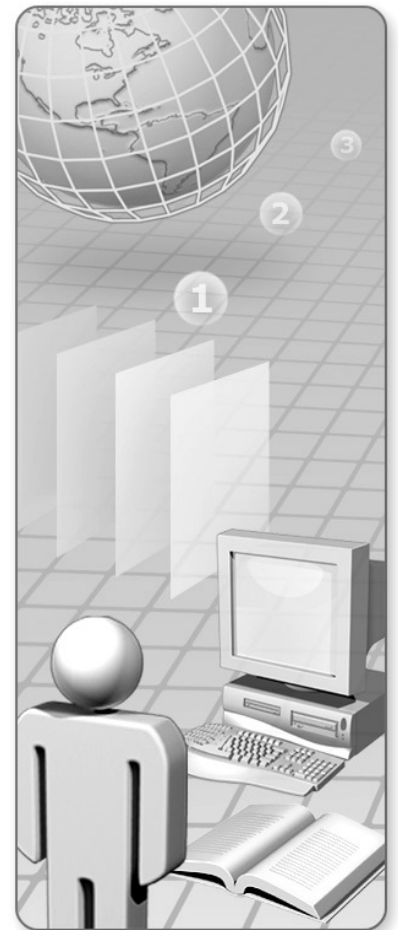


SVRHOL06: Windows Server® 2008 – Windows Server 2008 Management

Table of Contents

| | |
|--|----|
| Introduction | 1 |
| Exercise 1: Using Server Manager | 4 |
| Exercise 2: Managing a Server Using Windows PowerShell | 9 |
| Exercise 3: Managing a Remote Computer with WinRM | 14 |
| Appendix | 18 |



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links are provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2007 Microsoft Corporation. All rights reserved.

Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Introduction

Estimated time to complete this lab

90 minutes

Objectives

After completing this lab, you will be able to:

- Use Server Manager to manage roles and features.
- Use WinRM to perform remote server management.
- Query server information using Windows PowerShell.

Prerequisites

Before working on this lab, you must have:

- An understanding of roles and features
- The ability to work in a command line environment

Overview of Lab

In this lab you will explore the technologies that provide new Windows Server 2008 management capabilities. You will begin by analyzing a server configuration using Server Manager, and then by performing role and feature management. You will also perform some basic server administration using ServerManagerCMD. You will then use Windows PowerShell to review server settings, and perform diagnostic analysis of the server. Finally you will configure WinRM and use a combination of event subscriptions and remote shell commands to remotely administer a Server Core installation.

Scenario

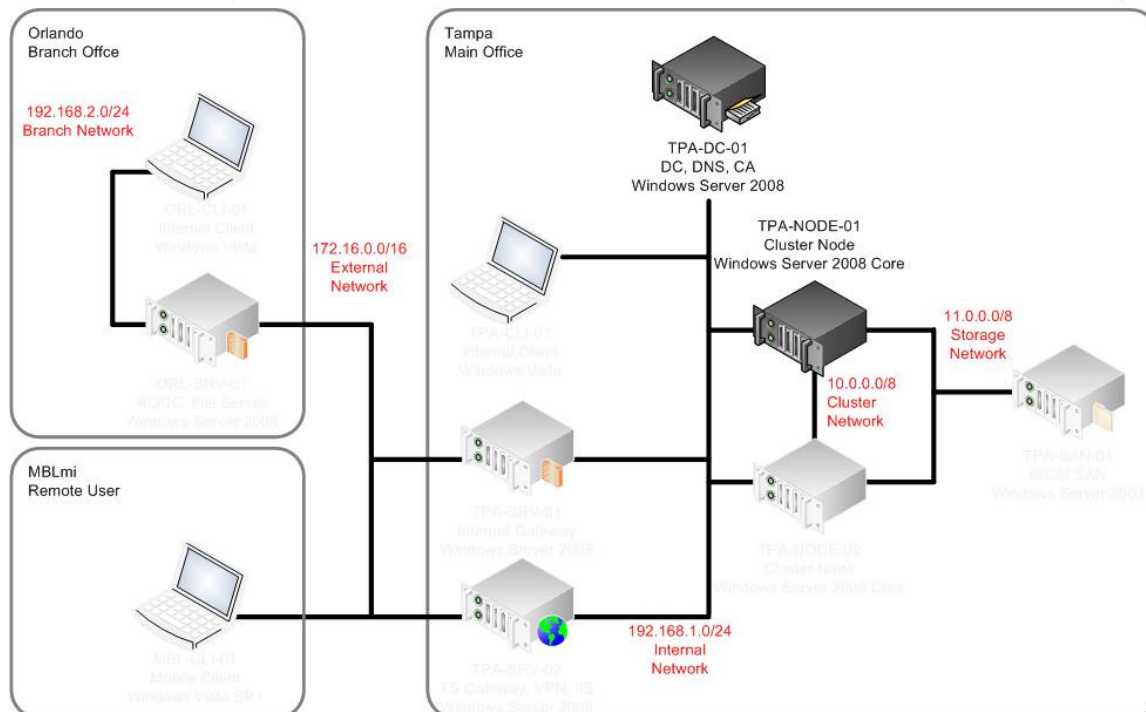
This lab is implemented using Woodgrove Bank. Woodgrove Bank is a local investment bank with two offices. The main office is located in Tampa, Florida. There is a branch office in Orlando, FL. Several remote users work from home offices in Miami. Woodgrove Bank has standardized on Windows Server 2008 and Windows Vista. They have implemented technologies such as TS Gateway, Failover Clustering, Read Only Domain Controller, and Network Access Protection. The relevant parts of the network are shown below. Computers you will use in this lab are highlighted in dark grey.

