Lab Objective

Learn how to use the Event Viewer

**Lab Procedures**

**Step 1. Looking at Events**

**1.** Log on to the Server01 server using the **Administrator** account and the password **Password01**. The Server Manager console opens.

**2.** When Server Manager opens, open the Toolsmenu and select Event Viewer. The Event Viewer console opens.

**3.** Expand the Windows Logs folder and click the System log. The contents of the log appear in the detail pane.

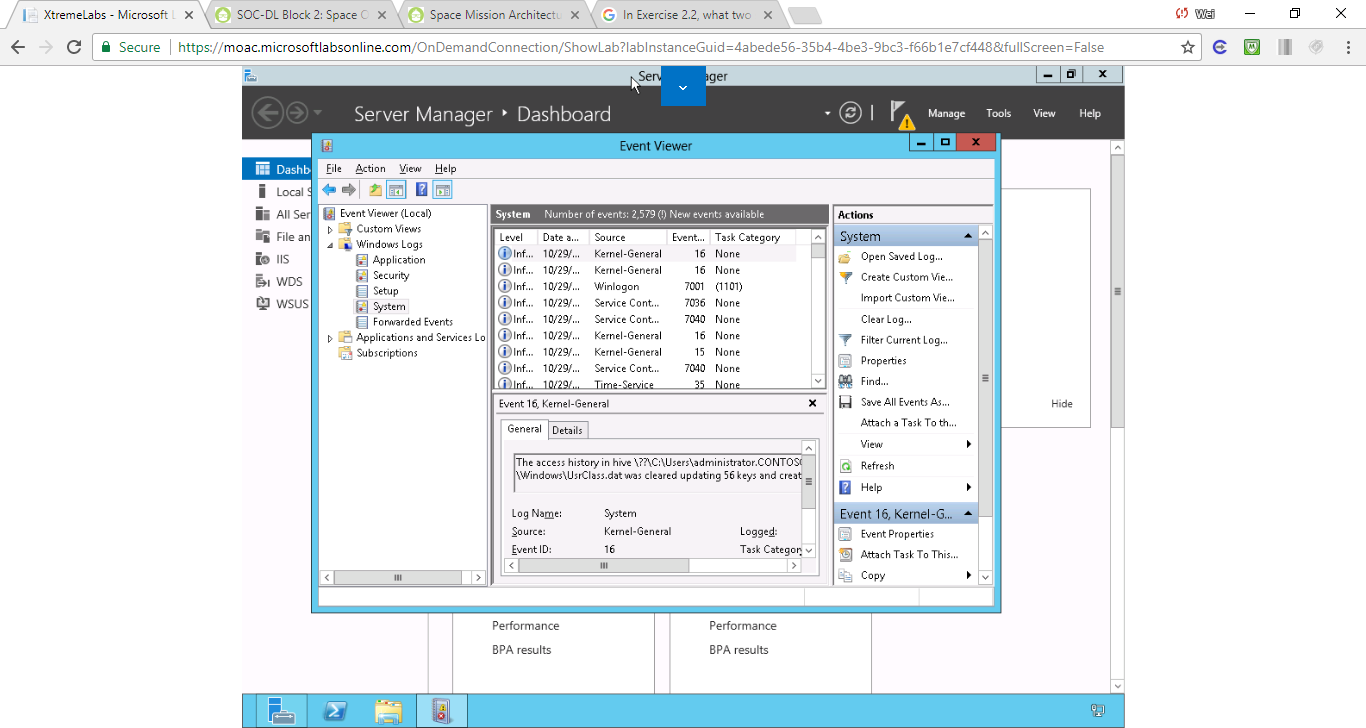


Figure 2579 events appear in the System log

**4.** From the Action menu, select Filter Current Log. The Filter Current Log dialog box appears.

**5.** In the Event Level area, select the Critical and Warning check boxes. Then click OK.

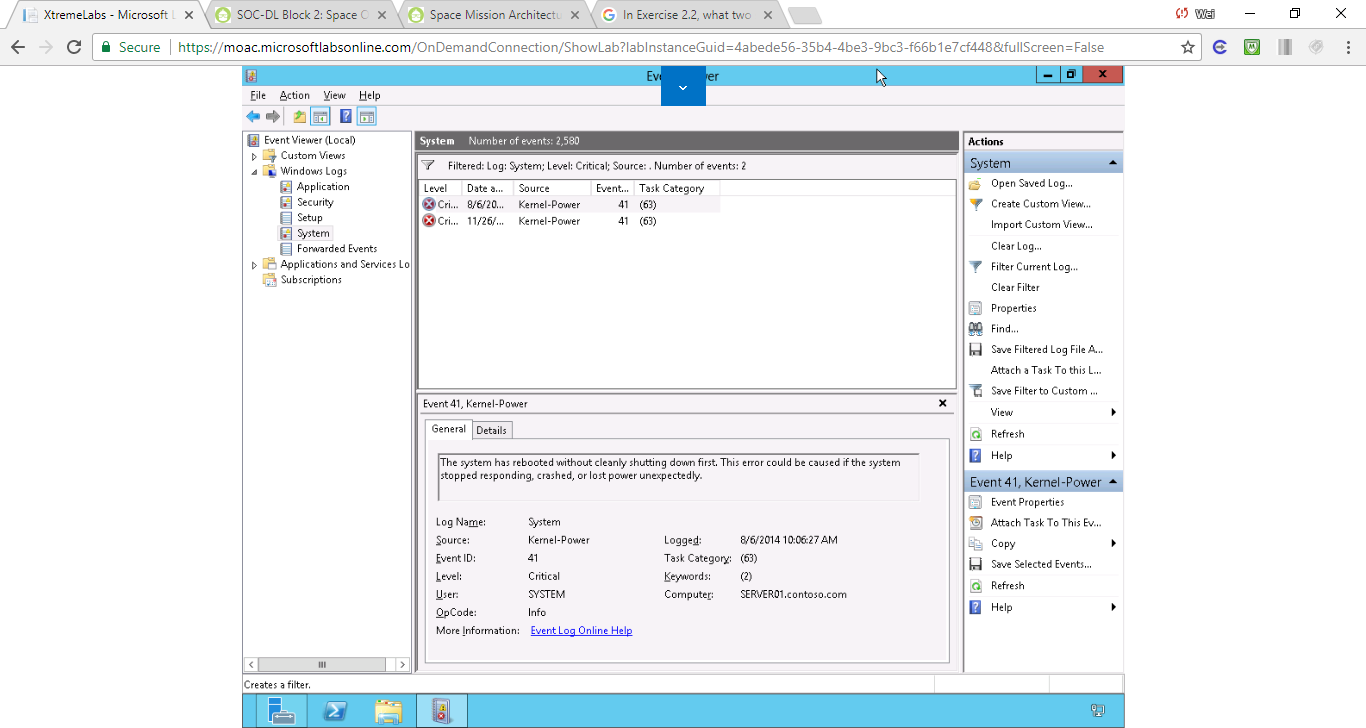


Figure . 2 critical events appear in the System log now

**6.** From the Action menu, select Create Custom View. The Create Custom View dialog box appears.

**7.** In the Logged drop-down list, select Last 7 days.

**8.** In the Event Level area, select the Critical and Warningcheck boxes.

**9.** Leave the By log option selected and, in the Event logs drop-down list, select the Application, Security, and System check boxes, as shown in Figure 3-1.

