

Microsoft® Virtual Labs



**Managing Windows Server
2008 Using New Management
Technologies**

Microsoft®

Table of Contents

| | |
|------------------------------------------------------------------------------------|----------|
| Managing Windows Server 2008 Using New Management Technologies..... | 1 |
| Exercise 1 Using Task Scheduler and Event Viewer to Respond to System Events | 2 |
| Exercise 2 Creating Custom Scheduled Tasks..... | 6 |
| Exercise 3 Managing Computers Using Windows Remote Management (WinRM) | 9 |

Managing Windows Server 2008 Using New Management Technologies


| | |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Objectives | <p>After completing this lab, you will be better able to:</p> <ul style="list-style-type: none"> ▪ Manage event logs, subscriptions, and views ▪ Configure event subscriptions ▪ Analyze system performance and reliability using reliability and performance reporting |
| Scenario | <p>In this lab you will use a Windows 2008 Member Server to manage a Windows 2008 Server Domain Controller using new Windows management technologies. From your Windows 2008 Member Server, you will use event log views and event log subscriptions to identify problems occurring on your server. You will then create custom tasks to alert you when specific problems occur on the server. Finally you will review server performance and reliability data using custom reports.</p> <p><i>Note: During the course of this lab you may encounter one or more User Account Control prompts. These prompts will ask you to confirm an action you have just taken. When you encounter a User Account Control prompt, select the option which confirms the action you have taken and you will be able to proceed with the next step in the exercise. A shield icon appears after each instruction which invokes a User Account Control dialog box.</i></p> <p><i>Note: The steps in this lab are intended to provide an overview of the technology presented. They are not intended to, and may not follow, Microsoft best practices or guidance on the technology presented.</i></p> <p><i>Note: This lab uses pre-release software. While every effort has been taken to ensure the functionality of the steps documented, some steps may still not function as intended at all times.</i></p> |
| Prerequisites | <p>Before working on this lab, you must have:</p> <ul style="list-style-type: none"> • An understanding of performance monitoring • An understanding of event logs • An understanding of scheduled tasks • An understanding of WMI |
| Estimated Time to Complete This Lab | <p>60 Minutes</p> |
| Computer used in this Lab | <p> NYC-DC-1  NYC-SRV-1</p> <p>The password for the Woodgrovebank \Administrator account on this computer is: pass@word1.</p> |


Exercise 1



Using Task Scheduler and Event Viewer to Respond to System Events

Scenario

In this exercise you will use the new Event Viewer in Windows 2008 Server to monitor and more effectively respond to system events. You will first create a custom event view to filter system events to only relevant events. You will then use a WinRM based event subscription to monitor events on a remote system. WinRM based event subscriptions forward select events from a remote computer to a destination computer. Once you have created the event subscription, you will create a custom task to provide an interactive notification to an operator. The WinRM provider is included with Windows 2008 Server. It is configured to start automatically. You only need to configure the service.

| Tasks | Detailed Steps | | | | | | | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|---------------|--------------|-------|------------|---------------------|
| <p>Complete the following 2 tasks on:</p> <p> NYC-DC-1</p> <p>1. Create a Custom Event View</p> | <p><i>Note: In this task you will create a custom event view which will filter the events to only events that are relevant to you. Event views are a powerful way to parse multiple types of events in multiple event logs. By focusing the event view on only important or actionable events, you increase your chance of identifying a performance or reliability problem before it causes system downtime. Event views are also useful in branch office environments, allowing you to create a view of all critical events that span all servers.</i></p> <p><i>Note: Perform this procedure on the NYC-DC-1 computer as Woodgrovebank\Administrator</i></p> <ol style="list-style-type: none"> On the Start menu, in Start Search, type compmgmt.msc and then press ENTER. Under Computer Management (Local), expand Event Viewer and then click on Custom Views. On the Action menu, click Create Custom View. In the Create Custom View dialog box, create a new view with the following settings and then click OK. <table border="1" data-bbox="587 1383 1352 1556"> <thead> <tr> <th>Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Logged:</td> <td>Last 24 hours</td> </tr> <tr> <td>Event level:</td> <td>Error</td> </tr> <tr> <td>Event log:</td> <td>Windows Logs/System</td> </tr> </tbody> </table> <ol style="list-style-type: none"> In the Save Filter to Custom View dialog box, in Name type Error Events (24 hours) and then click OK Review the contents of the Error Events (24 hours) view. | Setting | Value | Logged: | Last 24 hours | Event level: | Error | Event log: | Windows Logs/System |
| Setting | Value | | | | | | | | |
| Logged: | Last 24 hours | | | | | | | | |
| Event level: | Error | | | | | | | | |
| Event log: | Windows Logs/System | | | | | | | | |
| <p>2. Add a Custom Event to the System Log and View it in the Event View</p> | <p><i>Note: In this task you will use the EventQuery command to record a custom event in the Event log. This event will meet the criteria of the event view you created in the previous task. You will use your event view to review the custom event in the event log. When performing configuration tasks via script, such as those used to configure Windows 2008 Server Core, you can use this command to record success or failure of script actions.</i></p> <p><i>Note: Perform this task on the NYC-DC-1 computer as</i></p> | | | | | | | | |

