Skip to content

Chapter 5. Manage configuration and protection

There is more to managing a private cloud than just deployment and monitoring. You often times need to ensure that the configuration of the servers that host private cloud resources, as well as the workloads running within the private cloud, do not deviate too far from their appropriate configuration. You need to ensure that the servers that host private cloud resources, as well as the workloads running within the private cloud, are kept current with software updates. You also need to ensure that the workloads and the servers that they run on are regularly backed up and able to be recovered, both for business continuity purposes and to accomplish data retention objectives.

Objectives in this chapter:

Objective 5.1: Manage compliance and configuration

The practice of server administration increasingly involves not just ensuring that a workload functions in a reliable manner, but that servers themselves are configured in a way that meets legislative requirements. In many industries, computers must meet configuration standards dictated by legislation. The compliance functionality of the system center suite allows you to assess whether workloads in a private cloud are configured in a manner that meets the organization's legal responsibilities.

This section covers the following topics:

Implementing System Center Process Pack for IT GRC

GRC is an acronym for governance, risk management, and compliance. The IT GRC Process Pack allows you to provide automated compliance management through the System Center suite. The System Center Process Pack for IT GRC allows you to manage IT operations and information management; it does not include other governance, risk management, and compliance functionality for other areas such as organizational accounting and business operations.

A control objective is a desired state result that has been met through risk assessment. For example, a control objective might be that user accounts of contract workers have an expiry date. This objective might have been selected after risk analysis found that some contractors had network access after their contract term finished. Control activities allow control objectives to be accomplished.

The System Center Process Pack for IT GRC uses the following System Center segments:

- **Service Manager** This hosts the System Center Process Pack for IT GRC and allows you to run the controls and activities that are necessary to meet control objectives. The System Center Process Pack for IT GRC requires that Service Manager be configured with the Active Directory, Operations Manager, and Configuration Manager connectors.
- **Service Manager data warehouse** This allows you to generate compliance and risk reports to audit and review compliance information. It is required for System Center Process Pack for IT GRC reporting.
- **Configuration Manager site server** Configuration Manager provides configuration drift reporting. Configuration drift occurs when a computer's configuration changes from those

specified in a desired configuration baseline. It requires the deployment of Configuration Manager agents on monitored computers.

- **Operations Manager** This manages alerts generated when computers drift from the desired configuration baseline. It requires the deployment of the Operations Manager agent on to monitored computers.

You install the System Center Process Pack for IT GRC on to the Service Manager server. After you have the Process Pack, run the MpSyncJob to synchronize Service Manager with the data warehouse. Then import the IT Compliance Management Libraries into Service Manager and the desired Configuration Management configuration items and baselines into Configuration Manager.

More Info: **System Center Process Pack for IT GRC**

You can learn more about the System Center Process Pack for IT GRC at *http://technet.microsoft.com/en-us/library/dd206732.aspx*.

When implementing a compliance program, it is occasionally necessary to configure program exceptions. You create exceptions for services or servers that cannot be made compliant with control objectives. You can create the following exception types:

- **Control activity scope exceptions** This type of exception allows you to exclude specific control activities when checking compliance.
- **IT GRC program exceptions** This type of exception allows you to exclude a specific computer from an IT GRC program.
- **IT GRC policy exceptions** This type of exception allows you to exclude control activities that are not applicable to your organization.

Exam Tip

Remember the different exception types that you can create when implementing a compliance program.

Understanding compliance settings

Compliance settings, which in previous versions of System Center Configuration Manager was termed Desired Configuration Management, allows you to monitor and remediate the configuration of computers.

Configuration Manager's compliance settings functionality uses configuration items and configuration baselines. A configuration item includes one or more settings that you want to assess to determine the compliance state of a computer. The configuration item includes compliance rules to evaluate the settings, as well as providing severity ratings for noncompliance. Some configuration items can be configured for remediation, which allows you to alter a non-compliant setting so that it is compliant. Configuration baselines are collections of software updates, configuration items, and other configuration baselines.

More Info: **Introduction to Compliance Settings**

You can learn more about compliance settings in Configuration Manager at *http://technet.microsoft.com/en-au/library/gg681958.aspx*.

Configuration items

Configuration Manager supports the following types of configuration items for assessing the compliance of computers:

- **Application configuration item** Use this type of configuration item to determine application compliance, including whether the application is installed and whether it is configured in a

specific manner.

- **Operating system configuration item** Allows you to determine operating system configuration compliance, such as whether particular roles or features are installed and particular registry keys are configured.
- **Software updates configuration item** Available when you manage software updates with Configuration Manager, and allows you to assess whether a computer has specific software updates installed.

For example, to create a configuration item related to whether Remote Desktop is enabled on a target computer running the Windows Server 2012 R2 operating system, perform the following steps:

1. In the Assets And Compliance workspace of the Configuration Manager console, select the Configuration Items node under the Compliance Settings node. On the ribbon, click Create Configuration Item.
2. On the General page of the Create Configuration Item Wizard, provide a name and ensure that the type of configuration item is set to Windows, as shown in Figure 5-1.

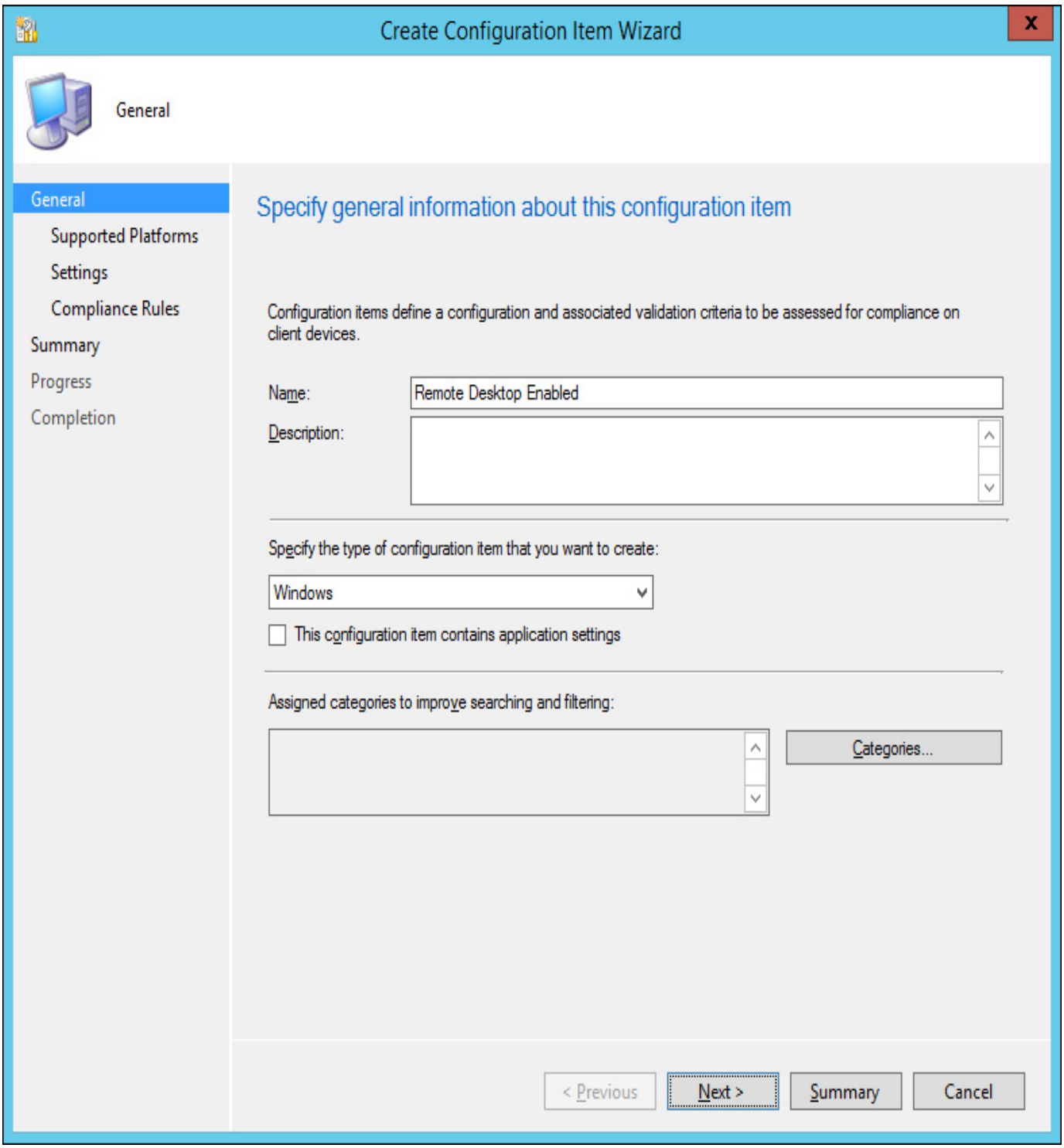

FIGURE 5-1 Create Configuration Item Wizard

3. On the Supported Platforms page, ensure that Windows Server 2012 R2 is selected, as shown in Figure 5-2. You should only select the operating systems that you want the configuration item assessed for on this page.