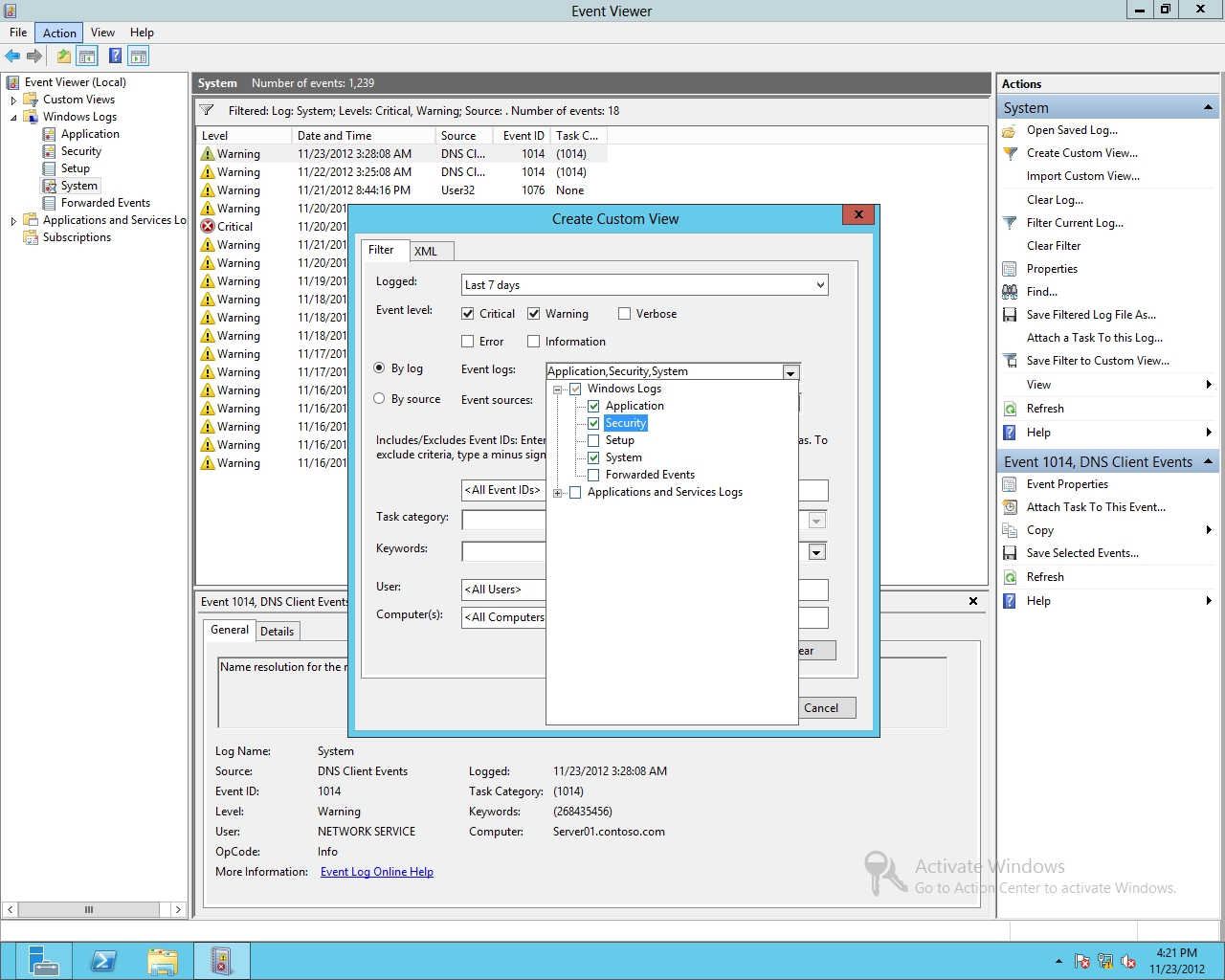


Figure 3-1

Selecting the type of logs

**10.** Click OK. The Save Filter to Custom View dialog box appears.

**11.** In the Name text box, type **Critical & Warning**. Then click OK. The Critical & Warning view you just created appears in the Custom Views folder.

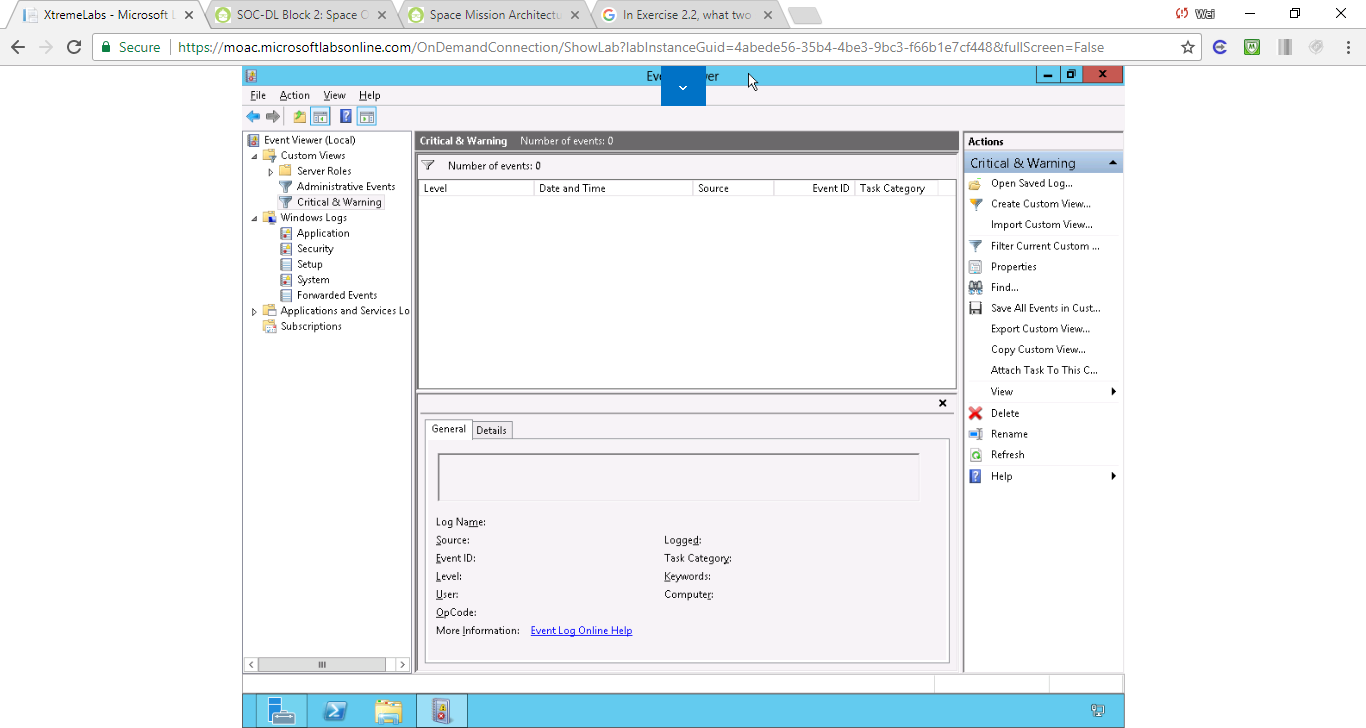


Figure 3 In the Name text box, type Critical & Warning. Then click OK. The Critical & Warning view you just created appears in the Custom Views folder. No event appears in the Critical & Warning custom view.

