Lab LW08: Managing Windows Vista Using New Management Technologies

Abstract
This lab is intended for IT professionals who are responsible for managing Windows Vista client computers in large enterprises. In this lab you will learn to use the new Event Viewer and Task Scheduler to perform preventative maintenance and react to system events. You will schedule tasks that occur based on event triggers, and configure actions such as email messages. Finally you will explore WinRM for remote system managed using WMI. By the end of this lab you will be able to configure enterprise management of Windows Vista.

Objectives
In this lab you will complete the following:
- Explore new Event Log features in Windows Vista
- Use new Scheduled Tasks features to automate Windows Vista management
- Perform computer management using WinRM

Scenario
Contoso has several thousand Windows Vista workstations, and monitoring each one is becoming a huge part of the workload. To solve this issue, you will use the new desktop management features in Windows Vista to centralize more of the information that you use to monitor and administer client computers. You will first use Windows Event Viewer to create custom views of all of the errors that are being logged. You will then use the Task Scheduler to automate a common administrative task and also to send an email to the administrator in the event of a specific action being triggered. Finally you will use the WinRM command line tool to monitor the services running on your Windows Vista computers and send actions directly to them from your own workstation.

Prerequisites
- Familiarity with Event Viewer
- Familiarity with Task Scheduler
- Understanding of scripting and WMI.

Time to complete the labs
60 minutes
For more information on Vista Management Technologies

- [http://technet2.microsoft.com/WindowsServer/en/Library/9d08e3bf-ced4-4ac3-bc3c-753af4458e6c1033.mspx](http://technet2.microsoft.com/WindowsServer/en/Library/9d08e3bf-ced4-4ac3-bc3c-753af4458e6c1033.mspx)

Support Information

This lab is built and supported by HynesITe, Inc. See what’s possible at [www.hynesite.biz](http://www.hynesite.biz).
Exercise 1
Exploring the Event Logs in Windows Vista

In this lab we will explore the Event Logs and create custom views; allowing the administrator a single repository for all errors being logged on multiple Windows Vista computers. We will then look for failed Group Policy updates and send an email to the administrator when the Event Viewer records this specific event.

- Exploring the Event Logs in Windows Vista and Create Custom Views

You will be using Computer Management to explore the default views in the Event Viewer, create your own custom views to quickly scan for specific events every time you launch the Event Viewer, and analyze event details. The XML format of the event details are easier to automate and manage using tools like Microsoft Operations Manager than the old text-based events the previous versions offered.

**Important:** Perform the following exercise from Client1

1. Log on to Client1 as Contoso\administrator with a password of P@ssw0rd
2. Click Start, right-click Computer and then click Manage.

Notice that Views, Global Logs, Application Logs and Subscriptions are now available. Global logs contain the standard logs found in previous versions of Windows while the new Application Logs are a new more scalable framework for applications to store application specific non-operational events.

4. Expand Global Logs, and then select System. A list of events will now appear in the Upper-middle pane. Select any of these events to see information about it in the lower-middle pane.
5. Click the Details tab. Notice the new schematized (XML) representation of the event you selected.
6. In the Actions pane, click Filter. In the Filter dialog box, select Error and Critical, and then click OK. (screen resolution should be 1024x768 in order to view this dialog box).
7. In the Actions pane, click Save Filter as View.
8. In the Save Filter as View box, in the Name field type Errors Only and then click OK.
9. In the Explorer pane, expand the Views node. You should now see Errors only listed as a custom view
10. Expand Application Logs and notice the different log files available. You can click each of these individually to see the events related to the individual applications.
11. Right-click Views and then click Create View. In the Event Log drop down box, expand Glogal Logs, select System, then expand Application Logs, expand Microsoft, and then Windows. We will create a single view to span multiple logs.

12. Select DateTimeControlPanel and then scroll down to select Group Policy. Click anywhere within the box to compact the drop-down list and then select the Critical, and Error check boxes.

13. In the Event Source drop down, select Microsoft-Windows-DateTimeControlPanel and Microsoft-Windowns-GroupPolicy. Click anywhere within the box to compact the drop down list, then click OK.

14. In the Save Filter as View box, in the Name box type Group Policy and Time Errors. Click OK then View the results of this view in the upper-middle pane.