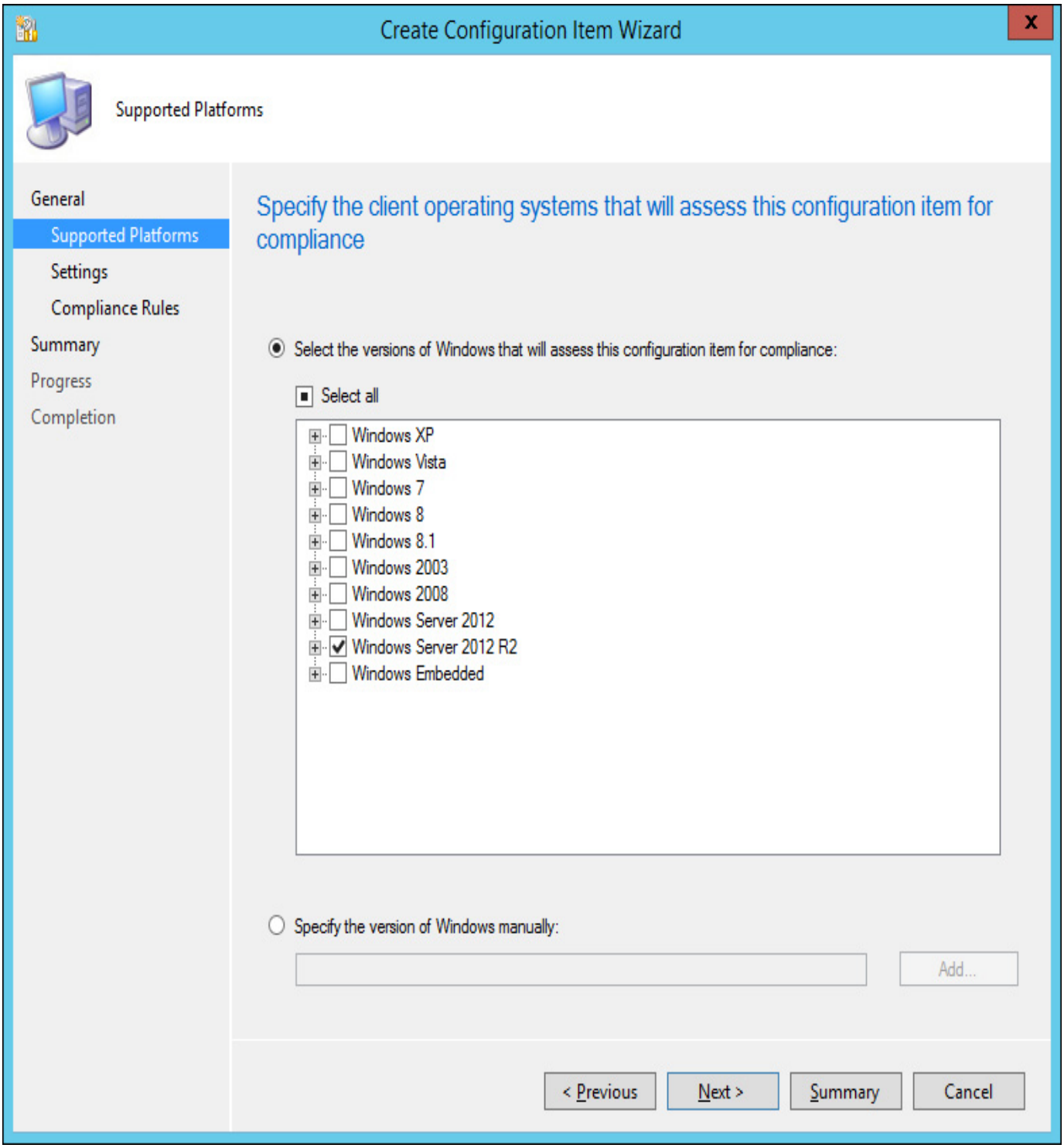

FIGURE 5-2 Select Windows versions

4. On the Settings page, click New. This will launch the Create Setting dialog box.
5. In the Create Setting dialog box, click Browse.
6. In the registry tree, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server, and select the fDenyTSConnections registry value. In this scenario, the value is set to 0, which allows Remote Desktop connections. Enable the This Registry Value Must Satisfy The Following Rule If Present Equals 0, as shown in Figure 5-3.

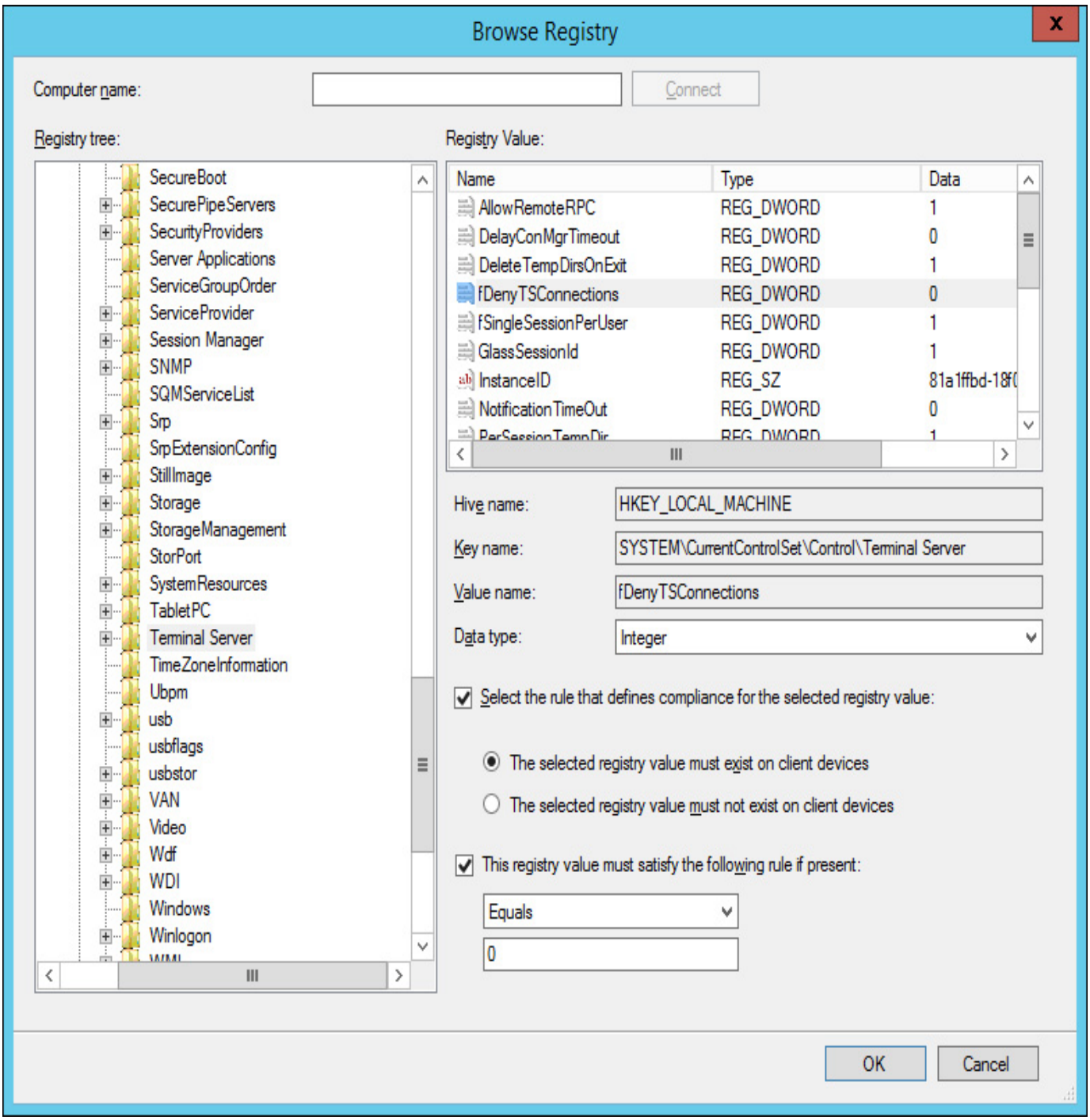

FIGURE 5-3 Browse Registry

7. Enter a name for the rule. On the Compliance Rules page, click the fDenyTSConnections Equals 0 condition, and click Edit. Select the Remediate Noncompliant Rules When Supported and Report Noncompliance If This Setting Instance Is Not Found check boxes, and set the Noncompliance Severity For Reports to Critical, as shown in Figure 5-4.

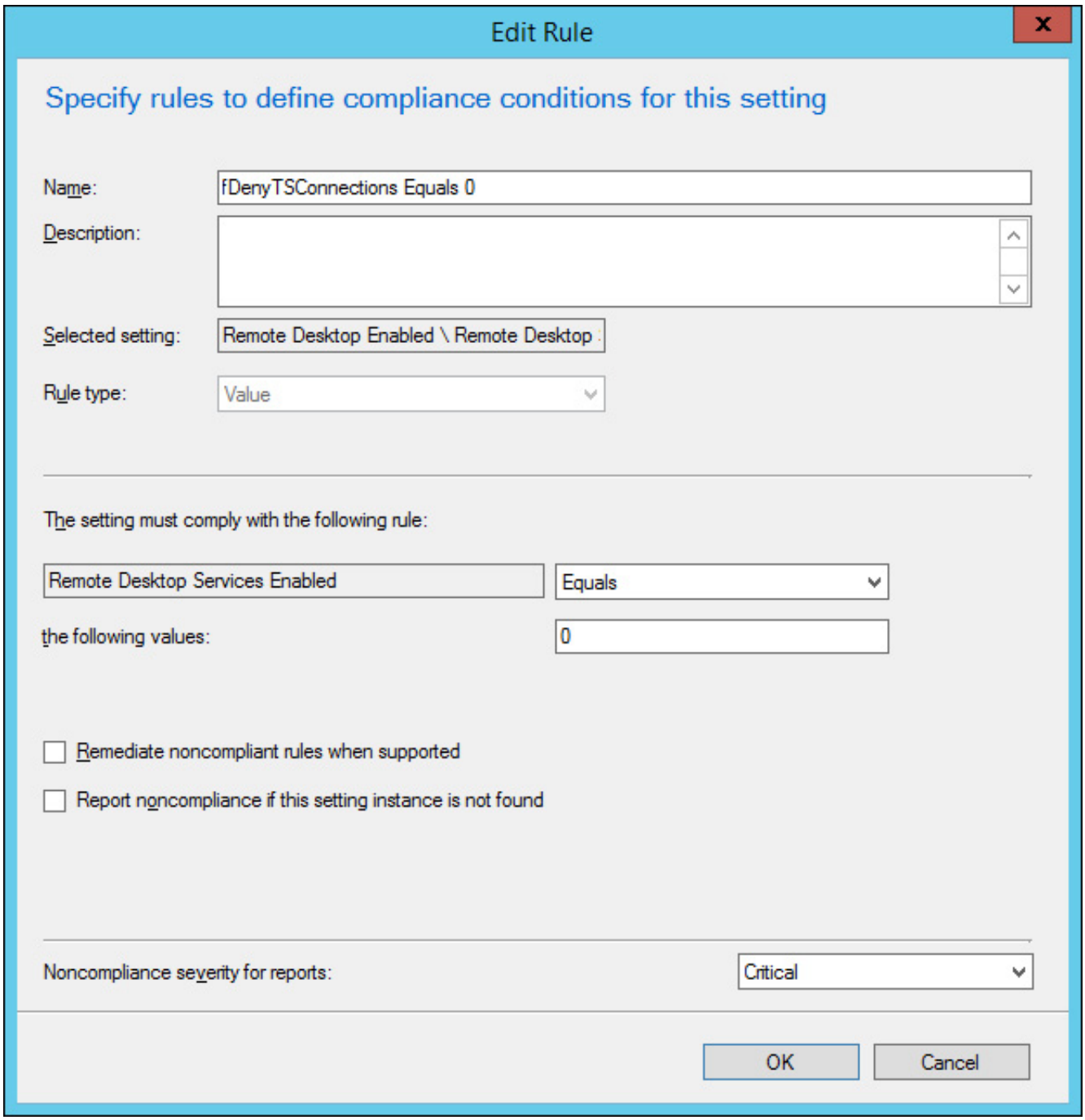

FIGURE 5-4 Edit Rule

8. Complete the wizard to create the configuration item.

More Info: **Configuration Items**

You can learn more about configuration items at *http://technet.microsoft.com/en-us/library/gg712331.aspx*.

