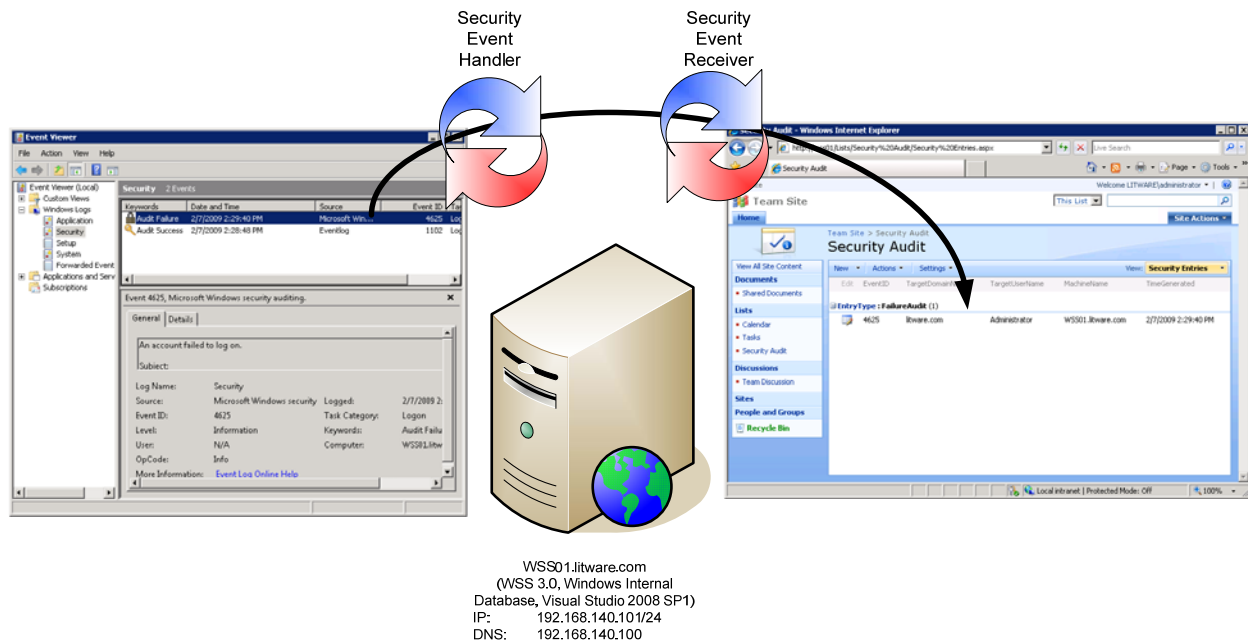


Deploying the Non-Integrated Security Audit Solution

The following procedures describe step by step how to deploy the non-integrated version of the Security Audit Solution, which consists of two Windows services and a custom SharePoint list for security entries. The Security Event Handler service registers as an event sink with the Event Log subsystem in order to receive the audit entries that the system writes into the Security event log. It then passes the information to the Security Event Receiver service through a Named Pipe. The Security Event Receiver service then creates a corresponding list item in the SharePoint Security Audit list.



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 Development Environment"* that you can find in the companion material.

To deploy the custom SharePoint list:

1. Log on to WSS01 as Litware\Administrator and copy the **Step1** 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:\Step1\SPSecAudit.wsp` and press Enter to add the custom solution to SharePoint.
5. Type `Stsadm.exe -o deploysolution -local -allowgacdeployment -name SPSecAudit.wsp -force` and press Enter to deploy the custom solution in the SharePoint farm.

6. Type **Stsadm.exe -o activatefeature -filename SecurityAuditList\feature.xml -url http://wss01** and press Enter to activate the custom list feature in the http://wss01 Web application.
7. Close the **Command Prompt**.

To create a custom SharePoint list for Security Entries:

1. Logged on to WSS01 as Litware\Administrator, click **Start**, click **Run**, type **http://wss01**, 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.

To install the Security Audit Windows Services:

1. Logged on to WSS01 as Litware\Administrator, click **Start** and then click **Computer**.
2. Open the **C:\Step1** folder and double-click **SecurityAuditSetup.msi**.
3. In the **Security Audit** dialog box, click **Next**.
4. In the **Select Installation Folder** dialog box, accept the defaults and click **Next**.
5. In the **Confirm Installation** dialog box, click **Next**.
6. In the **Installation Complete** dialog box, click **Close**.
7. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
8. In Registry editor, open the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityEventReceiver\Parameters** key.
9. Verify that the **ListName** parameter matches the name of your Security Audit list.
10. Change the **SiteURL** to match the URL of your SharePoint site, such as **http://wss01**.
11. Click **OK** and close Registry editor.

To test the Security Audit Windows Services:

1. Logged on to WSS01 as Litware\Administrator, click **Start**, point to **Administrative Tools**, and then click **Services**.
2. Right-click the **Security Event Handler** service and click **Start**.
3. Verify that both, **Security Event Handler** and **Security Event Receiver** are started successfully.
4. Log off from WSS01 and then attempt to log on by using the Litware\Administrator account with an *incorrect* password in order to generate a security event.
5. Log on again as Litware\Administrator, click **Start**, click **Run**, type **http://wss01**, and then click **OK**.
6. In the left navigation pane, under **Lists**, click **Security Audit**.
7. 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**.

8. Verify that the Security Audit solution has created a Security Audit list item for the failed logon security event. Note that the service performs this task in the background. If the entry does not appear immediately, refresh the Web page in Internet Explorer.
9. Log off on WSS01.