Woodgrovebank.com

Windows Server 2008 Management Scenario

Windows Server 2008 - JumpStart Clinics

Core Infrastructure Diagram



Woodgrove Bank has completed the implementation of its new core infrastructure consisting of Windows Server 2008 and Windows Vista. After evaluating the completed installations, Woodgrove Bank has identified areas where better management of resources using the tools included in the Windows Server 2008 operating system would lower operational costs and increase IT efficiency. Specifically, they have decided that all administrators should use Server Manager to interactively manage roles and features as well as maintain health status on servers. They have also decided that any new servers would be configured with appropriate roles and services using ServerMangerCMD. They have evaluated a large number of automation tools and scripts and decided that migration to Windows PowerShell will reduce maintenance of tools and training of staff, while giving them better options as new products emerge. Finally, they have decided to consolidate event logs from several servers onto a single server, so that the logs for the entire network can be analyzed from one place.

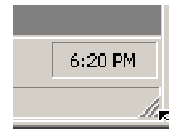
Virtual Machine Technology

This lab makes use of Microsoft Virtual Server 2005 or Microsoft Virtual PC, which are applications that allow you to run multiple virtual computers on the same physical hardware. During the lab, you will switch among different windows, each of which contains a separate virtual machine.

Before you start the lab, familiarize yourself with the following basics of virtual machines:

- To switch the focus for your mouse and keyboard to the virtual machine, click inside the virtual machine window.

- To remove the focus from a virtual machine, move the mouse pointer outside the virtual machine window.
- To mimic the CTRL+ALT+DELETE key combination inside a virtual machine, use <RIGHT>ALT+DEL. The <RIGHT>ALT key is called the host key.
- To enlarge the size of the virtual machine window, drag the lower-right corner of the window as seen in the screenshot. This function works in Virtual PC only.
- To switch to and from full-screen mode, press <RIGHT>ALT+ENTER.



Computers in this lab

This lab uses computers as described in the following table. Before you begin the lab, you must start the virtual machines and then log on to the computers. Ensure the TPA-DC-01 virtual machine is fully started before starting any other virtual machines.

| Virtual Machine | Role |
|-----------------|----------------------------------|
| TPA-DC-01 | Domain Controller |
| TPA-NODE-01 | Server Core that must be managed |

All user accounts in this lab use the password **Passw0rd!**

Note Regarding Pre-release Software

Portions of this lab include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered as a result of using pre-release software.