Create a Task based on an Event

The Contoso manager wants to react more quickly to the error events being logged in the Windows Vista client computers. In the following exercise you will use the Task Scheduler to create a task which will email the administrator in the event of a failed Group Policy update. To make sure Group Policy fails to update we will stop the NetLogon service ensuring that Client1 can not find the Domain Controller.

1. To stop the NetLogon service, on Client1 click Start\All Programs\Accessories and open a Command Prompt and type all on a single line net stop netlogon and then press ENTER.

2. Still in the Command Prompt, type gpupdate /force.

   *Note: This will attempt to update the Group Policy objects, but due to the NetLogon issue, this will fail.*


4. In the Upper-Middle pane, select event 1127. In the Actions pane, select Attach Task to This Event. The Task Scheduler will now launch. Notice the Log, Source and Event ID cannot be changed as these are automatically setup as triggers for the new task. Click Next.

   *Note: Event 1127 will be recorded every time Group Policy fails to update, regardless of the reason.*

5. With Action highlighted in Blue, select Start a Program and then click Next.
6. Notice you can browse for a specific program or script, adding arguments as necessary.  *Note: This is where you would attach a script that might do a NET TIME to re-sync the local clock with the DC.*  Click Back.

7. Select Send an Email and then click Next.  Fill in the information from the table below, then click Next and Finish:

| From:     | Client1                           |
| To:       | administrator@contoso.com         |
| Subject:  | Group Policy failed to update     |
| Text:     | Group Policy has failed to update. This could be because of a Time sync error. Networking error or Authentication error. Open the Event Viewer and look for event 1127 for more information. |
| Attachment: |                                   |
| Server:   | DC1                               |

8. A message box will open telling you the task was successfully created.  Click OK.

9. Restore the Command Prompt window and type `gpupdate /force`

   *Note: The netlogon service is still stopped so again, this will fail.*

10. Toggle back to Computer Management.  Ensure you have the recent event 1127 on the top line of the Errors Only view.  If not, Refresh the view.

11. Open Windows Mail by clicking E-Mail on the Start menu.  Read the new message in your Inbox from Client1.  Close the message and then close Windows Mail.

12. Toggle back to the Command Prompt window and type `net start netlogon` and then press ENTER.  Close the Command Prompt window.

Configure an Event Subscription

An Event Subscription gives a single administrator a place to go to forward events being logged from one or more Windows Vista computers.  Using this single repository the administrator can monitor more Windows Vista computers in less time.

*Note: You can complete the steps for this exercise in this BETA version, but the results will not be supported until the final release.  Go through the exercise to become familiar with Event Subscriptions.*

1. In the Event Viewer tree, select Subscriptions.

2. In the Actions pane, click Add.

3. Name the subscription Errors Client1 and Client2.  In the Description field type *This will forward all errors from Client1 and Client2 to a single log file.*
4. In the **Source Computers** section, click **New** and then type **Client1**. Click **OK**, and repeat this step entering **Client2** in the **computer name** field.

5. Under **Subscription Source** click **Filter**. This is the same filter box that see saw in the previous exercise. Click the drop down arrow next to **Event log**, and then check the box next to **Global Logs**.

6. Select the **Critical** and **Error** check boxes and select the **XML** tab.

   **Note:** Notice the X-Path XML query is automatically generated and displayed. This can be used in conjunction with the command line subscription utility `wecutil` to programmatically create subscriptions or this query can be edited manually for more complex queries that go beyond the Event Viewer tool.

7. Click **OK** two times.

8. In the **Credentials for Subscription Source** dialog box, type `P@ssw0rd`, and then click **OK**.

   **Note:** The **Yellow Warning** icon next to the subscription name is there because the query can not run in this release of Windows Vista. In future versions of Vista, forwarded events will appear in a **Global Log** called **ForwardedEvents**.
Exercise 2  
Creating Scheduled Tasks

The Task Scheduler in Windows Vista allows you to automate more of the tasks that have previously been done manually. Because of some of the applications that get used by the Contoso employees, the hard disks need to get defragmented weekly. In this exercise, you will use the Task Scheduler to create a task to run at a fixed time, create a task based on conditional triggers, and configure the AT service account.

Note: You'll notice that Windows Vista already ships with a defrag task in the box.

Create a task to run at a fixed time.

We will create a defrag.exe task which will defragment our hard disk weekly. The defragmentation will run each Friday night at 11:30 PM.