Configuration baselines

Configuration baselines can include configuration items, software updates, and other configuration baselines. To create a configuration baseline that includes the Remote Desktop configuration item configured earlier, perform the following steps:

1. In the Assets And Compliance workspace of the Configuration Manager console, select Configuration Baselines under Compliance Settings.
2. On the ribbon, click Create Configuration Baseline. This will launch the Create Configuration Baseline dialog box.
3. On the Create Configuration Baseline dialog box, specify a name for the baseline, and then click Add, and then click Configuration Items.

4. On the Add Configuration Items dialog box, click the Remote Desktop Enabled configuration item, and click Add, as shown in Figure 5-5.

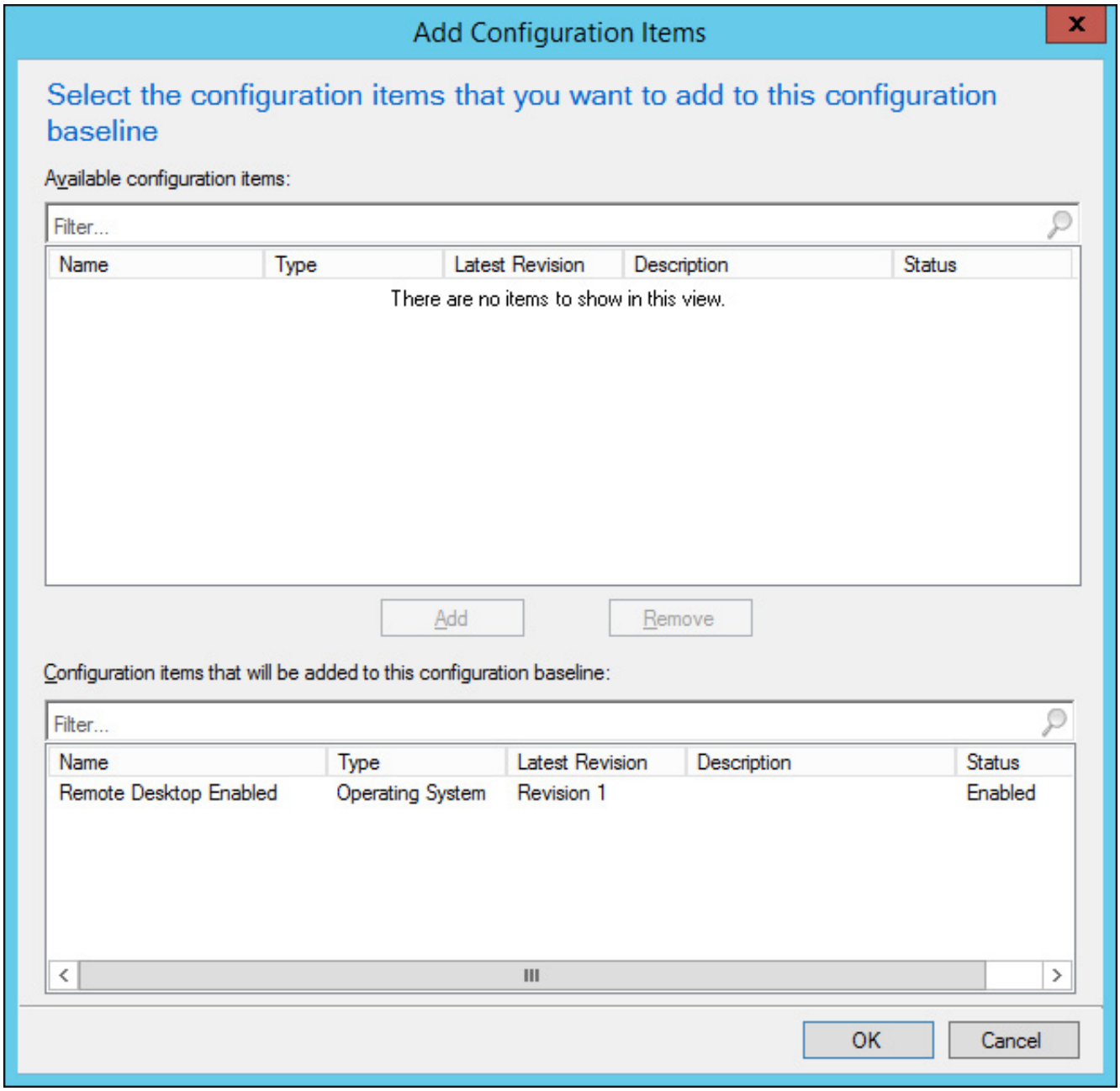

FIGURE 5-5 Add Configuration Items

5. Verify that the configuration item is present, as shown in Figure 5-6, and then click OK.

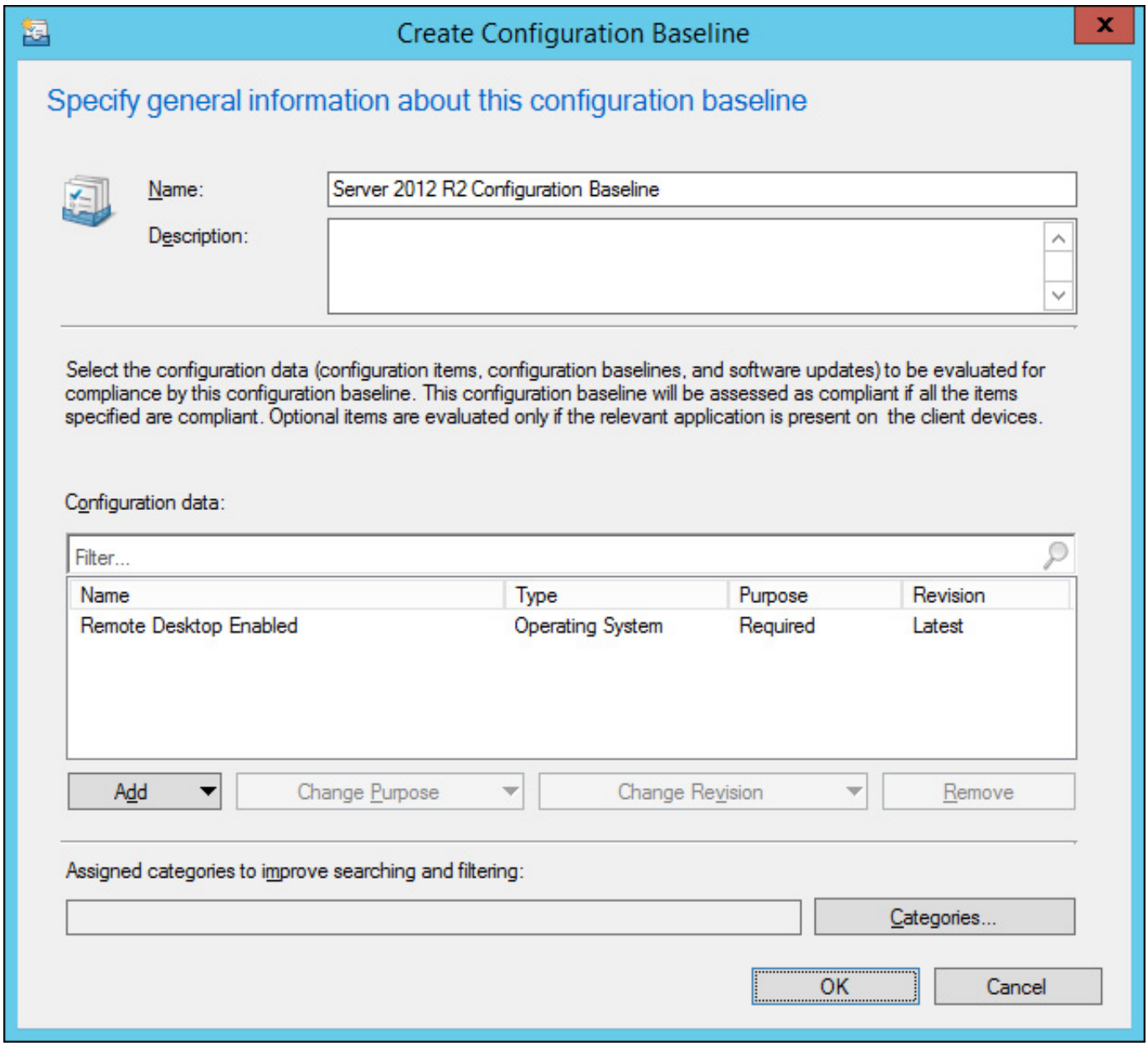

FIGURE 5-6 Create Configuration Baseline

To deploy the configuration baseline to a collection, select the configuration baseline, and click Deploy on the ribbon. When deploying the baseline, select the collection to which you want to deploy the baseline, and also choose whether you want to enable remediation. Figure 5-7 shows the Server 2012 R2 Configuration Baseline deployed to the Windows Server 2012 R2 Servers collection with the remediation option enabled.