**12.** Right-click System (under Windows Logs) and click Clear Filter.

**13.** Leave the Event Viewer console open for the next exercise.

**Step 2. Adding a Task to an Event**

**1.** Using Server Manger, open the Tools menu and click Services. The Services console opens.

**2.** Scroll down and right-click Print Spooler and click Restart.

**3.** Go back to the Event Viewer. You should have two new entries in the System Logs with the Event ID of 7036. The one should say “The Print Spooler service entered the stopped state,” as shown in Figure 3-2. Right-click this event and click Attach Task to This Event.

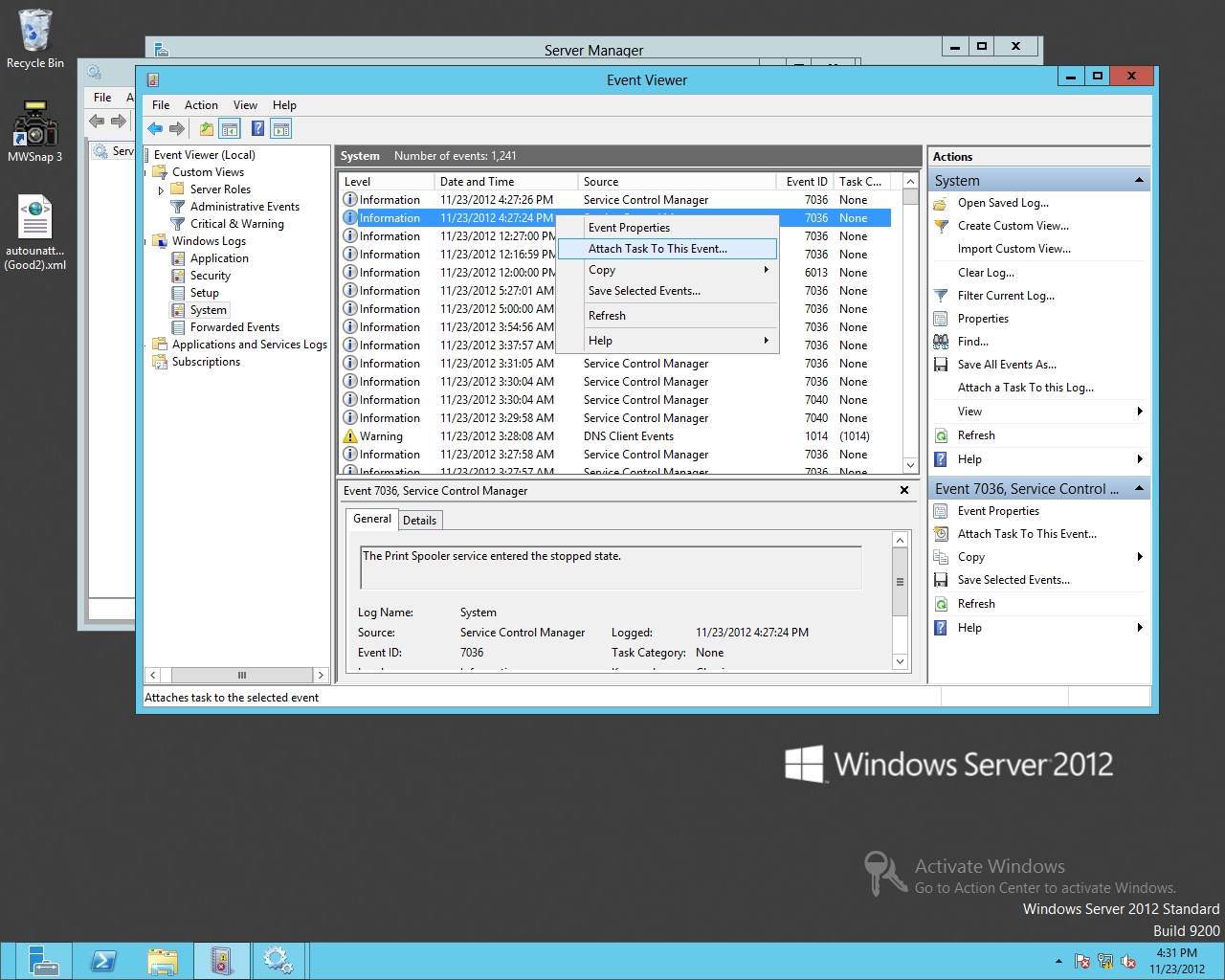


Figure 3-2

Attaching a task to an event