| Tasks | Detailed Steps | | | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|--|--|
| | <p>Woodgrovebank\Administrator.</p> <ol style="list-style-type: none"> On the Start menu, right-click Command Prompt and then click Run as administrator. In the command prompt, type the following command and then press ENTER. <pre>Eventcreate /T ERROR /ID 100 /L SYSTEM /D "Application Error #1" /SO MyApp</pre> In Computer Management, click Error Events (24 Hours) and then in the Actions pane, click Refresh. Review the new entry on the top of the list of events. | | | | |
| <p>Complete the following task on:</p> <p> NYC-SRV-1</p> <ol style="list-style-type: none"> Create an Event Subscription on a Windows 2008 Member Server | <p><i>Note: In this task you will create an event subscription on a Windows 2008 Member Server computer which reports events that occur on a Windows 2008 Server Domain Controller. Event subscriptions are a new way to monitor multiple computer event logs from a single machine. An event subscription uses Windows Remote Management to query the event logs WMI provider on the remote computer using HTTP or HTTPS. The use of HTTP and HTTPS allows you to perform management tasks in environments that do not allow protocols such as RPC. This is useful if you want to remotely manage branch office servers without the need for RPC or VPN connections. The proven security of SSL and the integrated authentication in WinRM ensures this is done without introducing additional risk. The event subscription creates a copy of the remote event and stores it in a log of your choosing. The default location is a log called Forwarded Events. This log can contain all events from all remote computers to which you have event subscriptions. Each event subscription can be configured to use custom credentials, and can be configured to subscribe to only the events of your choosing.</i></p> <p><i>Note: Perform this task on the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> On the Start menu, in Start Search, type compmgmt.msc and then press ENTER. Under Computer Management (Local), expand Event Viewer and then click on Subscriptions. In the Event Viewer dialog box, click Yes. On the Action menu, click Create Subscription. In the Subscription Properties dialog box, in Subscription Name type MyApp Errors on NYC-DC-1 In Source Computers, click Add. In the Select Computer dialog box, type NYC-DC-1.woodgrovebank.com and then click OK. In Subscription Properties, select NYC-DC-1.woodgrovebank.com and then click Test. In the Event Viewer dialog box, click OK. <p><i>Note: The subscription fails because WimRM is not yet configured on NYC-DC-1. This will be completed in a future task.</i></p> <ol style="list-style-type: none"> In the Subscription Properties dialog box, click Select Events. In the Query Filter dialog box, configure the filter with the following settings and then click OK. <table border="1" data-bbox="586 1839 1349 1877"> <thead> <tr> <th data-bbox="586 1839 911 1877">Setting</th> <th data-bbox="911 1839 1349 1877">Value</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table> | Setting | Value | | |
| Setting | Value | | | | |
| | | | | | |