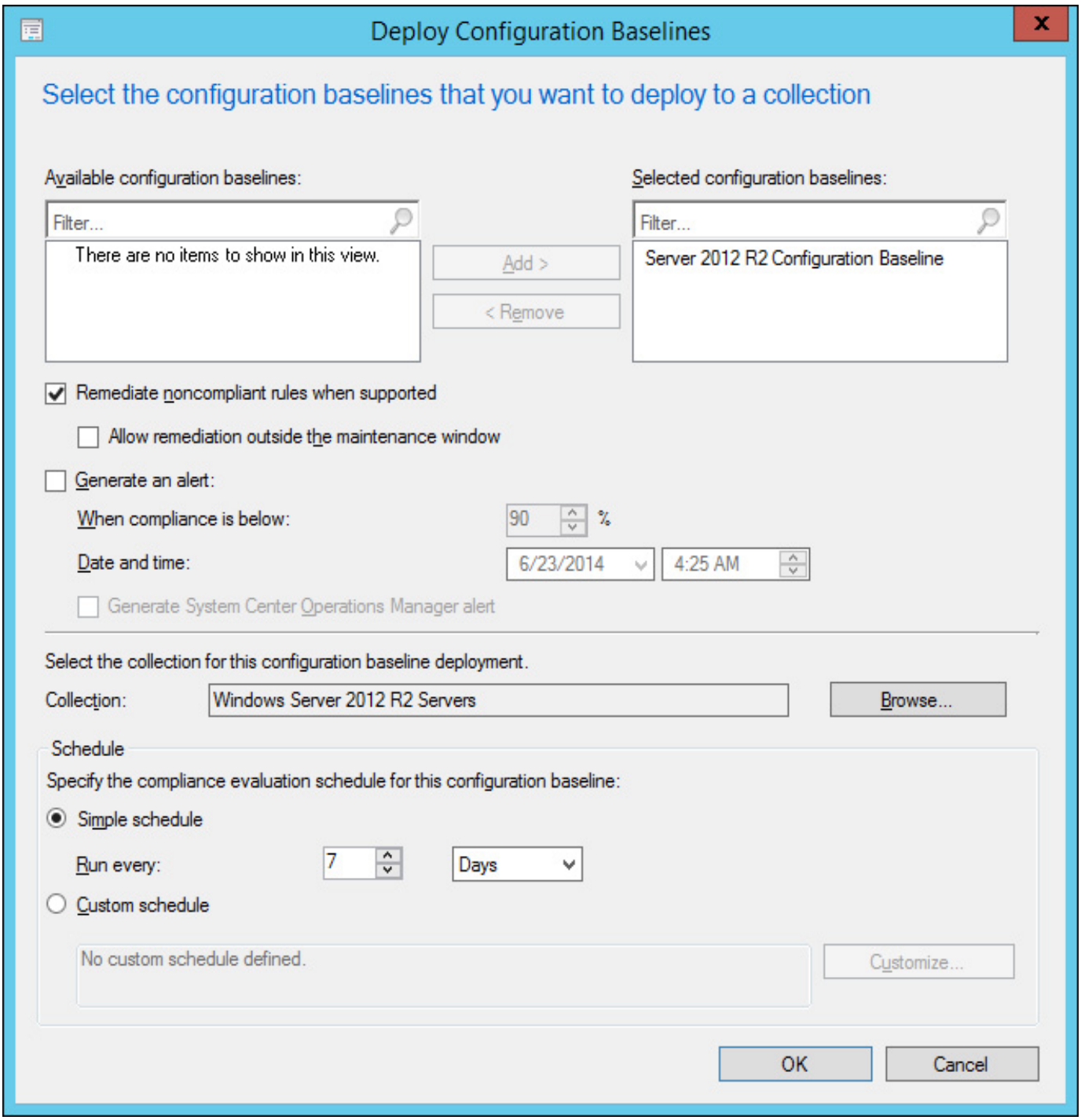

FIGURE 5-7 Deploy Configuration Baselines

Once the configuration baseline has been deployed, you'll be able to view a list of compliant and non-compliant computers from the Configuration Baseline node, by selecting the baseline in Deployments node in the Monitoring workspace, or by viewing reports in the Compliance And Settings Management report category.

More Info: **Configuration Baselines**

You can learn more about configuration baselines at *http://technet.microsoft.com/en-us/library/gg712268.aspx*.

Remediation

Certain types of configuration items can be remediated, but only when the item is included in a baseline deployment that you have also configured for remediation. Remediation is only available for the following types of computer related configuration items:

- Registry value
- Scripts

- WQL query configuration items

You can configure remediation to be performed, either by creating a value if it is not present, altering a value if it exists but is not compliant (for example, changing a registry value), or by running a remediation script. The remediation script will need to alter the setting to the desired state.

Using Desired State Configuration

Desired State Configuration (DSC) is a feature new to Windows PowerShell 4.0 that allows you to manage the configuration of computers, accomplishing many of the objectives with Windows PowerShell that you could otherwise accomplish using compliance settings with Configuration Manager. You can use DSC to perform the following tasks:

- Ensuring that server roles and features are either enabled or disabled
- Managing registry settings
- Managing files and directories
- Managing service and the state of processes
- Managing user and group accounts
- Software deployment
- Managing environment variables
- Assessing configuration state
- Remediating configuration drift

When using DSC, you define a Windows PowerShell script block using the configuration keyword. This script block allows you to specify the desired configuration for each computer (termed nodes in DSC). Within the script block, you can define resource blocks as a way of configuring specific resources. When you invoke the configuration, a MOF file is created in a new directory that is a child of the current directory with the same name as the configuration block. The newly created MOF file stores configuration information about the target computers. You can enforce the configuration by running the Start-DscConfiguration cmdlet.

More Info: **Desired State Configuration**

You can learn more about Desired State Configuration at *http://technet.microsoft.com/en-us/library/dn249912.aspx*.

Understanding System Center Advisor

System Center Advisor is a cloud-based service that collects data from computers and generates alerts based on that data. For example, System Center Advisor can generate alerts about missing security updates, or where the configuration of a computer deviates substantially from best practice. The knowledge used to raise these advisory alerts comes from Microsoft's engineering support team, and reflects direct customer experiences running the products in production environments.

System Center Advisor includes the Advisor web service, hosted in Microsoft's cloud, an on premise gateway, and one or more agents, which you deploy to computers in your environment. The agent functions in a way that is similar to the Operations Manager agent. By connecting to the web portal, you can view alerts and advise on how to remediate those issues. Figure 5-8 shows a typical System Center Advisor deployment, with agents installed on local computers communicating with a gateway, that forwards collected data that is stored and analyzed in the cloud.

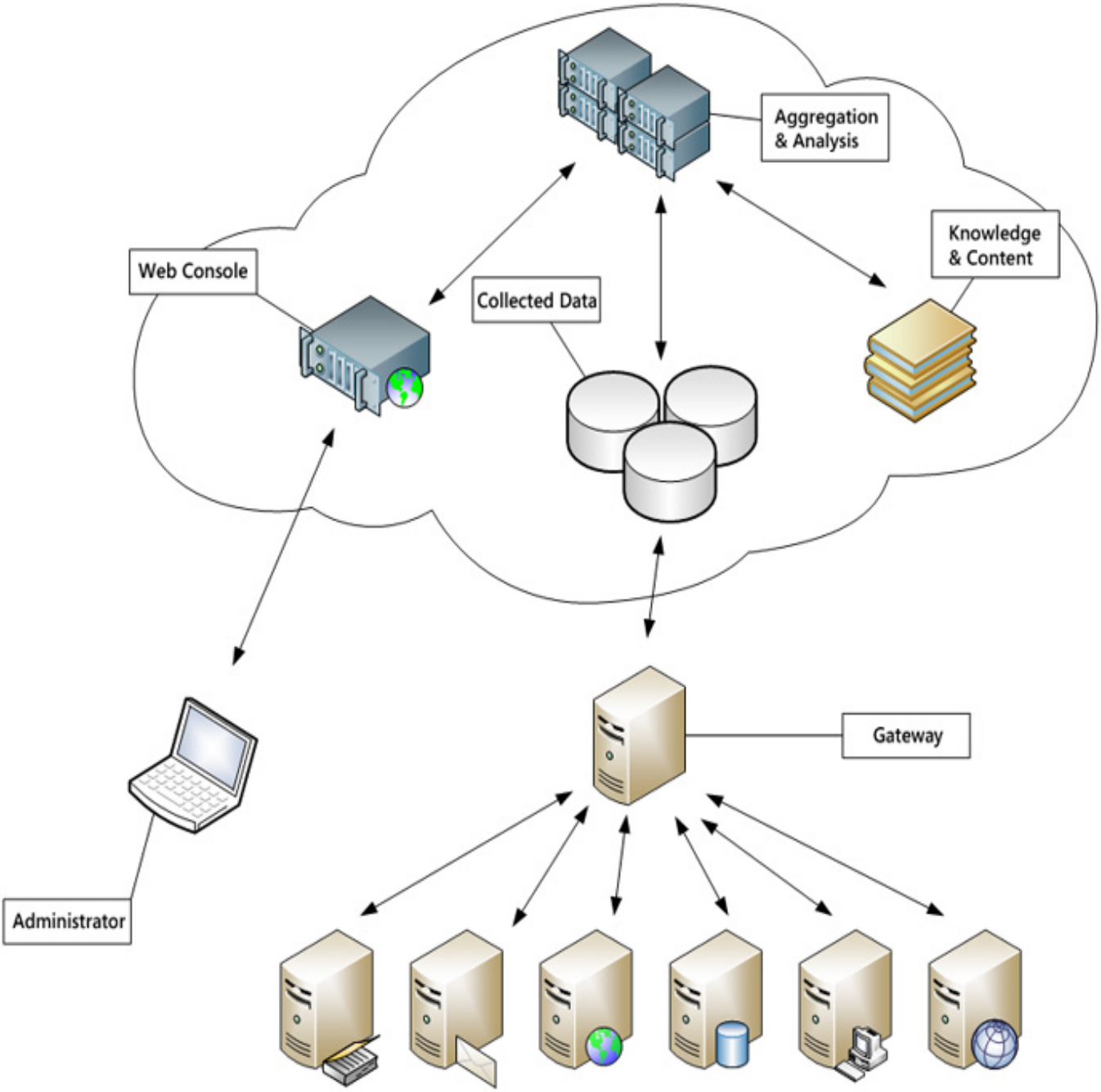

FIGURE 5-8 System Center Advisor

More Info: **System Center Advisor**

You can learn more about System Center Advisor at *http://onlinehelp.microsoft.com/en-us/advisor/ff962512.aspx*.

***Thought experiment*: System Center Advisor at Adatum**

You are planning on deploying System Center Advisor to a client named Adatum, who has a small number of servers as a way of monitoring whether those servers are current with the latest software updates. You deploy the System Center Advisor agent on to the servers on the internal network.

1. What server should you deploy on the perimeter network?
2. How will you review the status of the monitored servers?

Objective summary

- The System Center Process Pack for IT GRC allows you to perform compliance activities using Service Manager, Configuration Manager, and Operations Manager.
- A Configuration Manager compliance setting is a setting, such as an application or registry setting that can be checked.
- A configuration baseline is a collection of compliance settings, software updates, and other configuration baselines.
- Some compliance settings can be automatically remediated.
- Desired State Configuration allows you to check and remediate a computer's configuration using Windows PowerShell.
- System Center Advisor is a cloud-based monitoring service that can provide advice on how to better configure monitored servers.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following can you add to a Configuration Manager configuration baseline?
   - **A.** Configuration item
   - **B.** Compliance baseline
   - **C.** Software updates
   - **D.** Update baselines
2. Which System Center products are required to support the System Center Process Pack for IT GRC?
   - **A.** Configuration Manager
   - **B.** Operations Manager
   - **C.** Service Manager
   - **D.** Virtual Machine Manager
3. Which of the following connectors must you configure in Service Manager to support the deployment of the System Center Process Pack for IT GRC?
   - **A.** Active Directory
   - **B.** Orchestrator
   - **C.** Operations Manager
   - **D.** Configuration Manager

Objective 5.2: Manage Updates

This objective deals with the various methods you can use for managing software updates for your organization's private cloud deployment. The most basic method of managing software updates is to use Windows Server Update Services (WSUS). In a Microsoft private cloud environment, you are likely to use both Configuration Manager and VMM, both integrated with WSUS, to manage updates. You use VMM to manage updates for the servers involved in the virtualization infrastructure, and Configuration Manager to manage the updates for the virtual machines running within the private cloud.