Note Regarding User Account Control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that user's confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Exercise 1: Using Server Manager

Woodgrove Bank has decided to standardize on the use of Server Manager for interactive management of servers. Administrators are instructed to use remote desktop connections and Server Manager when checking health and status information. They have determined that because all information relevant to a role, including services, event logs, and best practices are stored in one location, they can reduce configuration mistakes and omissions. In addition they have decided that all listed best practices for each server role should be implemented.

In this task you will use Server Manager and ServerManagerCMD to review the configuration of the TPA-DC-01. You will then manage the roles and features and add new role services and features.

→ Reviewing Server Configuration using Server Manager

Server Manager provides a central location for accessing all information relating to a role. From this location you can evaluate the health of the role by checking services and event log entries, as well as receive guidance and best practice information. In this task you will review the status of the installed roles on the server, specifically focusing on the health of Active Directory.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Password!**.
2. On the Start menu, point to **Administrative Tools**, and then click **Server Manager**.
3. In **Server Manager**, review the contents of **Server Summary**.

The sever summary contains information that can give you a quick status of some of the most common server information such as IP address and Firewall status.

4. Scroll down and review the contents of **Roles Summary**.

This area contains the list of installed roles.

5. Scroll down and review the contents of **Features Summary**.

This area contains the list of installed features.

6. In **Server Manager**, in the navigation pane, click **Roles**.
7. In the **Roles** pane, click **Active Directory Domain Services**.
8. Under **Summary**, review the status of **Events** and **System Services**.
9. Scroll down, and under **Advanced Tools**, click **ADSI Edit**.

The most common tools and utilities are available as part of the role summary.

10. Close ADSI Edit

11. Under **Directory Service Tools**, click **Dsmgmt.exe**
12. Scroll down, under **Resources and Support**, click **Improve security and network traffic for a branch office by deploying a read-only domain controller**, and then review the **Description**.

→ Add a the FTP Server Role Service to the Web Server (IIS) Role

In this task you will use Server Manager to add a new role service to the Web Server (IIS) role. Role services are individual components that make up the functionality of a role. Some roles contain only one role services, while others, such as the Web Server (IIS) role, contain over 40 role services.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
2. In **Server Manager**, under **Roles**, click **Web Server (IIS)**, and then on the **Action** menu, click **Add Role Services**.
3. In the **Add Role Services** wizard, in **Role services**, check **FTP Publishing Service**, click **Next**, and then click **Install**.

This installation should take less than one minute.

4. When the **Add Role Services** wizard has completed, click **Close**

→ Add the DHCP Server Role to TPA-DC-01

In this task you will add the DHCP Server role to TPA-DC-01. The add new role wizard dynamically adjusts based on the role that is being installed. This allows you to install and configure multiple roles in one task, reducing configuration errors and the need for rebooting.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
2. In **Server Manager**, click **Roles**.
3. In the **Roles** pane, click **Add Roles**.
4. In the **Add Roles Wizard**, click **Next**.
5. On the **Select Server Roles** page, check **DHCP Server** and then click **Next**.

Note that the Add Roles Wizard adjusts to allow you to configure the DHCP server during the installation.

6. Complete the DHCP Server configuration pages using the values in the following table. If a value is not listed in the table, leave it at its default setting. When you have made the following configuration changes, click **Install**.

| Setting | Value |
|-----------------------------|---|
| Network Connection Bindings | Default |
| IPv4 DNS Settings | Default |
| IPv4 WINS Settings | Default |
| DHCP Scopes | Name: Network Starting IP: 192.168.1.20 Ending IP: 192.168.1.200 Subnet Mask : 255.255.255.0 Default Gateway: 192.168.1.2 |
| DHCPv6 Stateless Mode | Disabled |
| DHCP Server Authorization | Default |

The installation should take less than 2 minutes.

7. Click **Close** to close the **Add Roles Wizard**.
8. In **Server Manager**, under **Roles Summary**, click **DHCP Server**.
9. Review the information in the **DHCP Server** pane.

➔ Adding the Desktop Experience and Windows Backup Features to TPA-DC-01

In this task you will add two features that are commonly used on Servers. The Windows Desktop Experience adds tools such as Windows Media Player and the Windows Aero theme. This component is commonly added to servers that double as workstations such as those used by administrators or developers. It is also common on a server that functions as a Terminal Server to provide a better user experience to users. The Windows Backup Features allow you to schedule and configure server backup.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
2. In **Server Manager**, click **Features**.
3. In the **Features** pane, click **Add Features**.
4. In the **Add Features Wizard**, check **Desktop Experience** and **Windows Server Backup Features**.
5. In the **Add Features Wizard** dialog box, click **Add Required Features**, and then click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**

The installation should take less than 2 minutes.