| Tasks | Detailed Steps | | | | | | | | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------------|--------------|-------|------------|---------------------|-------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <table border="1"> <tr> <td data-bbox="586 197 911 233">Logged:</td> <td data-bbox="911 197 1349 233">Last 24 hours</td> </tr> <tr> <td data-bbox="586 233 911 268">Event level:</td> <td data-bbox="911 233 1349 268">Error</td> </tr> <tr> <td data-bbox="586 268 911 304">Event log:</td> <td data-bbox="911 268 1349 304">Windows Logs/System</td> </tr> <tr> <td data-bbox="586 304 911 361">Event ID's:</td> <td data-bbox="911 304 1349 361">100</td> </tr> </table> | Logged: | Last 24 hours | Event level: | Error | Event log: | Windows Logs/System | Event ID's: | 100 | <ol style="list-style-type: none"> l. In the Subscription Properties dialog box, click Advanced. m. In Advanced Subscription Settings, select Specific User and then click User and Password. n. In Credentials for Subscription Source, in Username type WOODGROVEBANK\Administrator, in Password type pass@word1, and then click OK. o. In the Advanced Subscription Settings dialog box, in Event Delivery Optimization, click Minimize Latency and then click OK. p. Click OK to close the Subscription Properties dialog box. q. In the Event Viewer dialog box, click Yes. Leave Computer Management open, you will use it again later in this exercise. |
| Logged: | Last 24 hours | | | | | | | | | |
| Event level: | Error | | | | | | | | | |
| Event log: | Windows Logs/System | | | | | | | | | |
| Event ID's: | 100 | | | | | | | | | |
| <p>Complete the following task on:</p> <p> NYC-DC-1</p> <p>4. Enable WinRM for Event Subscriptions</p> | <p><i>Note: In this task you will configure WinRM to listen on the external interface of the NYC-DC-1 computer. WinRM is enabled by default, but not configured to listen on any external interface on HTTP or HTTPS in Windows 2008 Server. For maximum security Windows 2008 server should be configured to use HTTPS at all times.</i></p> <p><i>Note: Perform this task on the NYC-DC-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> a. On the Start menu, right click Command Prompt and then click Run as Administrator. b. In the command prompt, type the following command and then press ENTER. <pre style="background-color: #f0f0f0; padding: 5px;">WINRM QuickConfig</pre> <ol style="list-style-type: none"> c. In the command prompt, type Y and then press ENTER. | | | | | | | | | |
| <p>Complete the following 2 tasks on:</p> <p> NYC-SRV-1</p> <p>5. Verify Event Subscriptions are Functioning Correctly</p> | <p><i>Note: In this task you will log a custom event on the NYC-DC-1 computer and review the event using your event subscription on the NYC-SRV-1 computer. The event subscription may take a few seconds to process the event.</i></p> <p><i>Note: Perform this task on the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> a. In Computer Management, navigate to System Tools/Event Viewer and then select Subscriptions. b. In the contents pane, click MyApp Errors on NYC-DC-1 and then in the Actions pane, click Retry. c. Verify that MyApp Errors on NYC-DC-1 shows a status of Active. d. On the Start menu, navigate to All Programs/Accessories, right-click Command Prompt and then click Run as administrator. e. In the command prompt window, type the following command and then press ENTER. <pre style="background-color: #f0f0f0; padding: 5px;">EVENTCREATE /S NYC-DC-1.woodgrovebank.com /L System /T Error /ID 100 /SO MyApp /D "MyApp Encountered an error"</pre> <ol style="list-style-type: none"> f. In Computer Management, navigate to System Tools/Event Viewer/Windows Logs and then click Forwarded Events. | | | | | | | | | |