This section covers the following topics:

- Managing updates with WSUS
- Managing updates with Configuration Manager
- Integrating WSUS with VMM
- Updating offline VMs

Managing updates with WSUS

WSUS is a Windows Server 2012 and Windows Server 2012 R2 role service that allows you to manage and deploy Microsoft operating system and application updates. Rather than having each computer in your organization connect over the Internet to acquire software updates, you can configure a server with the WSUS role installed to acquire these updates, and then to serve as a central distribution point. You can also integrate the WSUS role with Configuration Manager and with VMM, topics that are covered later in this section.

Configuring the WSUS server

Once you've installed the WSUS server role, you need to run the WSUS Server Configuration Wizard to configure how the WSUS server functions. The WSUS Server Configuration Wizard allows you to configure WSUS server settings. Running this wizard involves performing the following steps:

1. Choose whether the WSUS server will synchronize with Microsoft update, or synchronize with another WSUS server. If you synchronize with Microsoft update, the WSUS server will obtain updates from Microsoft's servers through the Internet. If you choose to synchronize with another WSUS server, you can choose to synchronize updates from that server, or configure the WSUS server as a replica, in which case you will synchronize approvals, settings, computers, and groups from the server. You configure replica servers in scenarios where you want to deploy multiple WSUS servers, but have them all use the same settings. Figure 5-9 shows a WSUS server configured to synchronize as a replica. When you configure a WSUS server as a replica, you don't need to choose languages, products, or classifications.

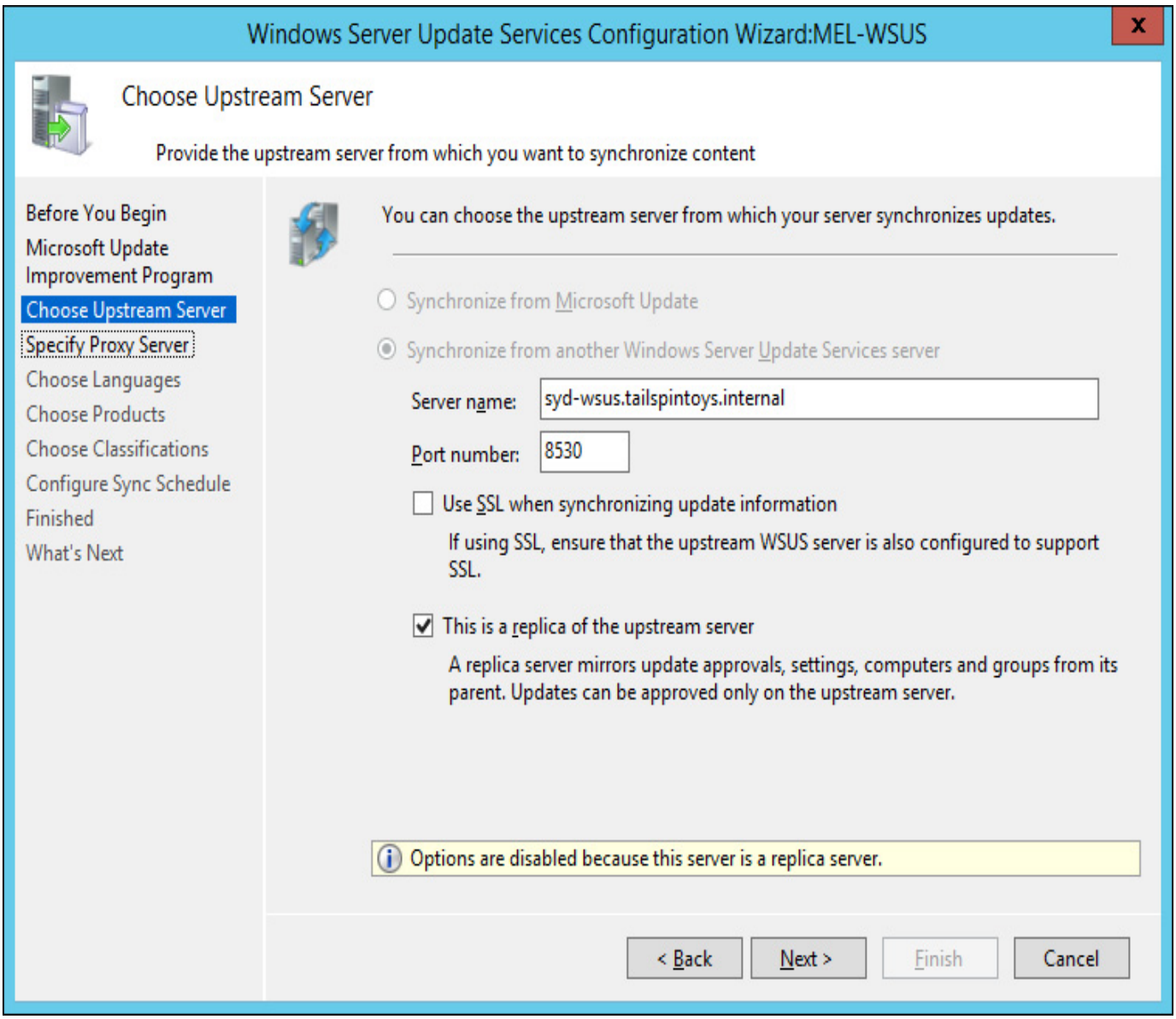

FIGURE 5-9 Windows Server Update Services Configuration Wizard

2. Next, you configure whether the WSUS server will use a proxy server during synchronization. If required, you can configure proxy server credentials.
3. The next step requires the WSUS server to synchronize with either Microsoft Update, or the upstream server. This allows the WSUS server to obtain a list of update types, language options, and products that the WSUS server will provide.
4. Once synchronization has completed, select whether to download updates in all languages, or updates in a specific language. Most organizations will only require updates in their local language. Figure 5-10 shows a configuration where only English is selected as the language.

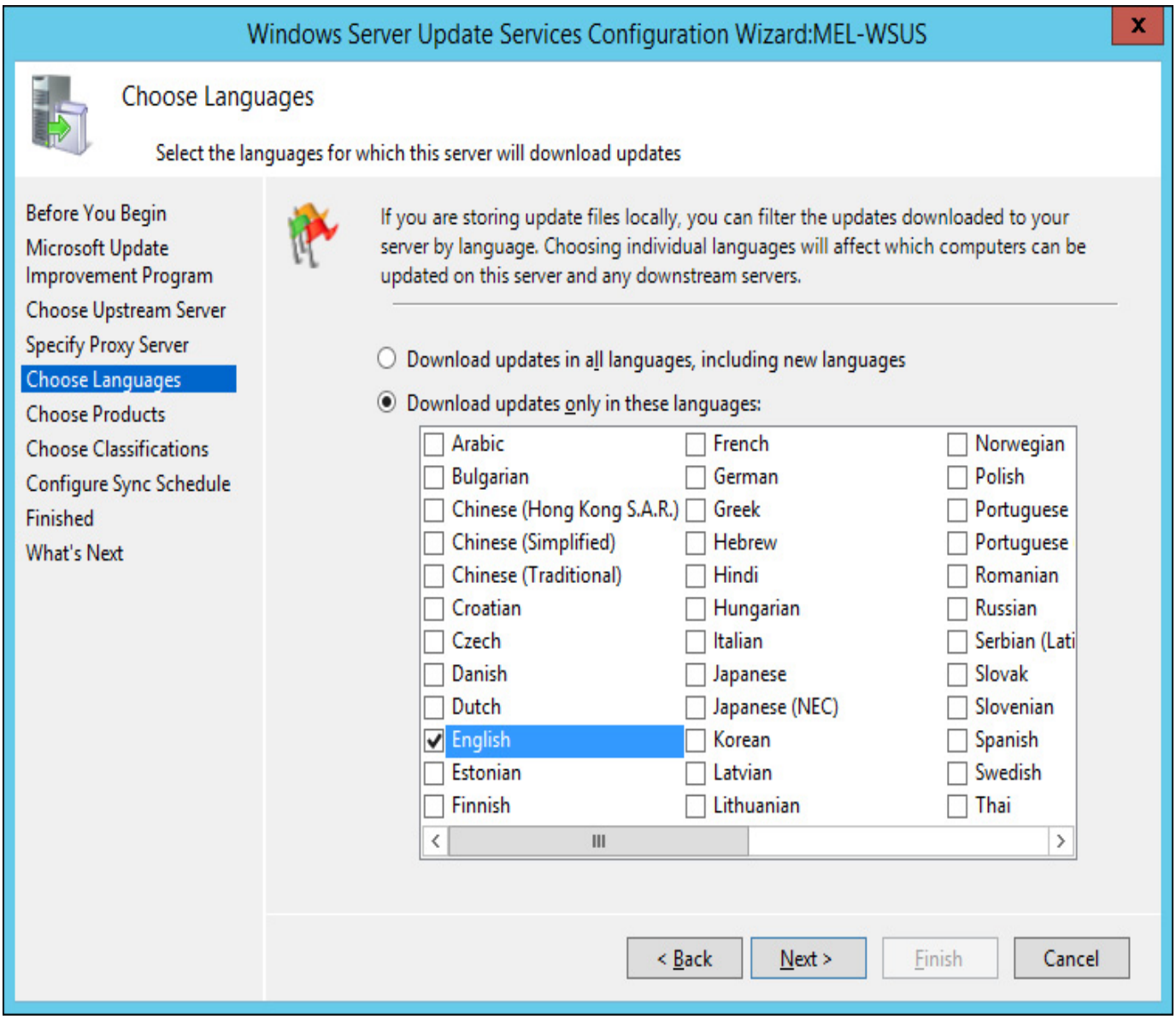

FIGURE 5-10 Update Services Configuration

5. On the Products page, select the products for which the WSUS server should obtain updates. To minimize the number of updates that will be downloaded, you should select only products that are used in your organization. Figure 5-11 shows the selection of updates for several System Center 2012 R2 products.