7. On the **Installation Results** page, click **Close**, and then in the **Add Features Wizard**, click **Yes**.

TPA-DC-01 will now restart. Wait for the computer to restart before proceeding. The restart should take between 2 and 5 minutes. On slower computers, this could take as long as 15 minutes.

8. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
9. In **Resume Configuration Wizard**, click **Close**.
10. Close **Server Manager**
11. On the **Start** menu, click **All Programs**.

Note Windows Media Player, Windows Photo Gallery and other tools are available.

12. On the **Start** menu, point to **Administrative Tools**, and then click **Services**.
13. In **Services**, in the contents pane, click **Themes**.
14. On the **Action** menu, click **Properties**.
15. In **Themes Properties (Local Computer)**, in **Startup** type, click **Automatic**, click **Apply**, and then click **Start**.
16. Close all open windows.

You cannot apply a theme until the themes service is started.

17. **Right-Click** the **Desktop**, and then click **Personalize**.
18. In **Personalization**, click **Theme**.
19. In **Theme**, select **Windows Vista**, and then click **OK**.
20. Close all open windows.
21. On the **Start** menu, point to **Administrative Tools**, and then click **Windows Server Backup**.
22. Close **Windows Server Backup**.

➔ Performing Server Management with ServerManagerCMD

ServerManagerCMD is a command line version of Server Manager that supports three critical operations. It allows you to add and remove roles, role services, and features, as well as display information on installed roles, role services and features. The display operation, accomplished using the `-query` parameter is very helpful when you are exploring the functionality of a server and to see the configuration of the server in one

command. In this task you will query the installed roles, role services, and features on TPA-DC-01 and then remove the Windows Backup features.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
2. On the **Start** menu, click **Command Prompt**.
3. In the **Command Prompt** window, type the following command and then press ENTER.

```
ServerManagerCMD -Query
```

4. In the **Command Prompt** window, type the following command and then press ENTER.

```
ServerManagerCMD -remove backup-features
```

5. Close the **Command Prompt** window.

Exercise 2: Managing a Server Using Windows PowerShell

Woodgrove Bank is interested in reducing the operational costs of their infrastructure, and in providing automation for many of the tasks that administrators typically perform. In the past they have used a combination of scripting, command line tools, batch files and custom management applications to accomplish this. The result is a complex set of tools with an inconsistent structure. They have determined that they spend as much time maintaining and supporting these tools as they do in performing the tasks manually. To solve this problem, Woodgrove Bank has decided to standardize all scripting and automation on Windows PowerShell.

In this exercise, you will explore Windows PowerShell. Microsoft Windows PowerShell command line shell and scripting language helps IT Professionals achieve greater productivity. Using a new admin-focused scripting language, more than 130 standard command line tools, and consistent syntax and utilities, Windows PowerShell allows IT Professionals to more easily control system administration and accelerate automation. Windows PowerShell is easy to adopt, learn, and use, because it works with your existing IT infrastructure and existing script investments, and because it runs on Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008. Exchange Server 2007, System Center Operations Manager 2007, System Center Data Protection Manager V2, and System Center Virtual Machine Manager leverage Windows PowerShell to improve efficiency and productivity.

Windows Powershell supports TAB key completion. You can complete many commands by typing the first few characters of the command and then pressing the TAB key.

For all tasks in this exercise, ensure you are logged on to TPA-DC-01 as Woodgrovebank\Administrator with a password of Passw0rd!, and that you have Windows PowerShell open.

→ Using Windows PowerShell Help

In this task you will explore the built-in help available in Windows PowerShell. Extensive help is available for all cmdlets using the Get-Help cmdlet.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank\Administrator** with a password of **Passw0rd!**.
2. On the **Start** menu, navigate to **All Programs/Windows PowerShell 1.0** and click **Windows PowerShell**.
3. In **Windows PowerShell**, type the following command and then press ENTER.

```
get-help get-command
```

The get-help cmdlet can be used to display detailed help on any other cmdlet.