**4.** When the Create Basic Task Wizard starts, click Next.

**5.** When the *When a Specified Event Is Logged* page opens, click Next.

**6.** On the Action page (see Figure 3-3), make sure Start a program is selected and click Next.

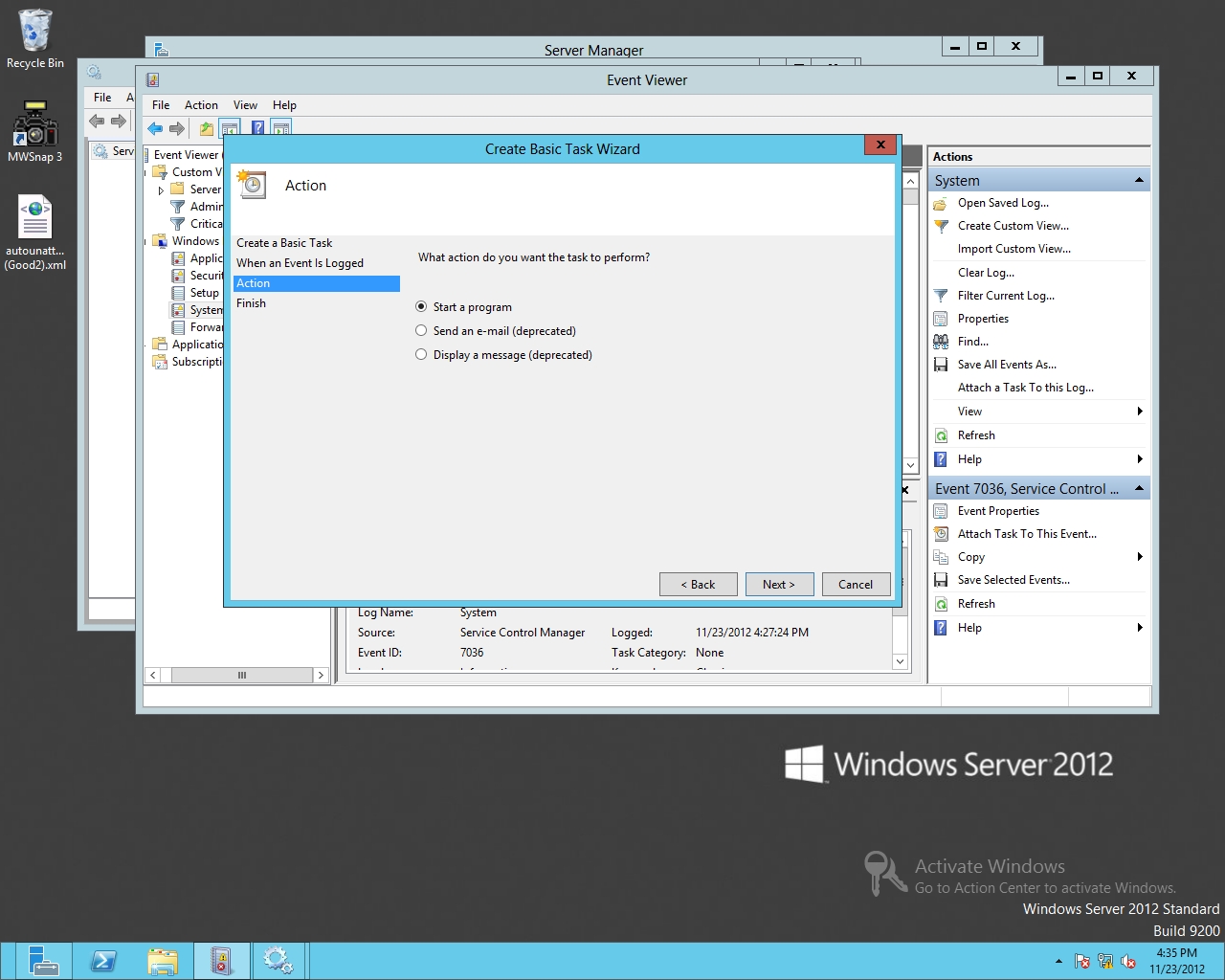


Figure 3-3

Selecting the task to perform

**7.** On the Start a Program page, type **Notepad** in the Program/script text box, as shown in Figure 3-4. Click Next.

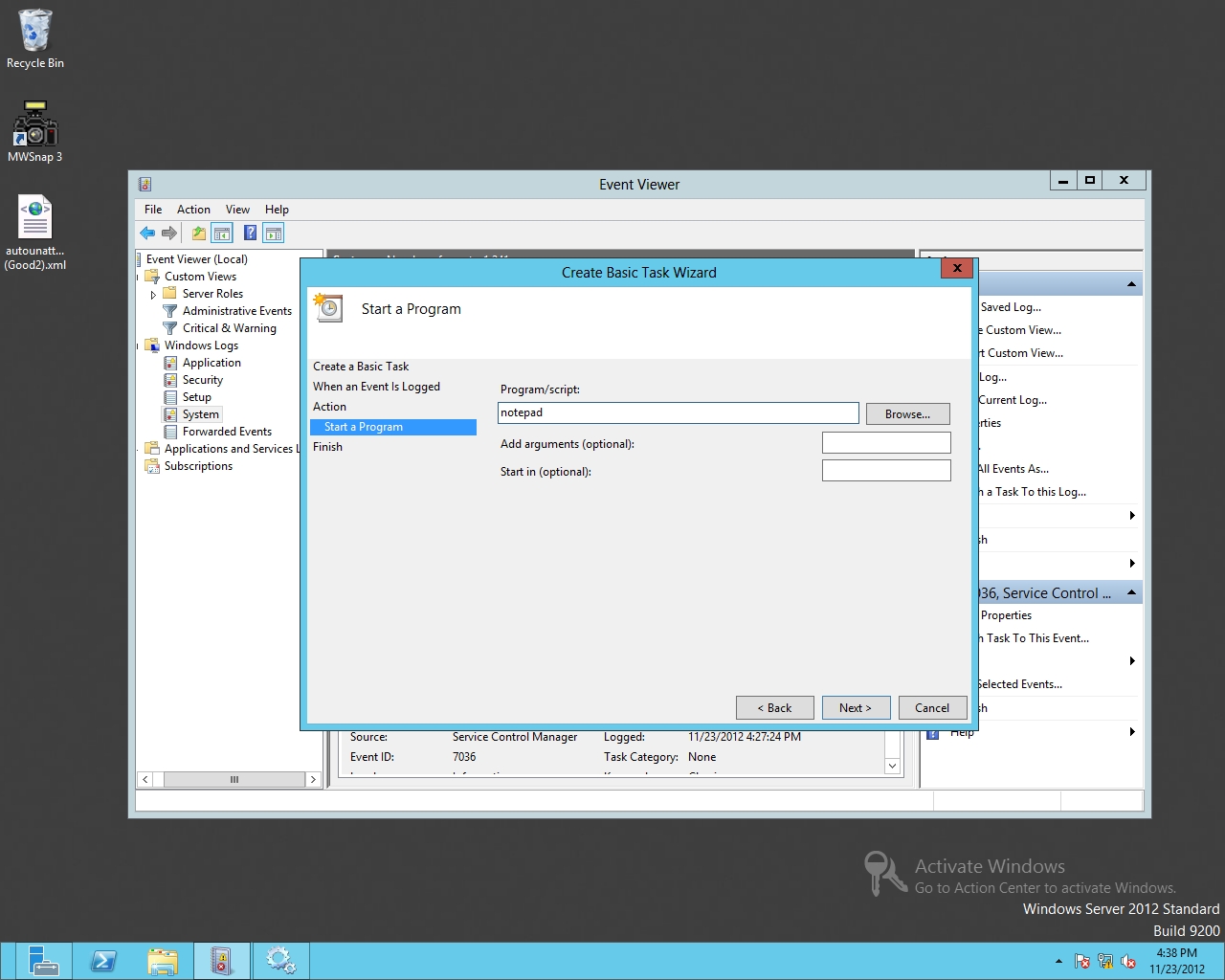


Figure 3-4

Specifying a program to start

**8.** On the Summary page, click Finish.

**9.** When an Event Viewer dialog box appears, click OK.

**10.** Close the Event Viewer.

**11.** Go back to the Services console. Right-click the Print Spooler service and click Restart. Notepad should have opened.