Important: Perform the following on Client1

1. In the Computer Management console, expand the Task Scheduler node and branches down to the Windows branch. Notice there are several tasks already listed that Windows Vista does automatically.

2. Select the Task Scheduler Library branch. In the Actions pane, click Run Task Scheduler Wizard.

3. Name the task Weekly Defrag and click Next.

4. Select Weekly and then click Next.

5. Select Friday and then change the time to 11:30:00PM and click Next.

6. Ensure Start a Program is selected in the Action window and then click Next. Browse to C:\windows\system32\defrag.exe. Click Next and then click Finish.

7. Expand Task Scheduler and click Task Scheduler Library. Notice the new task listed in the Upper-Middle pane. In the Lower-Middle pane you can see the details of the task.

8. Click the Triggers and Action tabs to see the details.

9. Right-click the task and click Properties.

10. Under User Options select Run whether user is logged on or not and then check Do not store password. Click OK.

11. In the Actions pane click Run. This will immediately run the task without waiting for the scheduled time. Note: You will not see the defrag application running.

12. In the Lower-Middle pane, click History. This will show you the events related to this task, and let you know whether or not it ran, or if there were any issues with running the task.
Create a Task to Respond to a System Event

The Contoso administrator monitors several secure workstations which get powered on, but not logged on. The administrator wants to be alerted if anyone does successfully log onto these machines. In this exercise you will create a task to run a program whenever the secure workstation gets logged on to. To prepare for this exercise you will first create a Visual Basic script which you will save to the root of the C:\.

To Create the Visual Basic script

1. On Client1 minimize Computer Management and click Start and then in the Start Search box type Notepad and then press Enter.

2. Type all on a single line, wscript.echo “You have just logged on to a secure workstation. An event just got logged in the Event Viewer alerting the administrator that this workstation has been logged on to.”

3. Save this file as C:\warning.vbs by clicking the File menu and then Save As. Fill in the Save As dialog box by using the information in the following table and then click Save:

File Name: "C:\Warning.vbs"

**Note:** Ignore the Apply Properties File error and hit Cancel.


2. Under User Options select Run only when a user is logged on.

3. Select the Triggers tab, and click New.

4. In the Begin the Task list, click On an Event.

5. Fill out the form using the information in the following table, and then click OK:

<table>
<thead>
<tr>
<th>Settings:</th>
<th>Simple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log:</td>
<td>Security</td>
</tr>
<tr>
<td>Source:</td>
<td>Microsoft-Windows-Security-Auditing</td>
</tr>
<tr>
<td>Event ID:</td>
<td>4624</td>
</tr>
</tbody>
</table>

**Note:** Event ID 4624 is generated when you log on to a computer.

6. Select the Actions tab and then click New.

7. In the Create New Action dialog box, next to Action select Start a Program and then click Browse.

8. In the Open dialog box, type C:\Warning.vbs and then press Enter.

9. In the Start in window, type C:\Users\administrator.CONTOSO\Desktop
10. Click **OK** two times, and then close Computer Management. Log off.

11. Log on to the Vista client as **administrator** and **P@ssw0rd** as the password.

12. Once your desktop appears, in the **Windows Script Host** dialog box click **OK**.


**Create Conditional Triggers**

Conditional Triggers are actions that get performed by Windows Vista in response to an Event. The Contoso administrator not only wants an event logged when someone logs onto the Secure Workstations, but would like to be notified via email as soon as it happens. In the following exercise you will create this Conditional Trigger and read the automatically generated email message.

1. Click **Task Scheduler**, and in the **Actions** pane, click **Create New Task**.

2. Name the task **Unlock Your Workstation** and select the **Triggers** tab.

3. Click **New**, and in the **Begin the task** drop down list, select **On workstation unlock**.

4. Click **OK** and then select the **Actions** tab.

5. Click **New** and in the **Action** drop down list, select **Send email**.

6. Fill out the **Settings** by using the table below, and then click **OK**.

<table>
<thead>
<tr>
<th>From:</th>
<th>Client1</th>
</tr>
</thead>
<tbody>
<tr>
<td>To:</td>
<td><a href="mailto:administrator@contoso.com">administrator@contoso.com</a></td>
</tr>
<tr>
<td>Subject:</td>
<td>Secure Workstation unlocked</td>
</tr>
<tr>
<td>Text:</td>
<td>Client1’s desktop has been successfully unlocked. This may result in a security issue.</td>
</tr>
<tr>
<td>Attachment:</td>
<td>Server: DC1</td>
</tr>
</tbody>
</table>

7. Click **New** and in the **Action** drop down list, select **Show Message**.

8. In the **Title** window, type **Unlocked Workstation**. Then in the **Message window** type “You have unlocked a secure workstation. An email was just sent to the Contoso administrator alerting him that this secure workstation was logged onto.” Click **OK**.