- In **Windows PowerShell**, type the following command and then press ENTER.

```
get-help get-eventlog -full
```

The full help details (including examples) are now displayed.

- In **Windows PowerShell**, type the following command and then press ENTER.

```
get-help get-eventlog -parameter *
```

The available parameters for the get-command are now displayed.

- In **Windows PowerShell**, type the following command and then press ENTER.

```
help get-eventlog -parameter *
```

The help command calls the get-help command – however you will note that now the help is displayed one screen at a time.

- In **Windows PowerShell**, press ENTER until the help has completed displaying.
- In **Windows PowerShell**, type the following command and then press ENTER.

```
get-help about_wildcard
```

Help for the topic of wildcards is now displayed on the screen.

→ Create and Manage Aliases

In this task, you will create an alias that will enable you to use a shorter command to run a single cmdlet or to launch an application in Windows PowerShell. Many PowerShell cmdlets have alias that represent familiar commands. For example the get-childitem has two aliases; DIR and LS.

- In **Windows PowerShell**, type the following commands, pressing ENTER after each line.

```
set-alias gh get-help
get-help
gh
```

gh can now be used as a shorthand version of get-help – the results from get-help and gh are identical.

- In **Windows PowerShell**, type the following commands, pressing ENTER after each line.

```
set-alias np c:\windows\system32\notepad.exe  
Np
```

Notepad now launches. Alias can be created to any single command or cmdlet.

3. In **Notepad**, in the **File** menu, click **Exit**.
4. In **Windows PowerShell**, type the following commands, pressing ENTER after each line.

```
remove-item alias:np  
np
```

An error occurs as the alias np no longer exists.

→ Create and Use Functions

In this task, you will create a function. A function in Windows PowerShell is a more complex version of an alias that supports the use of parameters. Functions can be created as shortcuts to complex PowerShell commands.

1. In **Windows PowerShell**, type the following command and then press ENTER.

```
function display-updatelog {notepad c:\windows\WindowsUpdate.log}
```

2. In **Windows PowerShell**, type the following command and then press ENTER.

```
Display-UpdateLog
```

The Windows Update Log file is now opened in Notepad.

3. In **Notepad**, in the **File** menu, click **Exit**.
4. In **Windows PowerShell**, type the following command and then press ENTER.

```
Remove-Item Function:Display-UpdateLog
```

→ Navigate the File System.

In this task you will use the traditional command line commands of CD and DIR and then compare them to the Windows PowerShell navigation commands.

1. In **Windows PowerShell**, type the following commands, pressing ENTER after each line.

```
cd c:\Windows  
dir  
ls  
set-location c:\ProgramData  
get-childitem
```

The CD alias calls the set-location cmdlet and the dir and ls aliases call the getchild-item cmdlet.

→ Modify the Registry.

In this task, you will use Windows PowerShell to navigate and view the registry of the local machine. In addition to viewing the registry, you can also manipulate it. This makes Windows PowerShell as functional as the REG command.

1. In Windows PowerShell, type the following commands, pressing ENTER after each line.

```
cd hk1m:
dir
cd Software\Microsoft\Windows\CurrentVersion\Run
gp . *
```

The properties of the RUN registry key are displayed. Note the first four properties are properties of the key specific to Windows PowerShell. The key entries are displayed after that list. The GP . * is short for get-itemproperty -path . -name *

→ Navigate the Certificate Store

In this task you will use Windows PowerShell to examine the trusted root certification authority's certificates on TPA-DC-01.

1. In **Windows PowerShell**, type the following commands, pressing ENTER and examining the results after each line.

```
cd cert:
dir
cd LocalMachine
dir
cd Root
dir
```

2. In **Windows PowerShell**, type the following command and then press ENTER.

```
get-childitem | format-list -property *
```

The formatted property details for the selected certificate are now displayed.

→ Display System Information using WMI

In this task, you will use Windows PowerShell to retrieve and view system information using WMI. You will view the status of system services and then view information on the motherboard installed in the computer.