**12.** Go back to the Server Manager. Open the Tools menu and click Task Scheduler. Task Scheduler opens.

**13.** Expand the Task Scheduler Library and click Event Viewer Tasks.

**14.** Right-click the *System\_Service Control Manager\_7036* task and click Delete, as shown in Figure 3-5.

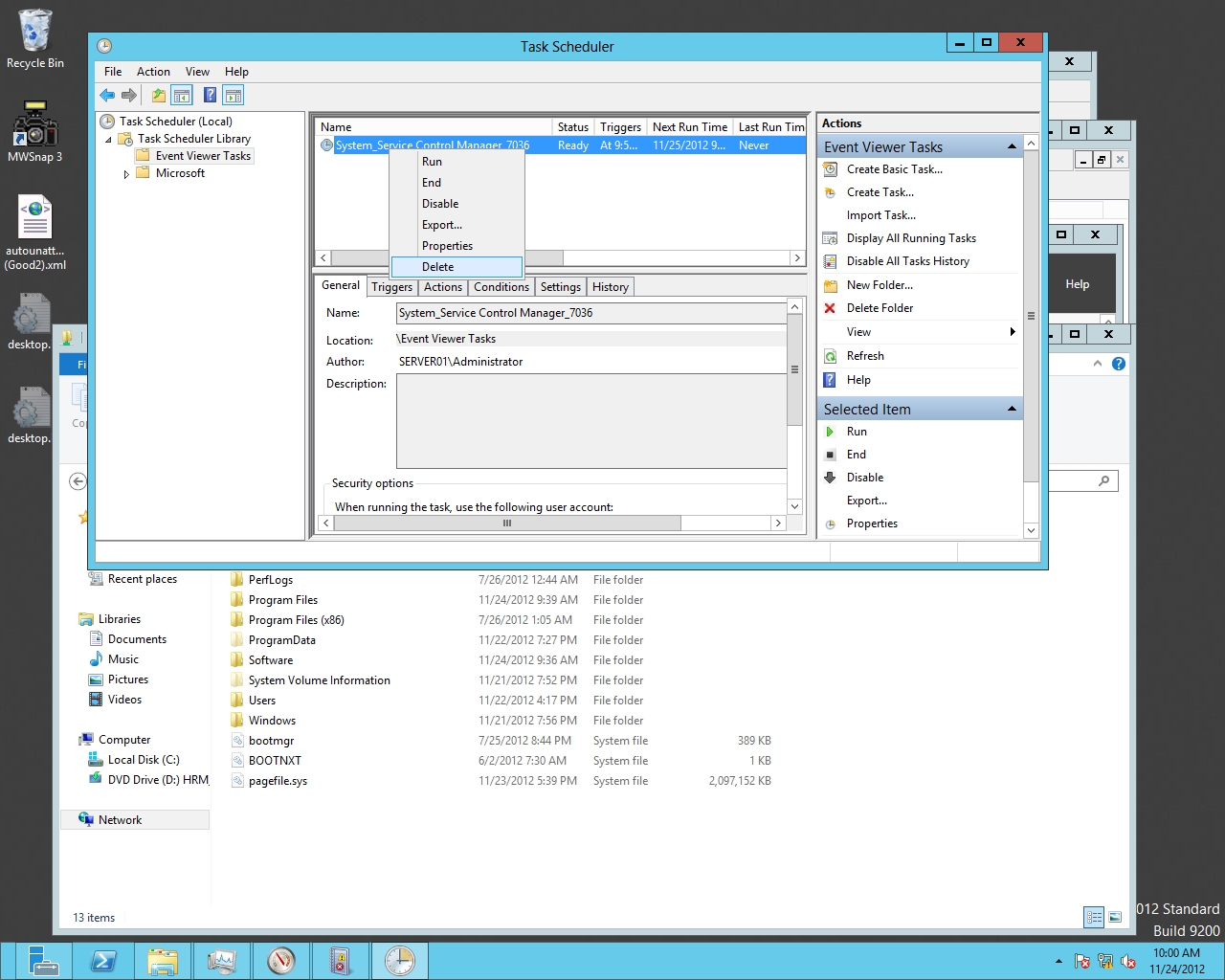


Figure 3-5

Deleting a task from Task Scheduler

**15.** When it asks if you want to delete this task, click Yes.

**16.** Close Task Scheduler, the Services console, and Notepad.

**Step 3. Creating a Subscription**

**1.** Restart **RWDC01** and login using the **contoso\Administrator** account and the password **Password01**. Log on to **Server02** using the **contoso\Administrator** account and the password **Password01**. The Server Manager console opens.

**2.** On Server02, right-click Start and choose Command Prompt (Admin).

**3.** At the command prompt, execute the following command:

winrm quickconfig

It is fine that the service is already running.

**4.** To add the collecting computer name to the Administrators group, execute the following command:

net localgroup “Administrators” Server01$@contoso.com /add

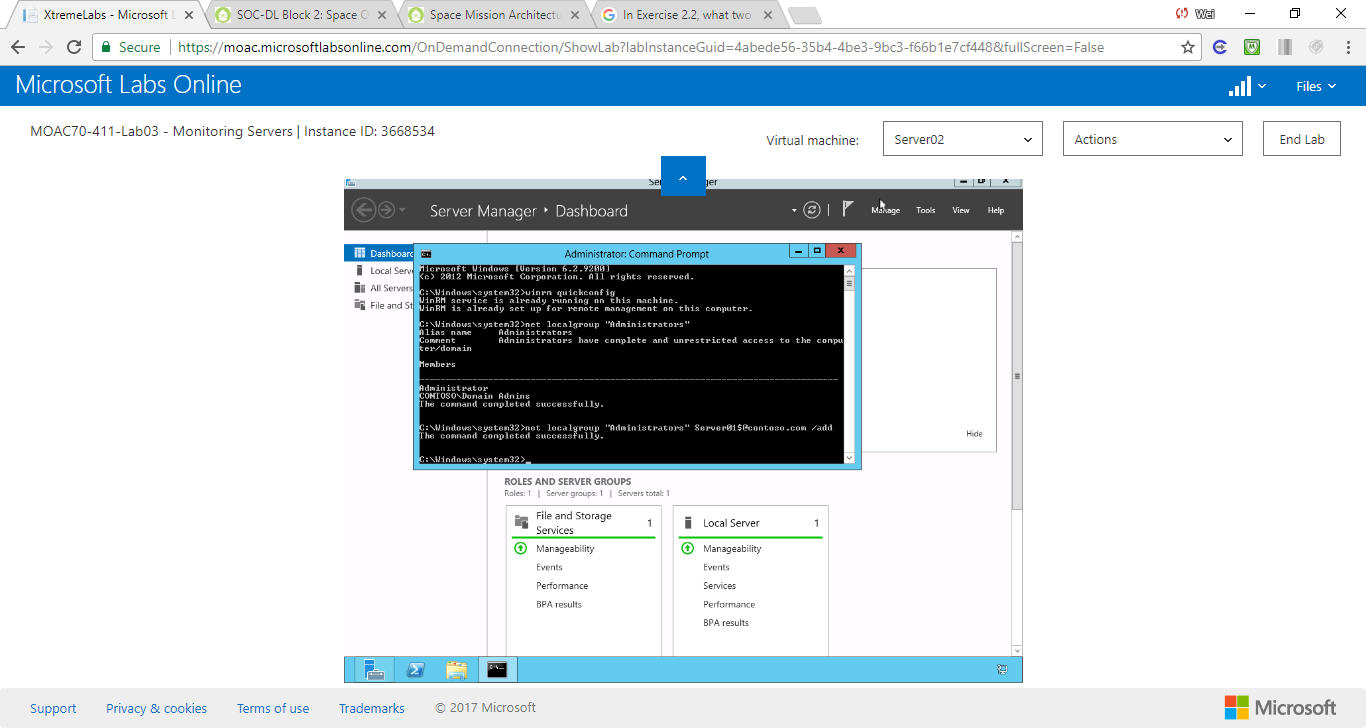


Figure . Execute the command: net localgroup “Administrators” Server01$@contoso.com /add

**5.** If a message appears, indicating that changes must be made, type **Y** and then press Enter.

**6.** Open the Event Viewer.

**7.** Click Subscriptions. When it asks if you want to start the service and configure the service to automatically start, click Yes.