| Tasks | Detailed Steps | | | | | | | | | | |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|------|------------------------------------------|--------|-------------------|--------------------------|-------------|----------------------------|-----------------------------------------|
| <p>6. Create an Alert Task Based On a Forwarded Event</p> | <p>g. In the contents pane, verify that an Error entry exists for MyApp.</p> <p><i>Note: In this task you will create a task based on an event. The new Task Scheduler in Windows 2008 Server has been extended to include the ability to launch tasks when system events occur. This is a very effective way to automatically respond to system events. Three types of actions are supported for events which allow you to run an application or script, display an alert, or sent an email message. This task will create an alert to notify the currently logged on user that an error has occurred.</i></p> <p><i>Note: Perform this task on the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <p>a. In Computer Management, navigate to System Tools/Event Viewer/Windows Logs and then click Forwarded Events.</p> <p>b. In the Contents pane, click MyApp Error, and then in the Actions pane click Attach Task To This Event.</p> <p>c. Complete the Create Basic Task Wizard using the following information.</p> <table border="1" data-bbox="586 722 1383 995"> <thead> <tr> <th>Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>MyApp Error 100 Interactive Notification</td> </tr> <tr> <td>Action</td> <td>Display a message</td> </tr> <tr> <td>Display a Message: Title</td> <td>MyApp Error</td> </tr> <tr> <td>Display a Message: Message</td> <td>Error 100 occurred in MyApp on NYC-DC-1</td> </tr> </tbody> </table> <p>d. In the Event Viewer dialog box, click OK.</p> <p>e. On the Start menu, navigate to All Programs/Accessories, right-click Command Prompt and then click Run as administrator.</p> <p>f. In the command prompt window, type the following command and then press ENTER.</p> <pre>EVENTCREATE /S NYC-DC-1.woodgrovebank.com /L System /T Error /ID 100 /SO MyApp /D "MyApp Encountered an error"E</pre> <p><i>Note: It may take up to 20 seconds for the error message dialog box to be displayed.</i></p> <p>g. In the MyApp Error dialog box, click OK.</p> | Setting | Value | Name | MyApp Error 100 Interactive Notification | Action | Display a message | Display a Message: Title | MyApp Error | Display a Message: Message | Error 100 occurred in MyApp on NYC-DC-1 |
| Setting | Value | | | | | | | | | | |
| Name | MyApp Error 100 Interactive Notification | | | | | | | | | | |
| Action | Display a message | | | | | | | | | | |
| Display a Message: Title | MyApp Error | | | | | | | | | | |
| Display a Message: Message | Error 100 occurred in MyApp on NYC-DC-1 | | | | | | | | | | |

Exercise 2

Creating Custom Scheduled Tasks

Scenario

The Task Scheduler in Windows 2008 Server allows you to automate more of the tasks that have previously been done manually. Windows Task Scheduler uses an event based model which allows you to define a series of conditions which trigger a scheduled task. The addition of event based triggers provides a powerful way to automate system management.

| Tasks | Detailed Steps | | | | | | | | | | | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|------|---------------|---------|--------|------------|-------------------|--------|-----------------|----------------|--------------------------------|
| <p>Complete the following 3 tasks on:</p> <p> NYC-SRV-1</p> <p>1. Create a task to run at a fixed time.</p> | <p><i>Note: 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.</i></p> <p><i>Note: Complete this task on the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> Click Start, Run and type MMC. From the MMC click File > Add/Remove Snap-in... Select Computer Management and Click Add. Select Local Computer, Click Finish and then OK. In Computer Management console, navigate to Task Scheduler\Task Scheduler Library. On the Action menu, click New Folder. Create a new folder named Custom Tasks. Click the Custom Tasks folder. In the Actions pane, click Create Basic Task. Complete the Create Basic Task Wizard wizard using the following information. <table border="1" data-bbox="586 1220 1352 1478"> <thead> <tr> <th>Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Weekly Defrag</td> </tr> <tr> <td>Trigger</td> <td>Weekly</td> </tr> <tr> <td>Recurrence</td> <td>11:30PM on Friday</td> </tr> <tr> <td>Action</td> <td>Start a program</td> </tr> <tr> <td>Program/Script</td> <td>C:\windows\system32\defrag.exe</td> </tr> </tbody> </table> <p><i>Note: Notice the new task listed in the Upper-Middle pane. In the Lower-Middle pane you can see the details of the task.</i></p> <ol style="list-style-type: none"> Click the Triggers and Actions tabs to see the details. In the Actions pane, click Properties. Under Security Options select Run whether user is logged on or not. Check Do not store password. Check Run with highest privileges and then click OK. In the Actions pane click Run. This will immediately run the task without waiting for the scheduled time. <p><i>Note: You will not see the defrag application running.</i></p> <ol style="list-style-type: none"> In the Lower-Middle pane, click History. This will show you the events related to | Setting | Value | Name | Weekly Defrag | Trigger | Weekly | Recurrence | 11:30PM on Friday | Action | Start a program | Program/Script | C:\windows\system32\defrag.exe |
| Setting | Value | | | | | | | | | | | | |
| Name | Weekly Defrag | | | | | | | | | | | | |
| Trigger | Weekly | | | | | | | | | | | | |
| Recurrence | 11:30PM on Friday | | | | | | | | | | | | |
| Action | Start a program | | | | | | | | | | | | |
| Program/Script | C:\windows\system32\defrag.exe | | | | | | | | | | | | |

