.wsp -force** and press Enter to deploy the custom solution in the SharePoint farm.

6. Type **Stsadm.exe -o execadmsvcjobs** and press Enter to start processing the deployment job in the SharePoint farm.
7. Type **Stsadm.exe -o displaysolution -name SPSecAudit.wsp** and press Enter to verify that the solution is fully deployed in the SharePoint farm. Make sure the deployment status is true (**<Deployed>TRUE</Deployed>**) or wait a few seconds and repeat this the displaysolution command.
8. Type **Stsadm.exe -o copyappbincontent** and press Enter to deploy the admin content in the Central Administration site.
9. Type **Stsadm.exe -o activatefeature -filename SecurityAuditList\feature.xml -url http://wss** and press Enter to activate the custom list feature in the http://wss Web application.
10. Close the **Command Prompt**.

To install the Security Audit Windows Services on WSS01 and WSS02:

1. Logged on to WSS01 as Litware\Administrator, click **Start** and then click **Computer**.
2. Open the **C:\Step6** folder and double-click **SecurityAuditSetup.msi**.
3. In the **Security Audit** dialog box, informing you that this setup requires the .NET Framework version 3.5, click **Yes** to download the framework from the Internet.
4. On the **.NET Framework 3.5 Service Pack 1** Web page, click **Install Now**.
5. Continue to confirm **Security Audit** dialog boxes by clicking **Add** twice and then **Close**, and click on **Install Now** again.
6. In the **File Download – Security Warning** dialog box, click **Run**.
7. In the **Internet Explorer – Security Warning** dialog box, verify that the file publisher is **Microsoft Corporation**, and then click **Run**.
8. In the **Microsoft .NET Framework 3.5 SP1 Setup** dialog box, select **I have read and accept the terms of the License Agreement** radio button, and then click **Install**.
9. Setup is now downloading the .NET Framework 3.5 SP1 from the Internet and then starts the installation routine.
10. In the **Setup Complete** dialog box, click **Exit**.
11. In the **Microsoft .NET Framework 3.5 SP1 Setup** dialog box informing you that you must reboot the computer, click **Restart Now**.
12. Log on as Litware\Administrator again, click **Start**, click **Computer**, open the **C:\Step6** folder and double-click **SecurityAuditSetup.msi** again.
13. In the **Security Audit** dialog box, click **Next**.
14. In the **Select Installation Folder** dialog box, accept the defaults and click **Next**.
15. In the **Confirm Installation** dialog box, click **Next**.
16. In the **Installation Complete** dialog box, click **Close**.
17. Repeat these steps on WSS02.

To Provision the Service Objects on WSS01 and WSS02:

1. Logged on to WSS01 as Litware\Administrator, click **Start** and then click **Command Prompt**.
2. Type **cd /D "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Bin"** and press Enter to change into the SharePoint Bin directory.

3. Type **Stsadm.exe -o securityevents -install -username "LITWARE\SPDefaultSite" -password 1qw\$t9x -provision** and press Enter to provision service and service instance objects for the Windows services in the SharePoint configuration.
4. Close the **Command Prompt**.
5. Repeat these steps on WSS02.

To create a custom SharePoint list for Security Entries:

1. Logged on to WSS01 as Litware\Administrator, click **Start**, click **Run**, type **http://wss**, and then click **OK**.
2. Click **Site Actions**, and then click **Create**.
3. Under **Custom Lists**, click **Security Audit List**.
4. On the **New** page, under **Name**, type **Security Audit** and then click **Create**.
5. Verify that the **Security Audit** list is created successfully.
6. Close Internet Explorer.

To Configure the Windows Services in SharePoint 3.0 Central Administration:

1. Logged on to WSS01 as Litware\Administrator, click **Start**, point to **Administrative Tools**, and then click **SharePoint 3.0 Central Administration**.
2. On the home page, under **Farm Topology**, click on **WSS01**.
3. Click on **Security Audit Event Receiver Service** and then on the **Security Audit: Security Event Receiver Settings** page, under **Target Site**, verify that the **Site URL** is **http://wss**, that the target **List Name** is **Security Audit**, and that the **Audit Mode** is **Failure Audit**.
4. Click **OK** and then on the **Services on Server: WSS01** page next to the **Security Audit Event Receiver Service** click **Start**.
5. In the **Windows Internet Explorer** dialog box, informing you that both services will be started on WSS01, click **OK**.
6. On the **Services on Server: WSS01** page, under **Server**, click on the arrow, select **Change Server**, and then click on **WSS02**.
7. On the **Services on Server: WSS02** page next to the **Security Audit Event Receiver Service** click **Start**.
8. In the **Windows Internet Explorer** dialog box, informing you that both services will be started on WSS02, click **OK**.
9. Verify that the **Status** switches to **Starting**. Wait a few seconds and then refresh the page. When the SharePoint Timer service has processed the service control job, the **Status** will switch to **Started**.
10. Close Internet Explorer and log off on WSS01 and WSS02, and then attempt to log on to WSS01 and WSS02 by using the Litware\Administrator account with an *incorrect* password in order to generate security events.
11. Log on to WSS01 again as Litware\Administrator, click **Start**, click **Run**, type **http://wss**, and then click **OK**.
12. In the left navigation pane, under **Lists**, click **Security Audit**.
13. Note the **EntryType: FailureAudit** heading, expand the node and if an **Internet Explorer** dialog box is displayed informing you that the about:blank site is blocked, click **Add** twice, and then click **Close**.

14. Verify that the Security Audit solution has created Security Audit list items for the failed logon security events. Note that the **MachineName** column lists both, events from **WSS01.litware.com** and **WSS02.litware.com** which confirms that the Security Audit solution is successfully tracking Security events on both front-end servers.
15. Log off on WSS01.