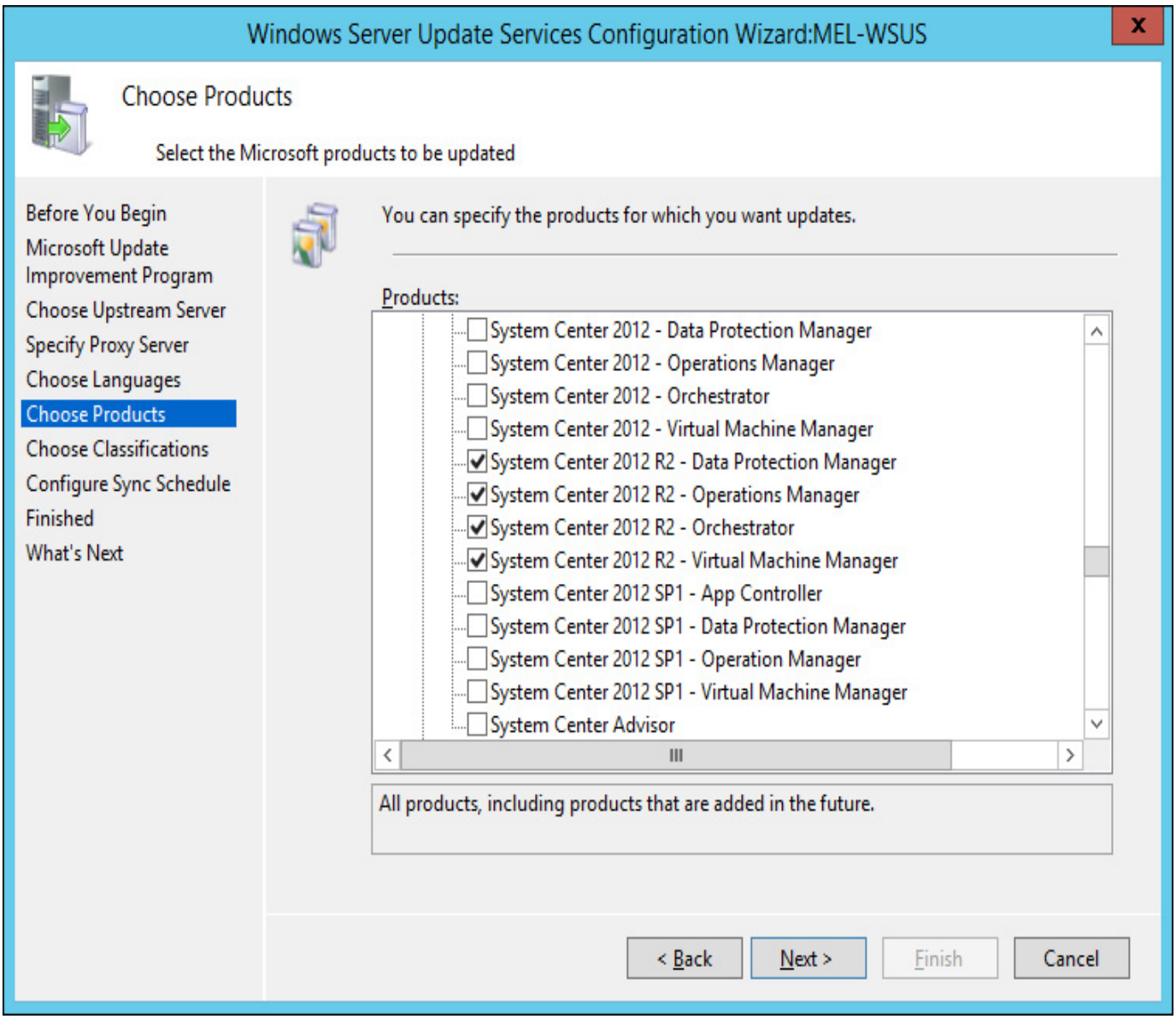

FIGURE 5-11 Product Selection

6. On the Classifications page, select which update classifications you want the WSUS server to synchronize. Figure 5-12 shows updates of all the classifications selected.

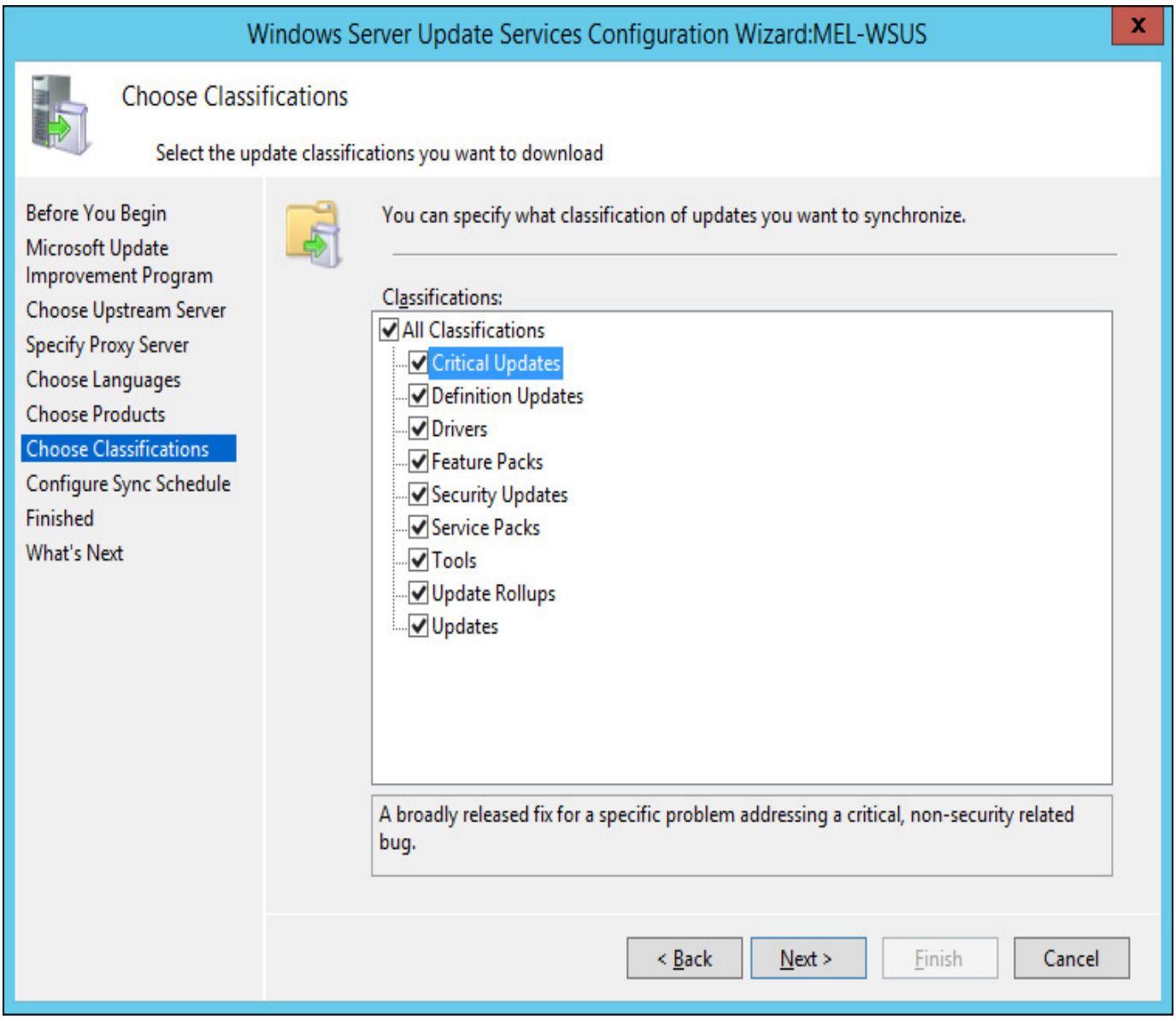

FIGURE 5-12 Choose classifications

7. The final step to take in configuring a WSUS server is to choose how often the WSUS server synchronizes, and to choose whether to perform an initial synchronization. The default is to have the WSUS server synchronize manually.

After deployment, you can modify the WSUS server's settings. For example, you might change the products, languages, or update classifications that the WSUS server uses when obtaining updates. You can also configure an "approvals only" WSUS server. An "approvals only" WSUS server is one where clients contact the WSUS server to determine which updates are approved for installation, but download the update files themselves from the Microsoft update servers on the Internet.

More Info: **Configuring WSUS**

You can learn more about integrating WSUS with VMM at *http://technet.microsoft.com/en-us/library/hh852346.aspx*.

Creating computer groups

You approve updates in WSUS on the basis of computer groups. This allows you to approve an update for deployment to one group, such as a test server group, whilst not deploying the update to every computer in your organization. You can assign computers to computer groups manually, or by using Group Policy. You should create the computer groups on the WSUS server prior to configuring WSUS computer group assignment through Group Policy. You'll only be able to manually assign computers to groups that have contacted the WSUS server for updates.

To create computer groups on the WSUS server, perform the following steps:

1. In the WSUS Server console, expand the Computers group, and then the All Computers group.
2. On the Actions pane, click the Add Computer group.
3. On the Add Computer Group dialog box, enter a name for the computer group. Figure 5-13 shows a computer group named Melbourne Infrastructure.

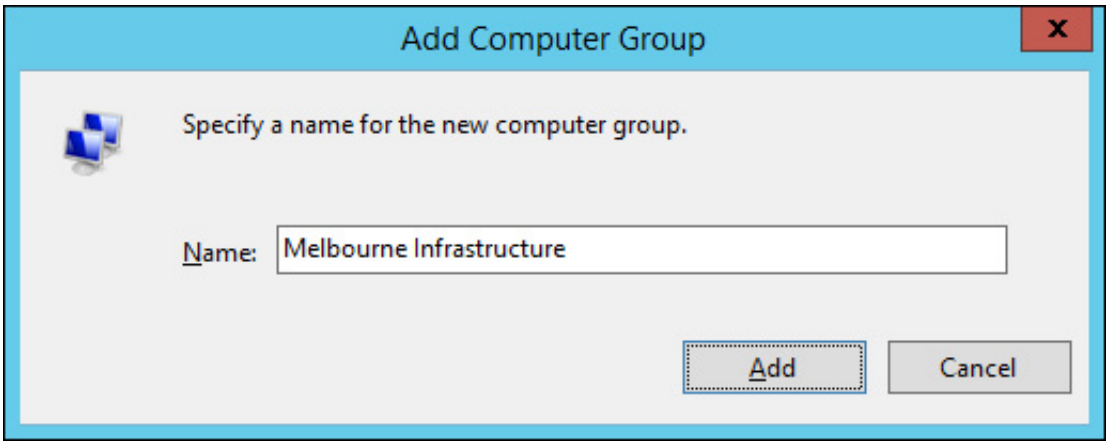

FIGURE 5-13 Add Computer Group

Once you've created the group, you can manually assign computers that have contacted the WSUS server to the group by moving them from the Unassigned Computers group. Computers assigned to groups through Active Directory will automatically be added to the appropriate group.