1. In **Windows PowerShell**, type the following commands, pressing ENTER and examining the results after each line.

```
Get-WMIObject win32_service | format-table
Get-WMIObject win32_baseboard | format-list -property *
```

→ Configuring The Script Execution Policy

Windows PowerShell does not run scripts by default. By default when you double click a Windows PowerShell script, it opens in Notepad. When you type a script name at the

command prompt, the script will only run if the execution policy allows it to run. There are several different execution policies, with unrestricted being the least secure. In this task you will set the execution policy for a single Windows PowerShell console session, as well as a system policy using Group Policy Editor.

1. In **Windows PowerShell**, type the following commands, pressing ENTER and examining the results after each line.

```
Get-help Set-ExecutionPolicy
Set-ExecutionPolicy unrestricted
```

2. On the **Start** menu, in **Start Search**, type **GPEdit.msc** and then press ENTER.
3. In **Local Group Policy Editor**, navigate to **User Configuration/Administrative Templates/Windows Components/Windows PowerShell**.
4. In the Contents pane, click **Turn on Script Execution** and then on the **Action** menu, click **Properties**.
5. In **Turn on Script Execution Properties**, click **Enabled**, in **Execution policy**, click **Allow local scripts and remote signed scripts**, and then click **OK**.

You are performing this change on the local policy. You may also make this change globally using a domain based Group Policy object. By default, the execution policy setting is only available on Windows Vista and later, but you may download the administrative template from the Windows PowerShell website.

6. Close **Local Group Policy Editor**.

Exercise 3: Managing a Remote Computer with WinRM

Woodgrove Bank has decided to use WinRM as a core part of its management strategy. By using WinRM for remote server management, Woodgrove Bank is able to reduce the use of complex DCOM or RPC based connections, and rely on HTTP connections that are properly secured using HTTPS and authenticated using Kerberos machine authentication. They have decided to use tools included in Windows Server 2008 such as event subscriptions and WinRS (WinRM Remote Shell) to ensure servers are running correctly and administer them when issues arise.

Windows Remote Management (WinRM) is a remote management technology which allows WMI commands and queries to be sent over an HTTP network connection. WinRM requires a listener and a client. In this exercise you will configure a WinRM listener on a Server Core computer, and then create an event subscription to manage the Server Core computer. You will then use WinRS to install an additional role on the Server Core computer.

→ Enable WINRM on TPA-NODE-01

In this task you will run the WinRM command to configure a listener on the Server Core machine. The quick configuration option creates a default HTTP listener which listens on all IP addresses, and uses Kerberos authentication.

1. Ensure you are logged on to **TPA-NODE-01** as **Woodgrovebank\administrator** with a password of **P@ssw0rd!**.

You will notice that TPA-NODE-01 is a ServerCore installation of Windows.

2. In the **Command Prompt**, type the following command, and then press ENTER.

```
WINRM QuickConfig
```

3. At the **Make these changes [y/n]?** prompt, press **Y** and then press ENTER.
4. In the **Command Prompt**, type the following command, and then press ENTER.

```
WINRM Enum Winrm/Config/Listener
```

This command will display the configuration of the listener. The configuration specifies that the listener is listening on HTTP on all IP addresses, and will negotiate the most secure communication method. You can configure the listener to use HTTPS, or listen on specific ports or addresses using the WinRM command.

→ Configure TPA-NODE-01 to Allow Event Subscriptions

Windows Server 2008 includes the Event Log Readers group. Event subscriptions use the machine account of the subscribing computer to connect to the target event log. In

this task you will give the machine account of TPA-DC-01 permission to read the event logs of TPA-NODE-01.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank/Administrator** using the password **Passw0rd!**.
2. On the **Start** menu, in **Start Search**, type **MMC**.
3. In **Console1**, on the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, in **Available snap-ins**, click **Local users and Groups** and then click **Add**.
5. In the **Choose Target Machine** dialog box, click **Another computer**, type **TPA-NODE-01**, and then click **Finish**.
6. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
7. In **Console1**, expand **Local Users and Groups (TPA-NODE-01)** and then click **Groups**.
8. In the contents pane, click **Event Log Readers**, and then on the **Action** menu, click **Add to group**.
9. In the **Event Log Readers Properties** dialog box, click **Add**.
10. In the **Select Users, Computers, or Groups** dialog box, click **Object Types**, check **Computers**, and then click **OK**.
11. In **Enter the object names to select**, type **TPA-DC-01**, and then click **OK**.
12. Click **OK** to close the **Event Log Readers Properties** dialog box.