| Tasks | Detailed Steps |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>this task, and let you know whether or not it ran, or if there were any errors with running the task.</p> <p><i>Note: You may have to refresh Task Scheduler Library to notice that the task has run.</i></p> |
| <p>2. Create a Task to Respond to a System Event</p> | <p><i>Note: The Woodgrovebank administrator monitors several secure servers which get powered on, but not logged on. The administrator wants to be alerted if anyone does successfully log onto these Servers. In this exercise you will create a task to display a message whenever the secure workstation gets logged on to.</i></p> <p><i>Note: Complete this task from the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> a. Click the Custom Tasks folder. b. In the Actions pane, click Create Task. c. In the Create Task dialog box, in Name type Log on to Secure Workstation. d. On the Triggers tab, click New. e. In the Begin the Task list, select At log on and then click OK. f. On the Actions tab, click New. g. In the New Action dialog box, in Action, select Display message, in Title, type Log on Warning, and then in Message, type You have just logged on to a secure workstation, ensure you log off when you are finished. h. Click OK to close the New Action dialog box. i. Click OK to close the Create Task dialog box. j. Close all programs and log off k. Log on to NYC-SRV-1 as WOODGROVEBANK\Administrator l. Once your desktop appears, in the Log on Warning dialog box click OK. |
| <p>3. Configure the AT Service Account</p> | <p><i>Note: The AT Service account is used by Windows 2008 Server when you schedule a task by using the command line, instead of the Task Scheduler user interface. In this task we will create an account to be used, instead of the default localsystem account.</i></p> <p><i>Note: Complete this task from the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <ol style="list-style-type: none"> a. On the Start menu, in Start Search, type compmgmt.msc and then press ENTER. b. In Computer Management, click Task Scheduler. c. In the Actions pane, click AT Service Account Configuration. d. In the AT Service Account Configuration dialog box, click Another User account, then click Change user. At the sign in box type WOODGROVEBANK\Administrator. Enter pass@word1 as the password and click OK. Then click OK again. e. On the Start menu, navigate to All Programs/Accessories, right-click Command Prompt and then click Run as administrator. f. In the command prompt, type the following command where hh:mm is three minutes after your current 2008 time using the 24 hr clock and then press ENTER. <div style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <pre>AT \\localhost hh:mm /every:m,t,w,th,f calc.exe</pre> </div> <ol style="list-style-type: none"> g. Read the message, and then minimize the command prompt. h. In the Computer Management console, expand Task Scheduler, click Task Scheduler Library and then in the Actions pane, click Refresh. i. The task AT1 will be listed as Ready. Wait for it to show as Running and then |



| Tasks | Detailed Steps |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>open your Task Manager by right-clicking the task bar and clicking Task Manager</p> <p><i>Note: You may have to refresh this screen again at the appropriate time.</i></p> <p>j. 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.</p> <p>k. Close the Task Manager and click the At1 scheduled task. In the Lower-Middle pane, select the History tab. Double click the top event listed and notice which user account is being used to run the task. Close the dialog box.</p> <p>l. 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.</p> <p>m. In Computer Management, in the contents page, click AT1 and then on the Actions menu, click End.</p> <p>n. In the Task Scheduler dialog box, click Yes.</p> <p>o. Close Computer Management. Close the Command Prompt window.</p> |

Exercise 3

Managing Computers Using Windows Remote Management (WinRM)

Scenario

Windows Remote Managed (WinRM) allows a Windows 2008 Server computer to be managed using WMI over HTTP or HTTPS. A WinRM listener is created on the computer to be managed. The WinRM listener accepts WMI based commands from a computer and returns the results of the commands. Commands can include queries or actions. WinRM is secured using a combination of WMI ACLs, HTTPS, and Kerberos, Windows Integrated, or Basic authentication. All communication is done using the SOAP protocol.