Group Policy settings

In domain environments, you use Group Policy to configure computers with the address of the WSUS server, as well as other configuration settings. Windows update related group policies are located in both the Computer Configuration and User Configuration nodes. Figure 5-14 shows Windows update related group policies.

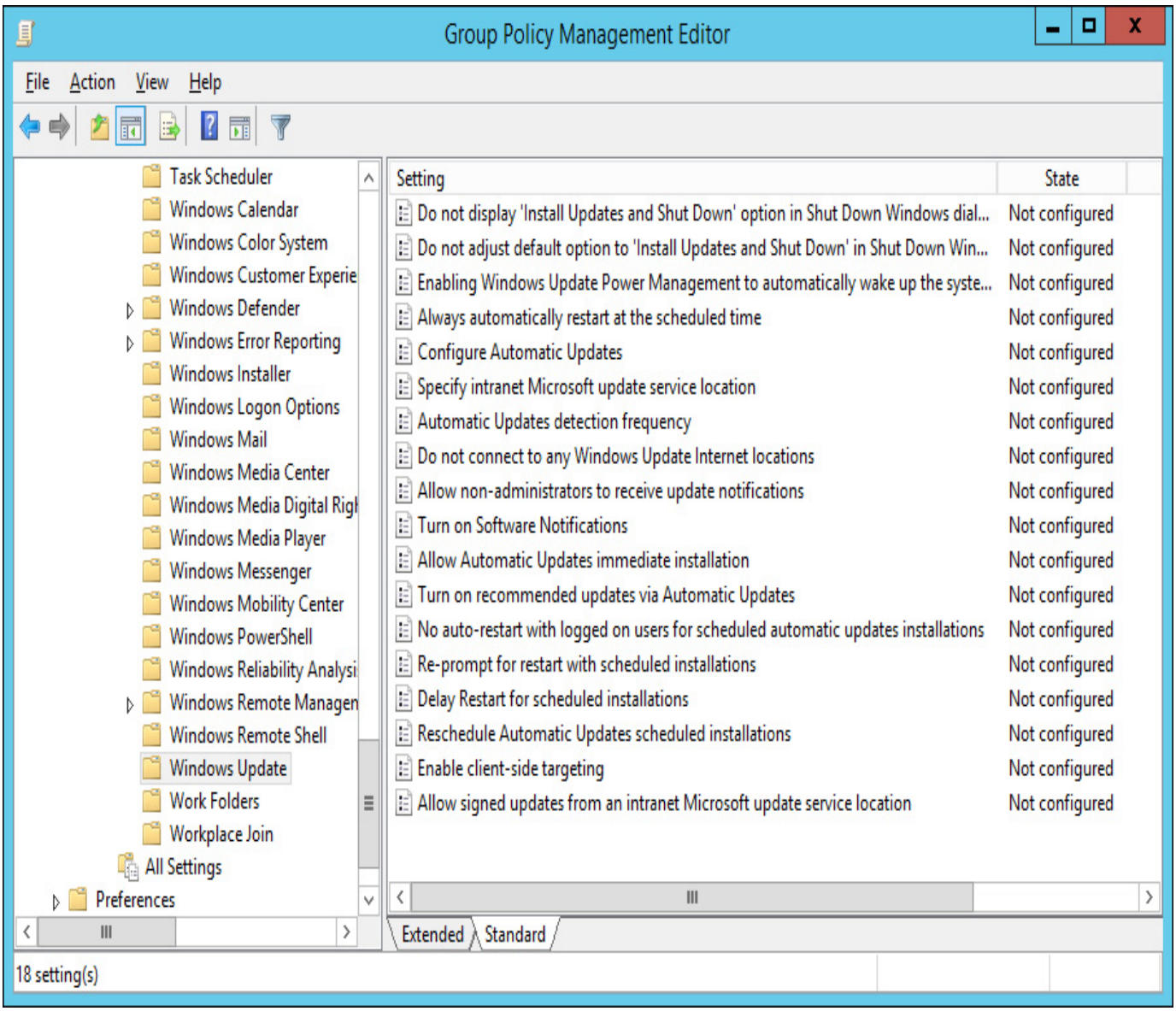

FIGURE 5-14 Windows update policies

More Info: **WSUS Group Policy Settings**

You can learn more about WSUS related Group Policy settings at *http://technet.microsoft.com/en-us/library/dn595129.aspx*.

You use the Specify Intranet Microsoft Update Service Location policy to configure a computer with the address of the WSUS server. Figure 5-15 shows this policy configured so that the computer subject to this policy will use the update server at *http://mel-wsus.tailspintoys.internal* on port 8530, which is the default port used by WSUS on Windows Server 2012 and Windows Server 2012 R2.

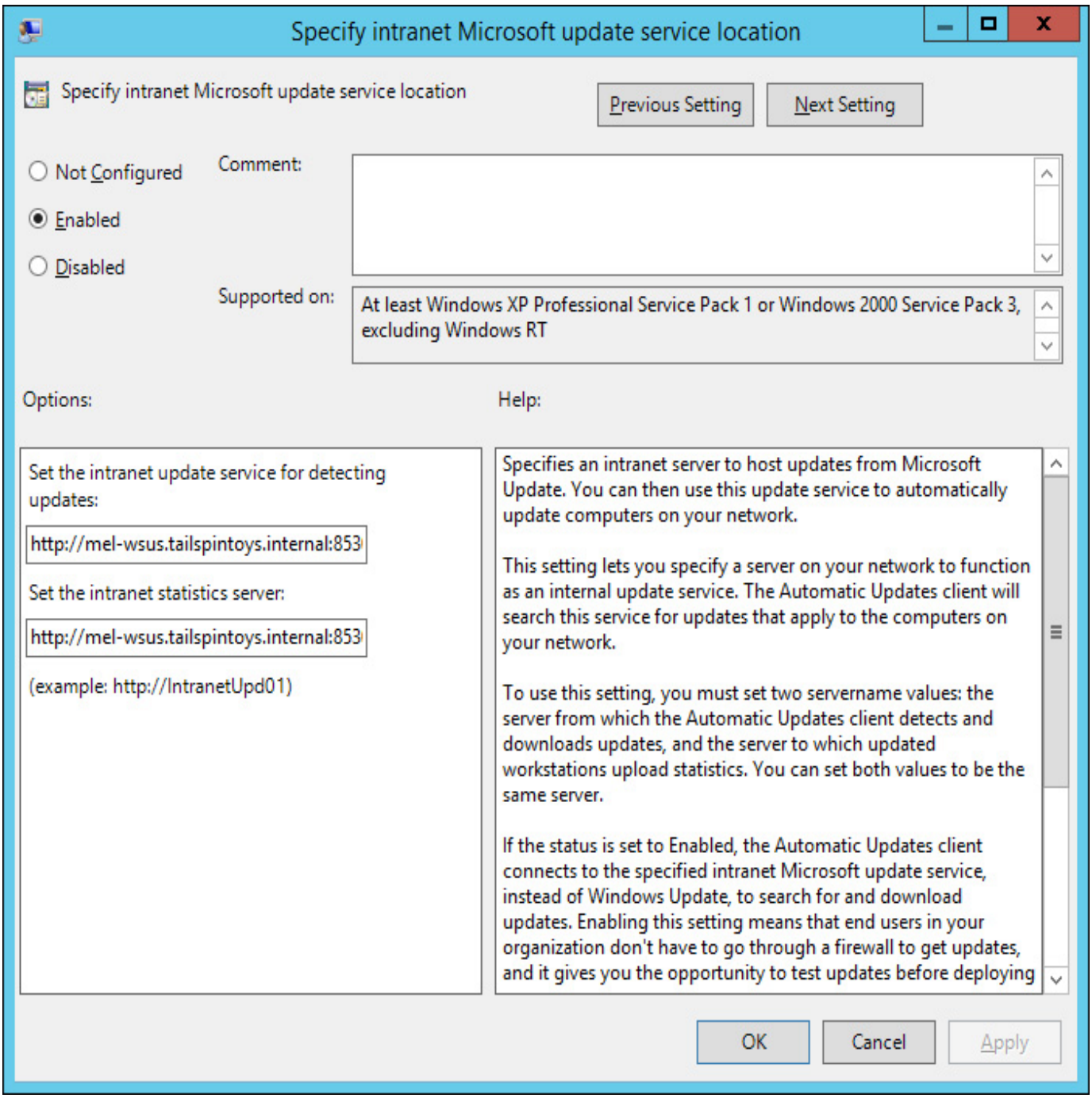

FIGURE 5-15 Local WSUS server

You assign computers to WSUS computer groups using the Enable client-Side Targeting policy. Figure 5-16 shows this policy configured for membership of the Melbourne Infrastructure WSUS computer group.