➔ **Subscribe to Events on TPA-NODE-01**

In this task you will create a new event subscription which copies all errors from TPA-NODE-01 to TPA-DC-01.

1. Ensure you are logged on to **TPA-DC-01** as **Woodgrovebank/Administrator** using the password **Passw0rd!**.
2. On the **Start** menu, point to **Administrative Tools**, and then click **Event Viewer**.
3. In **Event Viewer**, under **Windows Logs**, click **Application**.
4. On the **Action** menu, click **Clear Log**.
5. In the **Event Viewer** dialog box, click **Clear**.

By default, all forwarded events go to the forwarded events log. Later in this task you will use Windows PowerShell to query the forwarded events by querying the application log. Windows PowerShell is unable to query the Forwarded Events log.

6. In **Event Viewer**, click **Subscriptions**.

7. In the **Event Viewer** dialog box, click **Yes**.
8. In the **Actions** pane, click **Create Subscription**.
9. In the **Subscription Properties** dialog box, in **Subscription name**, type **Error System Events on TPA-NODE-01**.
10. In **Destination** log, select **Application**.

You will need to expand the treeview embedded in the drop-down list to locate the Application log. Check the Application log to select it.

11. In **Subscription type and source computers**, click **Select Computers**.
12. In the **Computers** dialog box, click **Add Domain Computers**.
13. In the **Select Computer** dialog box, type **TPA-NODE-01** and then click **OK**.
14. Click **OK** to close the **Computers** dialog box.
15. In **Events to collect**, click **Select Events**.
16. In the **Query Filter** dialog box, in **Logged**, select **Last 30 Days**, in **Event Level**, check **Critical**, in **Event logs**, select **System**, and then click **OK**.
17. Click **OK** to close the **Subscription Properties** dialog box.

→ Review the Events on TPA-NODE-01

In this task you will review the contents of the Application log on TPA-DC-01. This log will contain all events that meet the criteria of the subscription you created in the previous exercise.

18. In **Event Viewer**, under **Windows Logs**, click **Application**.
19. Review the listed events.

If no events appear, check the properties of your event subscription. Note that it may take a few minutes for the events to be retrieved from TPA-NODE-01

20. On the **Start** menu, navigate to **All Programs/ Windows PowerShell 1.0**, and then click **Windows PowerShell**.
21. In **Windows PowerShell**, type the following command and then press ENTER. This command will display events recorded in the Application log.

```
Get-eventlog Application | where {$_.MachineName -eq "TPA-NODE-01.Woodgrovebank.com"}
```

→ Use WinRM to Manage Roles and Features on TPA-NODE-01

In this task you will use the WINRM command in conjunction with the OCLIST command to install the print server role on TPA-NODE-01. The OCLIST command

provides the same functionality as ServerMangerCMD, but is only available on a ServerCore installation of Windows.

22. On the **Start** menu, click **Command Prompt**.

23. In the **Command Prompt**, type the following commands, pressing ENTER after each one.

```
WinRS -R:TPA-NODE-01 oc1ist  
WinRS -R:TPA-NODE-01 ocsetup Printing-ServerCore-Role
```

It is possible for the installation of the Printing Server role to take a very long time in this pre-release version of Windows. If the role installation does not complete in a timely manner, press CTRL+C to terminate it.

This is the end of this lab.

Appendix

This appendix contains additional information that relates to the contents of the Lab.

➔ Links to Reference Material

The following links represent additional information and resources that relate to this lab.

1. Server Manager resource page -
<http://www.microsoft.com/windowsserver2008/servermanagement.aspx>
2. WinRM Comamnd Line Reference -
<http://technet2.microsoft.com/windowsserver/en/library/9d08e3bf-ced4-4ac3-bc3c-753af4458e6c1033.aspx?mfr=true>
3. Windows PowerShell Home Page -
<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.aspx>