| Tasks | Detailed Steps |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Complete the following task on:</p> <p> NYC-SRV-1</p> <p>1. Configure the WinRM service</p> | <p><i>Note: WinRM is initially not configured to listen for remote management commands on any network interface. To configure WinRM to listen to remote management commands, you must configure a listener on at least one interface. In this task you will use the WinRM command line tool to create a default HTTP listener, which listens on all interfaces. This listener can be further secured by enabling HTTPS and limiting authentication methods to only the most secure methods. HTTPS is configured using the WinRM command, assuming a suitable computer authentication certificate is present on the server computer. Limiting authentication methods is done using Group Policy or the WinRM command.</i></p> <p><i>Note: Perform this task on the NYC-SRV-1 computer as Woodgrovebank\Administrator.</i></p> <p>a. On the Start menu, navigate to All Programs/Accessories, right-click Command Prompt and then click Run as administrator.</p> <p>b. In the command prompt, type the following command and then press ENTER.</p> <pre>WINRM QuickConfig</pre> <p>c. WinRM could already be configured on this server if so just go on to next step otherwise: In the command prompt, type Y and then press ENTER.</p> |
| <p>Complete the following 5 tasks on:</p> <p> NYC-DC-1</p> <p>2. Perform a GET Operation</p> | <p><i>Note: 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 NYC-SRV-1.</i></p> <p><i>Note: Perform this task on NYC-DC-1 as Woodgrovebank\Administrator.</i></p> <p>a. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm get wmicimv2/win32_service?name=WinRM -remote:NYC-SRV-1</pre> <p>b. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm get wmicimv2/win32_service?name=WinRM -remote:NYC-SRV-1 -format:pretty</pre> |
| <p>3. To Perform an Enumerate Operation</p> | <p><i>Note: 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.</i></p> <p><i>Note: Perform this task on NYC-DC-1 as Woodgrovebank\Administrator.</i></p> |

| Tasks | Detailed Steps |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>a. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm enumerate wmicimv2/win32_logicaldisk -remote:NYC-SRV-1</pre> |
| <p>4. To Perform an Invoke Operation</p> | <p><i>Note: 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 NYC-SRV-1.</i></p> <p><i>Note: Perform this task on NYC-DC-1 as Woodgrovebank\Administrator.</i></p> <p>a. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm invoke StopService wmicimv2/win32_service?name=W32Time -remote:NYC-SRV-1</pre> <p>b. The output should show StopService_OUTPUT ReturnValue=0</p> <p>c. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm invoke StartService wmicimv2/win32_service?name=W32Time -remote:NYC-SRV-1</pre> <p>d. The Output should now show StartService_OUTPUT ReturnValue=0.</p> <p>e. Again to verify this service has started, redo the GET operation above.</p> |
| <p>5. To Perform a PUT operation</p> | <p><i>Note: 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.</i></p> <p><i>Note: Perform this task on NYC-DC-1 as Woodgrovebank\Administrator.</i></p> <p>a. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm get winrm/config -remote:NYC-SRV-1</pre> <p>b. Notice in the resulting XML data, the MaxEnvelopeSizekb value of 150. We will now change this to be 100.</p> <p>c. In the command prompt, type the following command and then press ENTER.</p> <pre>winrm put winrm/config @{MaxEnvelopeSizekb="100"} -remote:NYC-SRV-1</pre> <p>d. Notice the resulting XML, and the new MaxEnvelopeSizekb value.</p> |
| <p>6. To Perform a Remote Shell operation</p> | <p><i>Note: The WS-Management Remote Shell operation allows certain non-interactive commands to be executed in the CMD shell on the remote machine. This is a very useful for performing remote operations.</i></p> <p><i>Note: Perform this task on NYC-DC-1 as Woodgrovebank\Administrator.</i></p> <p>a. In the command prompt, type the following command and then press ENTER.</p> <pre>winrs -remote:NYC-SRV-1 ipconfig /all</pre> <p><i>Note: Notice in the resulting data looks the same as if this command was executed on the local machine. The Hostname result shows the name of the remote machine.</i></p> |