**8.** Close the Command Prompt window.

**9.** On Server01, right-click Start and choose Command Prompt (Admin).

**10.** On Server01, at the command prompt, execute the following command:

wecutil qc

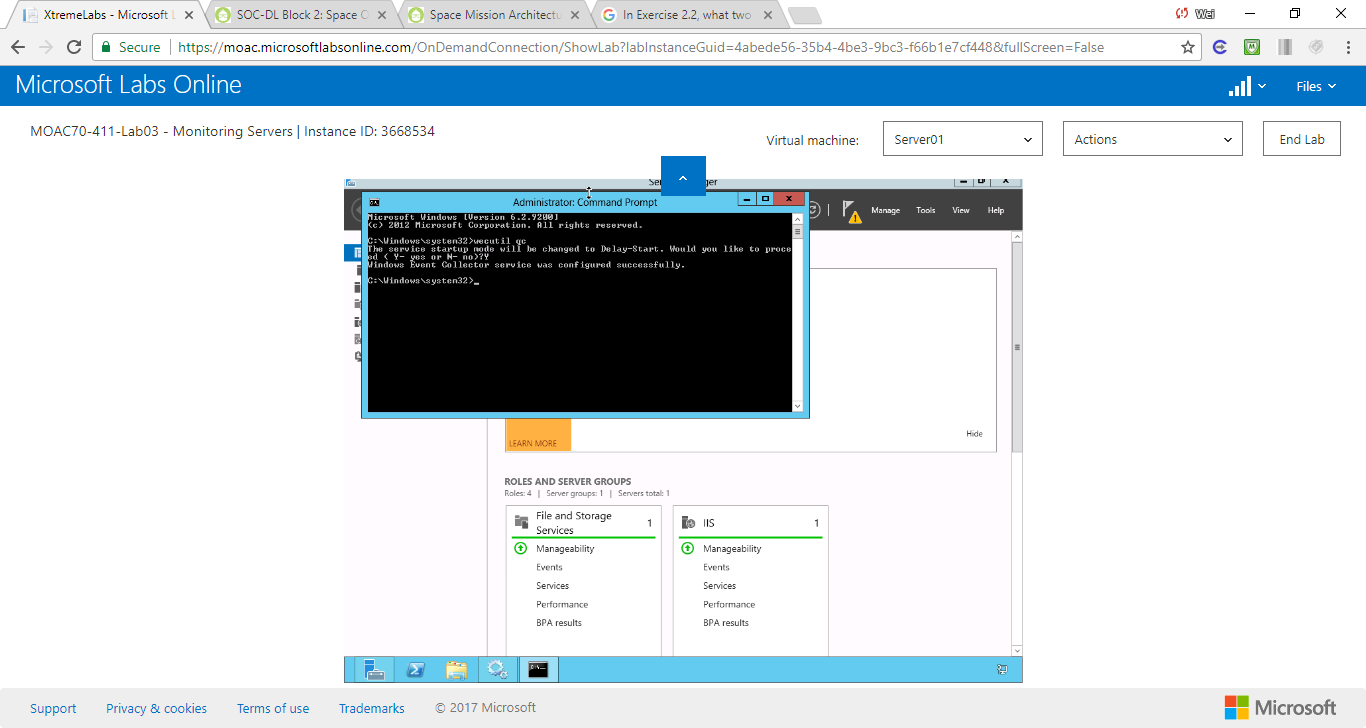


Figure Execute command: wecutil qc

**11.** If you are asked if you would like to proceed, type **Y** and press the Enter key.

**12.** Close the Command Prompt window.

**13.** Open Event Viewer.

**14.** On the Event Viewer, right-click Subscriptionsand choose Create Subscription (see Figure 3-6). The Subscription Properties dialog box opens.