9. Click **OK**, and then minimize Computer Management. Press Right-Alt+Del and **lock this computer**.

10. Log back on as **administrator** with password **P@ssw0rd**. Close the message window and then open **E-mail** from the **Start** menu. Read the new email and then close **Inbox-Windows Mail**.

**Configure the AT Service Account**
The AT Service account is used by Windows Vista when you schedule a task by using the command line, instead of the Task Scheduler user interface. In this section we will create an account to be used, instead of the default `localsystem` account.

1. In the **Computer Management** console, select and then right-click **Task Scheduler**. Click **AT Service Account Configuration**. Notice this defaults to System Account.

2. Click **This account** and ensure `contoso\administrator` is listed. Enter `P@ssw0rd` as the password and click **OK**.

3. Go to a command prompt and type:
   
   `AT \client1 hh:mm /every:m,t,w,th,f calc.exe`
   
   Where `hh:mm` is three minutes after your current Vista time using the 24 hr clock.

4. Read the message, and then minimize the command prompt. In the **Computer Management** console, right-click **Task Scheduler Library** and then click **Refresh**.

5. The task will be listed as **Idle**. Wait for it to show as **Running** and then open your **Task Manager** from the task bar. *Note: you may have to refresh this screen again at the appropriate time.*

6. Click the **Processes** tab and ensure **Show Processes from all users is selected**. Notice `calc.exe` is running in the background. It is running as the **Administrator** account, which is what you previously configured as the **AT Service Account**.

7. Close the **Task Manager** and click the **At1** scheduled task. In the Lower-Middle pane, select the **General** tab and notice which user account is being used to run the task.

8. Click and then right-click **Task Scheduler** in the Explorer pane, and then click **AT Service Account Configuration**. Change this back to **System Account** and click **OK**.

9. Click the **Task Scheduler Library** and then click the **At1** task. Notice in the Lower-Middle pane, the user account used to run this task has changed. *Note: You may have to refresh this view to notice the change.*

10. Right-Click the **At1** task and click **End**. Click **Yes** to confirm. End any other running tasks.

11. Close **Computer Management**. Close the **Command Prompt** window.
Exercise 3
Performing computer management using WinRM

The WinRM command line utility was introduced with Server 2003 R2 and has been integrated with Windows Vista. The Contoso administrator would like to make sure that only the required services are running on Client2. The administrator’s workstation is Client1, so he will use WinRM to remotely manage Client2 from his own workstation.

Configure the WinRM service

This service has to be configured on all of the clients that you will be administering. To configure the service, you will need to Start the service, configure a Listener on the remote client, and Enumerate the Listener. Additionally, the Windows Firewall will need to be configured to allow Remote Administration.

1. **To start the service:** On Client2, click Start\All Programs\Accessories. Right-click Command Prompt and click Run as administrator. *Note: This will open the command prompt window with elevated privileges.*

2. In the Command Prompt window, type `regsvr32 winhttp.dll` and then press Enter.
   
   *Note: For WinRM commands to work on a remote computer, IIS does not need to be running on the remote system, but the winhttp.dll needs to be registered.*

3. In the RegSvr32 dialog box Click OK.

4. In the Command Prompt window, type Net Start WinRM. This will start the WinRM service.

5. **To configure a Listener:** In the Command Prompt window type all on one line:
   ```
   winrm create winrm/config/Listener?Address=*+Transport=HTTP @{}
   ```
   and then press Enter.

   *Note: There is a space after HTTP. Also, please note that the Listener only needs to be configured on the remote client to listen for remote winRM commands.*

6. Read the output. If the command was typed correctly, you should see approximately 5 lines of data output, including Selector = *, HTTP

7. To confirm that the listener has been added: In the command prompt window type all on one line:
   ```
   winrm enumerate winrm/config/listener
   ```
   and then press Enter.