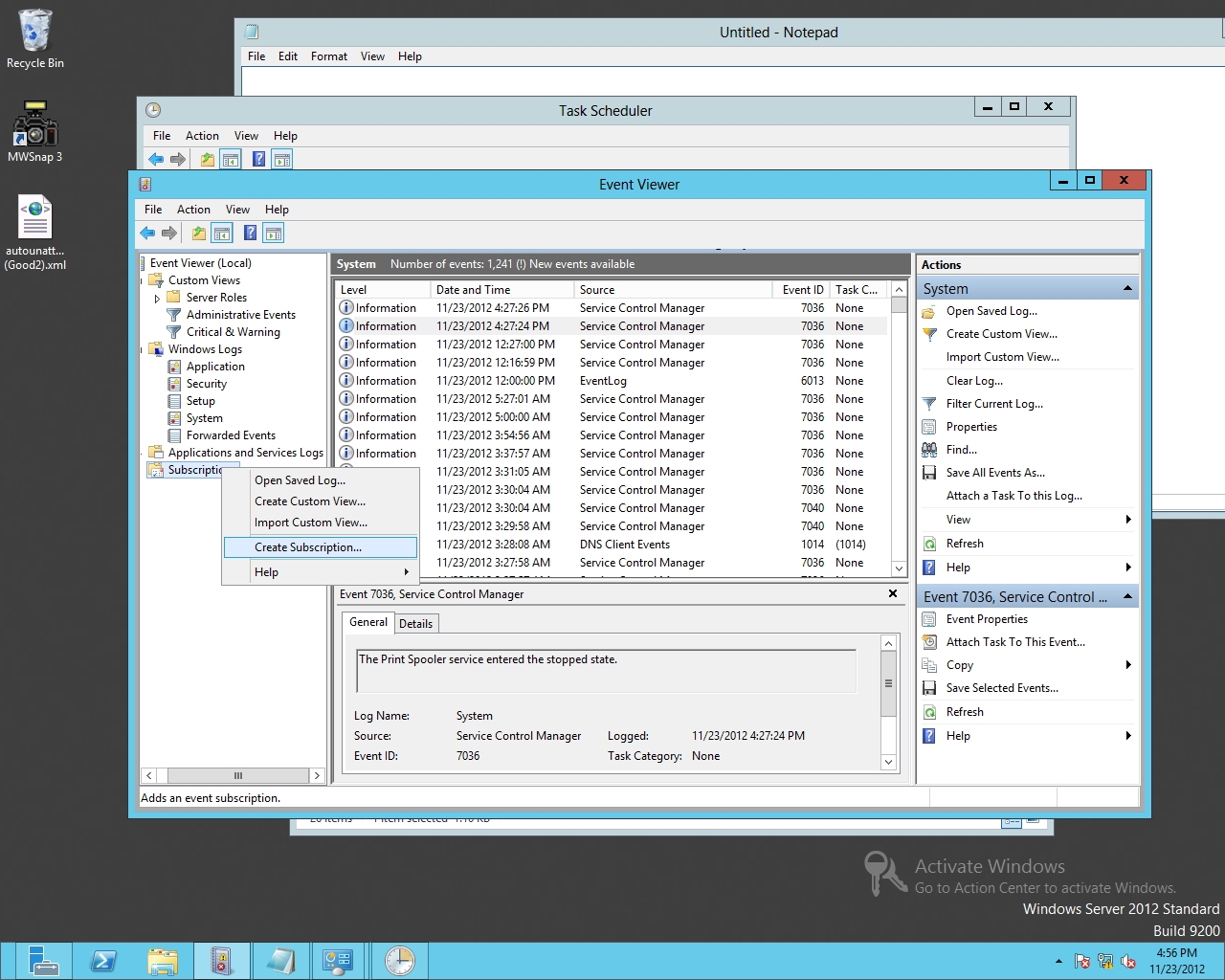


Figure 3-6

Creating a subscription

**15.** In the Subscription name text box (as shown in Figure 3-7), type **Server02**.

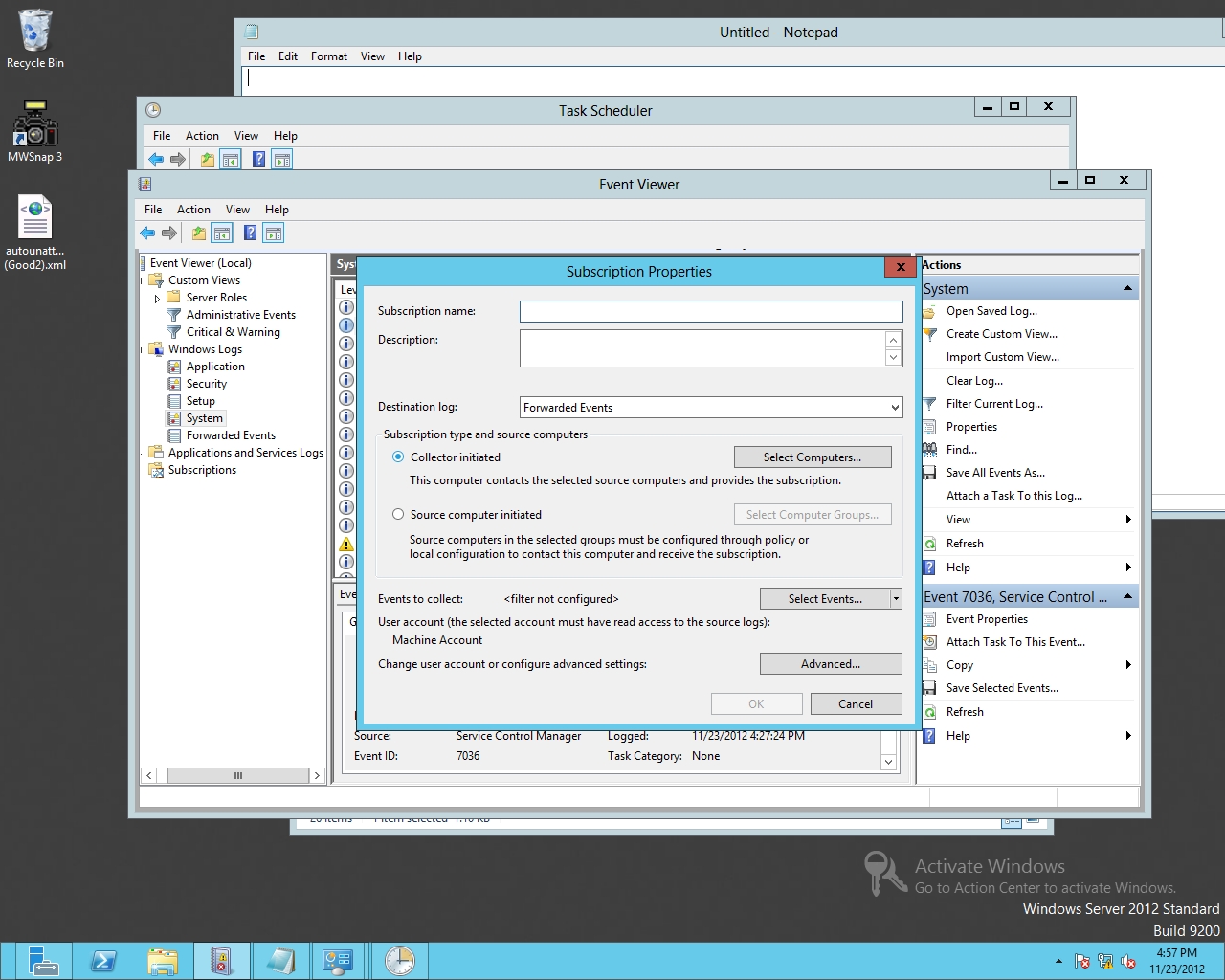


Figure 3-7

Specifying the Subscription Properties

**16.** Click Select Computers. The Computers dialog box opens.

**17.** Click Add Domain Computers. Type **Server02** in the Enter the object name to select text box and click OK.

**18.** If it asks you to specify a network password, use the username and password for contoso.com\administrator.

**19.** Click OK to close Computers dialog box.

**20.** Click Select Events. The Query Filter dialog box opens.

**21.** For Event Logs, click System logs.

**22.** Under Event level, type **7036** in the Includes/Excludes Event ID: text box, as shown in Figure 3-8. Click OK to close Query Filter dialog box.

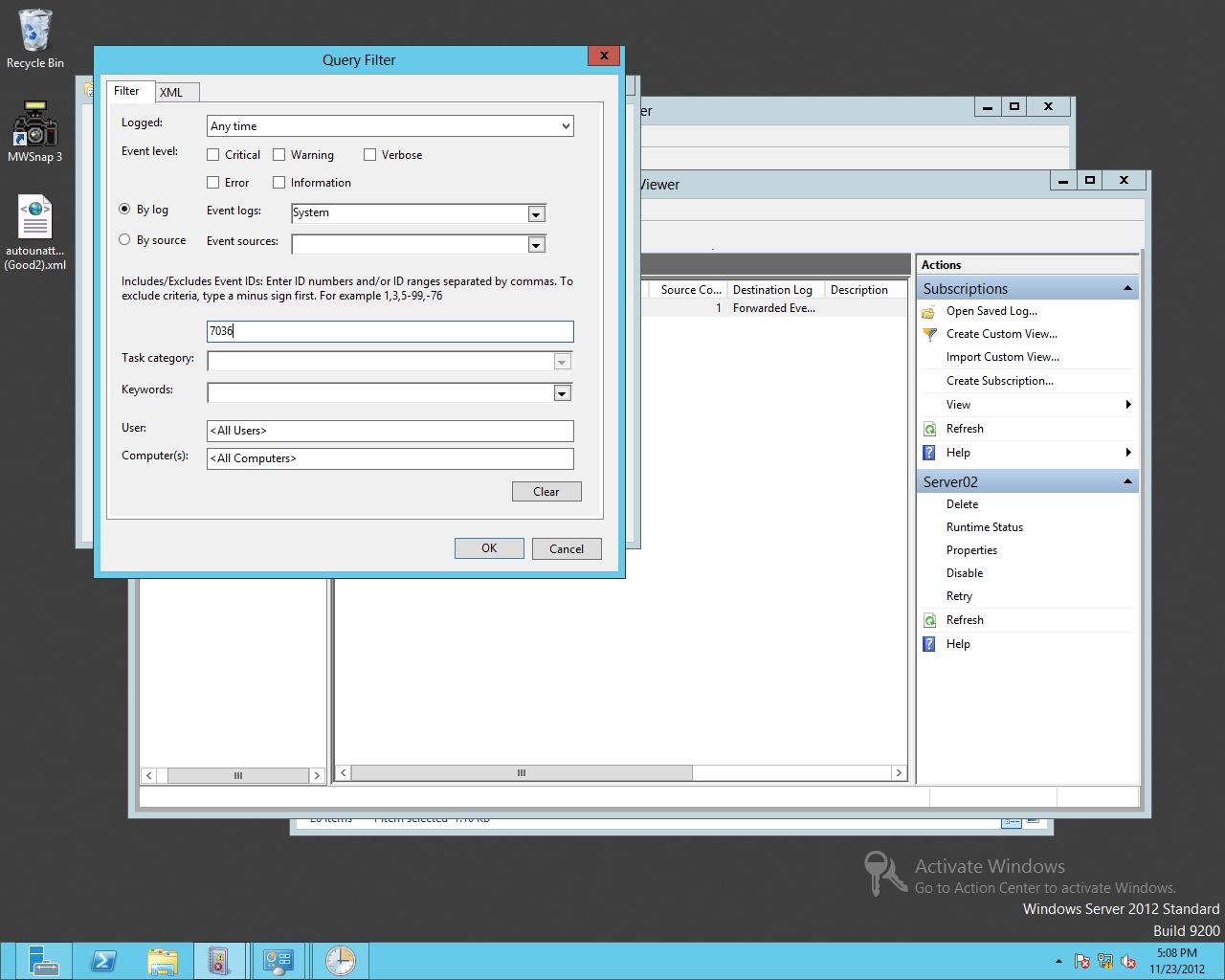


Figure 3-8

Specifying the Event to filter

**23.** Click OK to close the Subscription Properties dialog box.

**24.** On Server02, open the Servicesconsole. Right-click Print Spooler and click Restart. Close the Services console.

**25.** Go back to Server01. On the Event Viewer, click Forwarded Events under Windows Logs.

**26.** Disable the Windows Firewall on both servers.

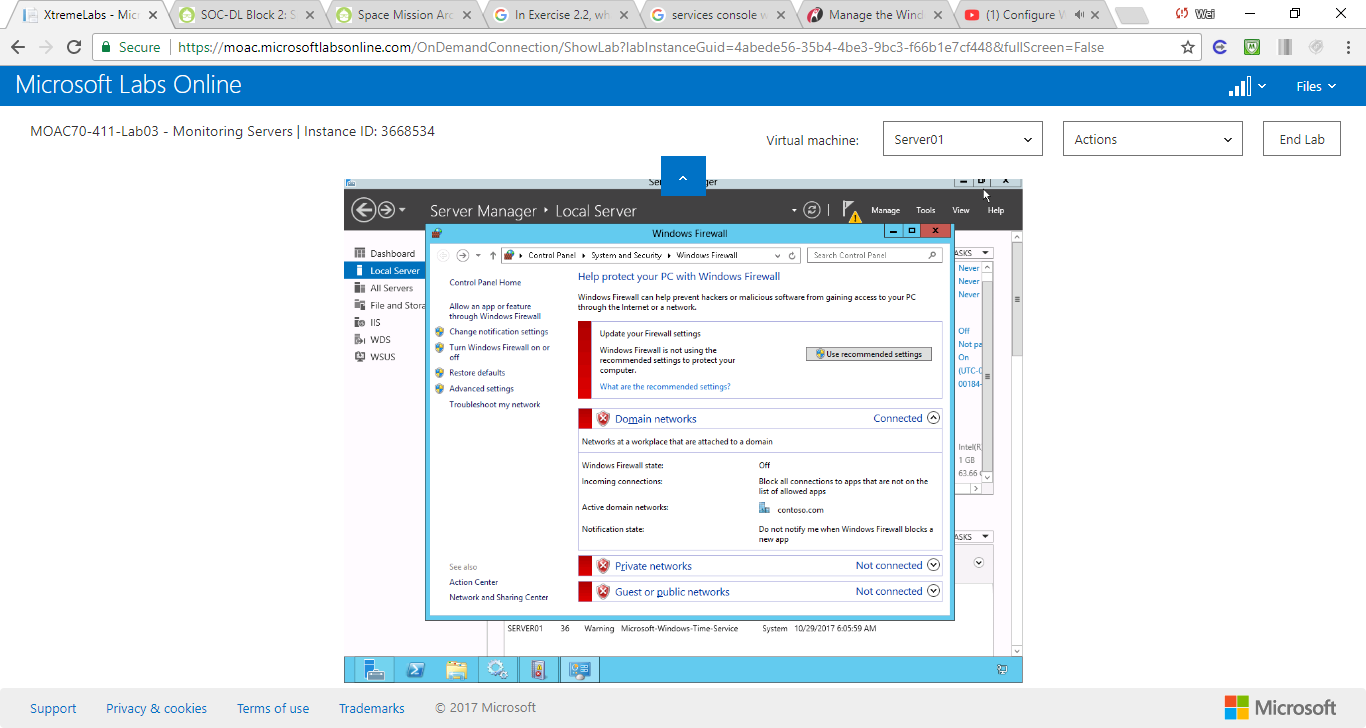


Figure . Disable the firewall

**27.** Restart the Print services on Server02.

**28.** After a few minutes, check to see if the events are displayed.

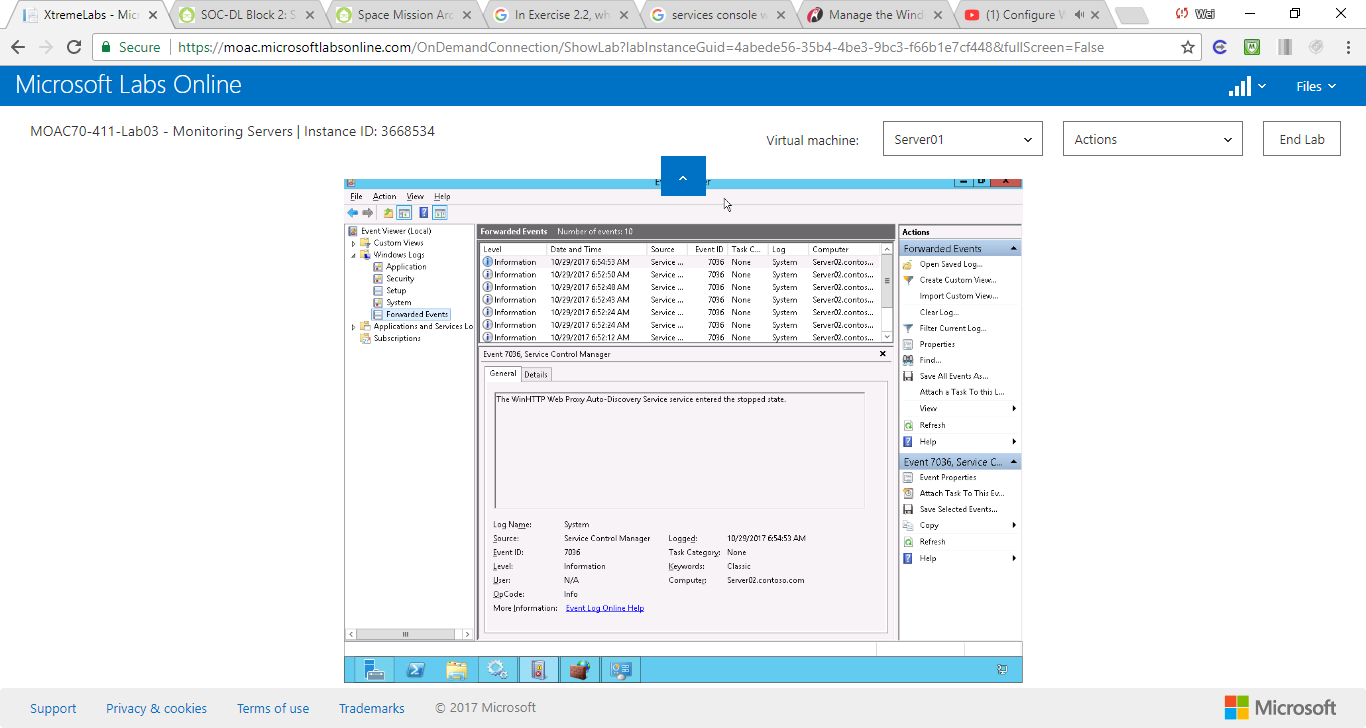


Figure . After the firewall is disabled, the events appear in forwarded events.

**29.** Close the Event Viewer and the Services console on Server02.

**30.** Close the Event Viewer on Server01.

**Lab Review Questions**

**1.** In Exercise 3.1, a busy server over a significant period of time will have hundreds, or even thousands, of events in the Event Viewer logs. What do you need to do when scanning through the event viewer looking for certain relevant events?

We can user a filter to narrow down the results to what we are interested.

**2.** In Exercise 3.1, what can you use to have one server catch errors from multiple servers that are displayed in the Event Viewer?

We can create a subscription to catch errors from different servers

**Lab Summary**

In this exercise, I used the Event Viewer to view the events stored in the Windows logs. Because there can be thousands of log entries, I have learned how to filter the logs so I can concentrate on what I need to focus on, and to set up subscriptions to consolidate the logs onto one server.