8. **To configure the Firewall on Client2 for Remote Administration:** In the Command Prompt window, type all on a single line: netsh firewall add portopening protocol=TCP port=80 name=”WinRM requests” mode=enable scope=subnet profile=Domain and then press Enter.

   *Note: In future versions of Vista, there will be a QuickConfig option that will handle most of these settings.*
9. Toggle back to Client1. Open a Command Prompt window with elevated privileges. Note: Follow step 1 from above.

10. To test the Listener on Client2: From Client1’s Command Prompt, window type all on one line: `winrm get wsman:\system\2005\06\this –machine:client2` and then press Enter.

11. Read the output. If the command completed successfully, you should see two lines of data describing this Operating System as OS: 6.0.5308.

   Note: We will do more GET operations in the next exercise. This was just to test the Listener.

To Perform a GET Operation

The WS-Management GET operation returns the value of a specific WMI object. In the following example, WS-Management retrieves the properties of the WinRM service running on Client2.

Important: Perform the following exercise from Client1

1. In the Command Prompt window, type all on a single line:

   `winrm get
   ?name=WinRM –machine:client2` and then press Enter.

2. Read the resulting output. If you typed this correctly, you should see a whole list of descriptions including the DisplayName, PathName, the StartMode and State of the WinRM service.

   Note: URI (Uniform Resource Identifier) aliases can be used to simplify this command line. For example, if the command includes `http://schemas.microsoft.com/wsman/2005/06/wmi`, then you can simply type `wmi`. The above command would become `winrm get wmi/root/…`

3. In the Command Prompt window, type all on a single line:


4. Read the resulting XML output. Again, notice some of the listed descriptions of the Print Spooler service.

   Note: Step 3 was done to show the functioning URI alias.

To Perform an Enumerate Operation

The WS-Management Enumerate operation returns a collection of objects. The resulting output will be similar to that of a GET operation, but instead of listing the information of a single object, it will list all of the objects.

1. From the Command Prompt type all on one line: `winrm enumerate cimv2/win32_LogicalDisk –machine:client2` and then press Enter.

2. Read the output. This will give information on all of the storage drives including the Partitioned Volumes, the Floppy drive and the CD drive.
To Perform an Invoke Operation

The WS-Management Invoke operation executes methods on the target object. In the following example, we will stop and start the Windows Time service on Client2.

Important: Perform the following exercise from Client1

1. From the Command Prompt window, type all on a single line: `winrm invoke StopService cimv2/win32_service?name=W32Time – machine:client2` and then press Enter.

2. The output should show `StopService_OUTPUT ReturnValue=0`

Note: To verify that this did stop the Time service, perform the GET operation from Step 3 on page 13; substituting W32Time for Spooler.


4. The Output should now show `StartService_OUTPUT ReturnValue=0`.

5. Again to verify this service has started, redo the GET operation above.

To Perform a PUT operation

The WS-Management PUT operation allows a value of keys to be set. In the following example the value of the MaxEnvelopeSizekb key will be re-configured.

1. From the Command Prompt window, type all on a single line: `winrm get wsman:Microsoft.com/wsman/2005/12/config – machine:client2` and then press Enter.

2. Notice in the resulting data, the MaxEnvelopeSizekb value of 150. We will now change this to be 100.

3. Type all on a single line:
   `winrm put wsman:microsoft.com/wsman/2005/12/config @{MaxEnvelopeSizekb="100"} –machine:client2` and then press ENTER.

   Note: There is a space after config.

4. Notice the resulting output, and the new MaxEnvelopeSizekb value.

To Delete the Listener

We will list all Listeners on Client2, and then delete them, as we are done with our exercise.

Important: Perform the following exercise from Client2

1. From the Command Prompt, type all on a single line: `winrm enumerate wsman:Microsoft.com/wsman/2005/12/config/Listener` and then press Enter.
2. There should be only one Listener displayed. It is using the **HTTP** protocol on port **80**, and has been **enabled**.

3. From the **Command Prompt** type all on a single line: `winrm delete wsman:Microsoft.com/wsman/2005/12/config/Listener?address=*+Transport=HTTP @{} and then press Enter.**

   **Note:** There is a space after **HTTP**.

4. Close the **Command Prompt** window and log off of the Vista client computers.