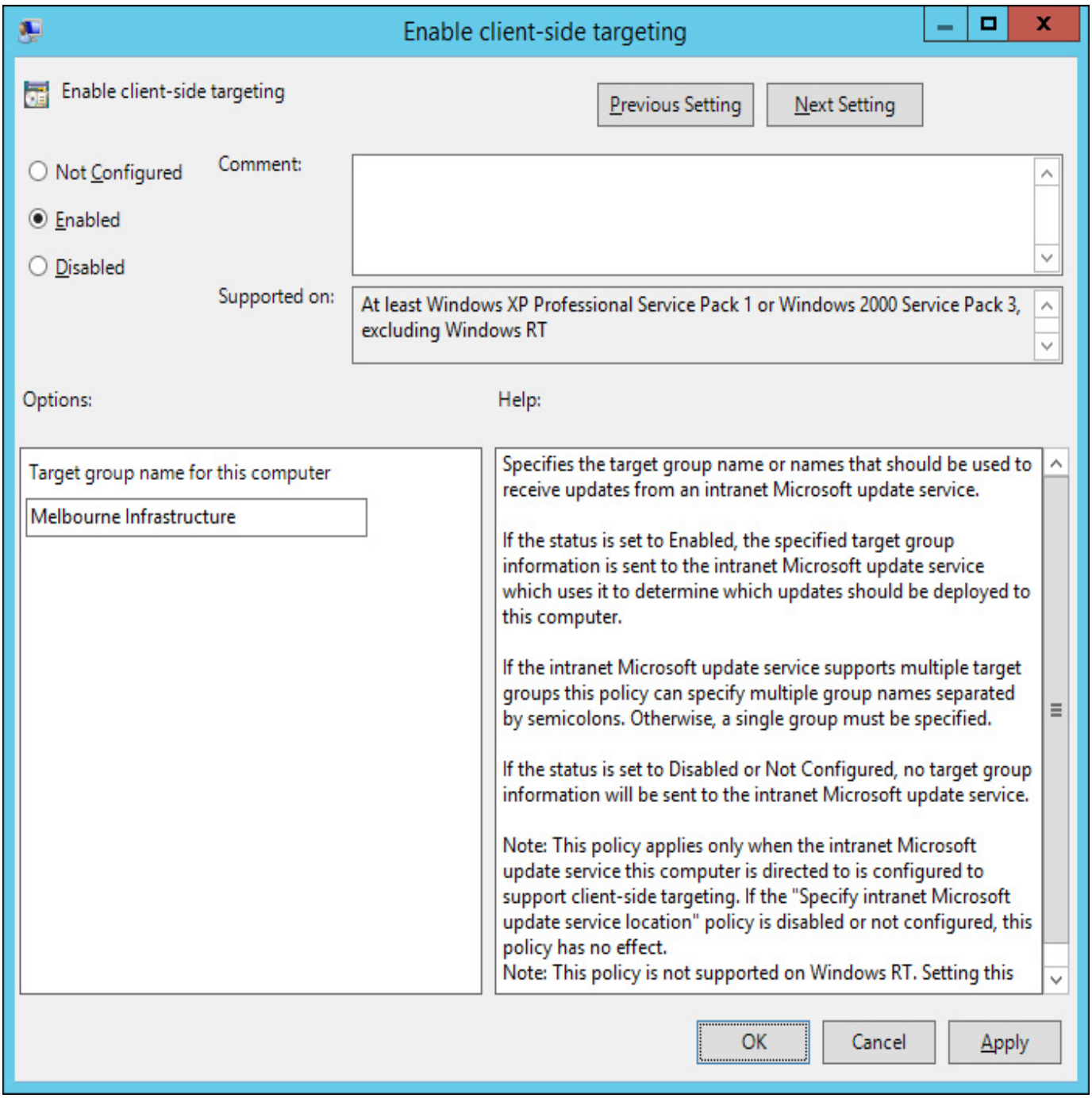

FIGURE 5-16 Client-side targeting

Approving updates

You can choose to manually approve WSUS updates, or configure auto-approval rules. You approve updates on a per-computer group basis. When you approve an update, you can have that update apply to the computer group and any computer groups that are nested members of that computer group. You can also choose to apply an update to a computer group, and exclude any computer groups that are nested members of that group.

To manually approve an update, perform the following steps:

1. In the Updates node of the WSUS console, locate the update that you want to approve for distribution, as shown in Figure 5-17.

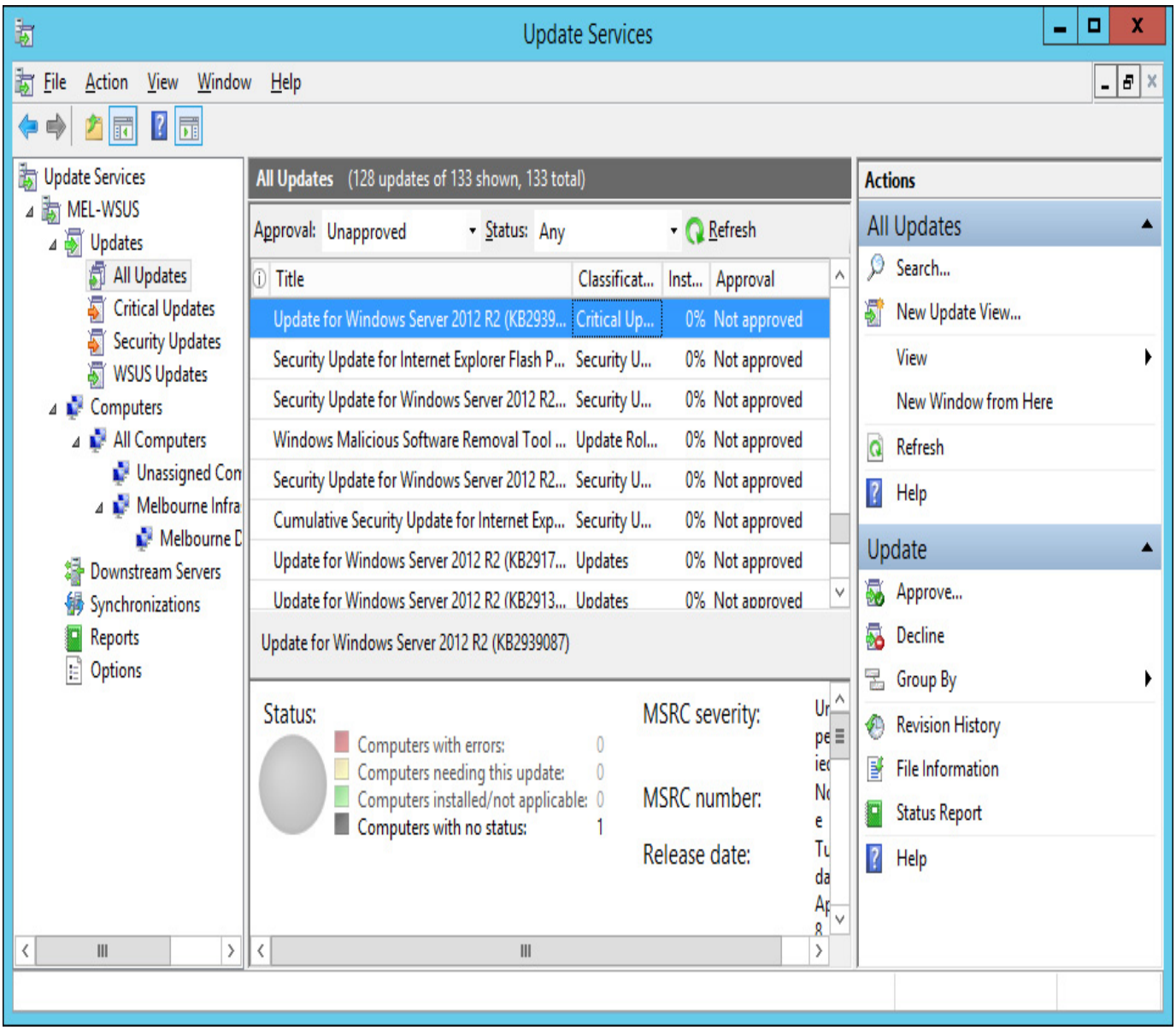

FIGURE 5-17 Update Services

2. On the Actions pane, click Approve.
3. On the Approve Updates dialog box, select the computer groups for which the update is approved. Figure 5-18 shows an update that is approved for the Melbourne Infrastructure group, but not approved for the Melbourne DHCP Servers group.

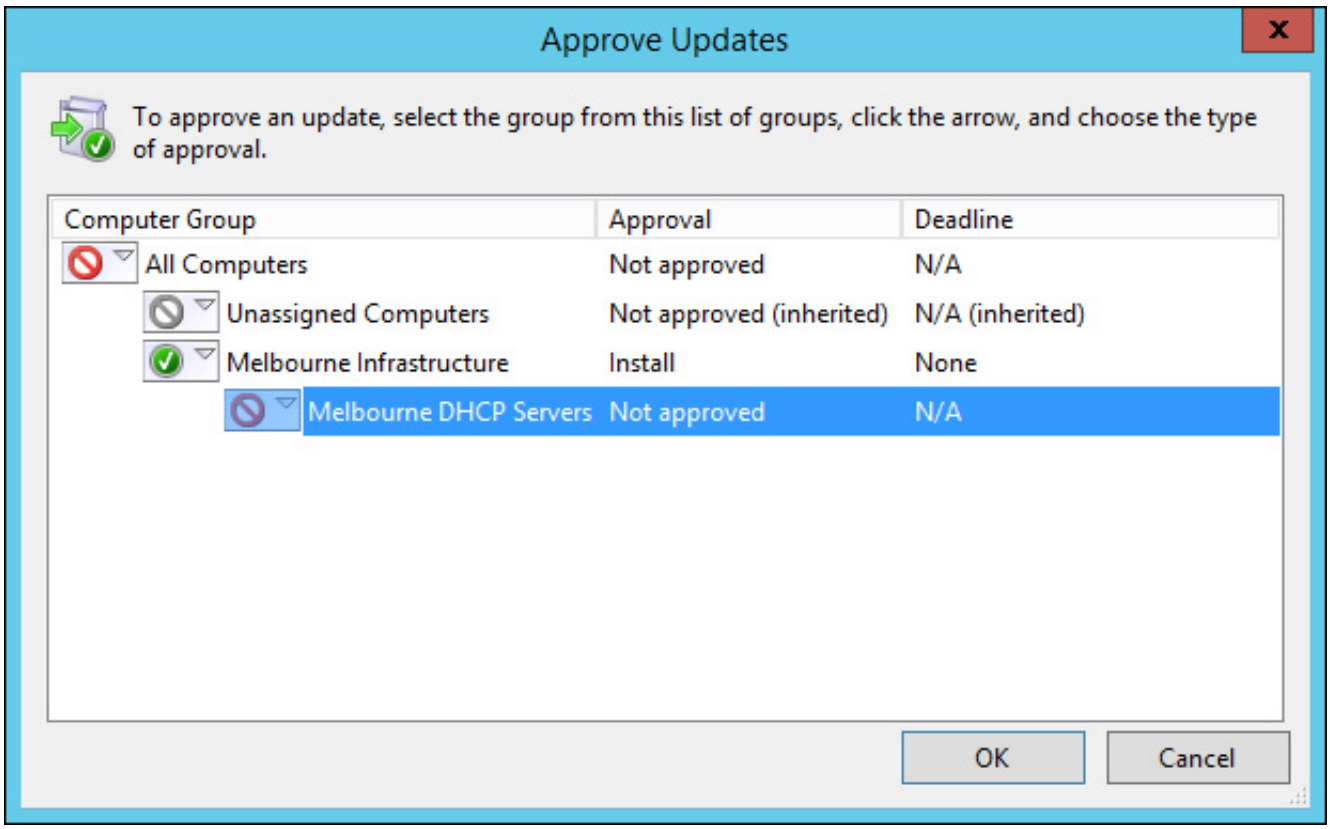

FIGURE 5-18 Approve Updates

Rather than manually approve updates, you can configure automatic approval rules so that new updates are automatically approved based on their properties. A default automatic approval rule, which is not enabled, will automatically approve critical and security updates to all computers that report to the WSUS server. To configure an automatic approval rule, perform the following steps:

1. In the Options node of the WSUS console, click Automatic Approvals.
2. On the Automatic Approvals dialog box, shown in Figure 5-19, click New Rule.

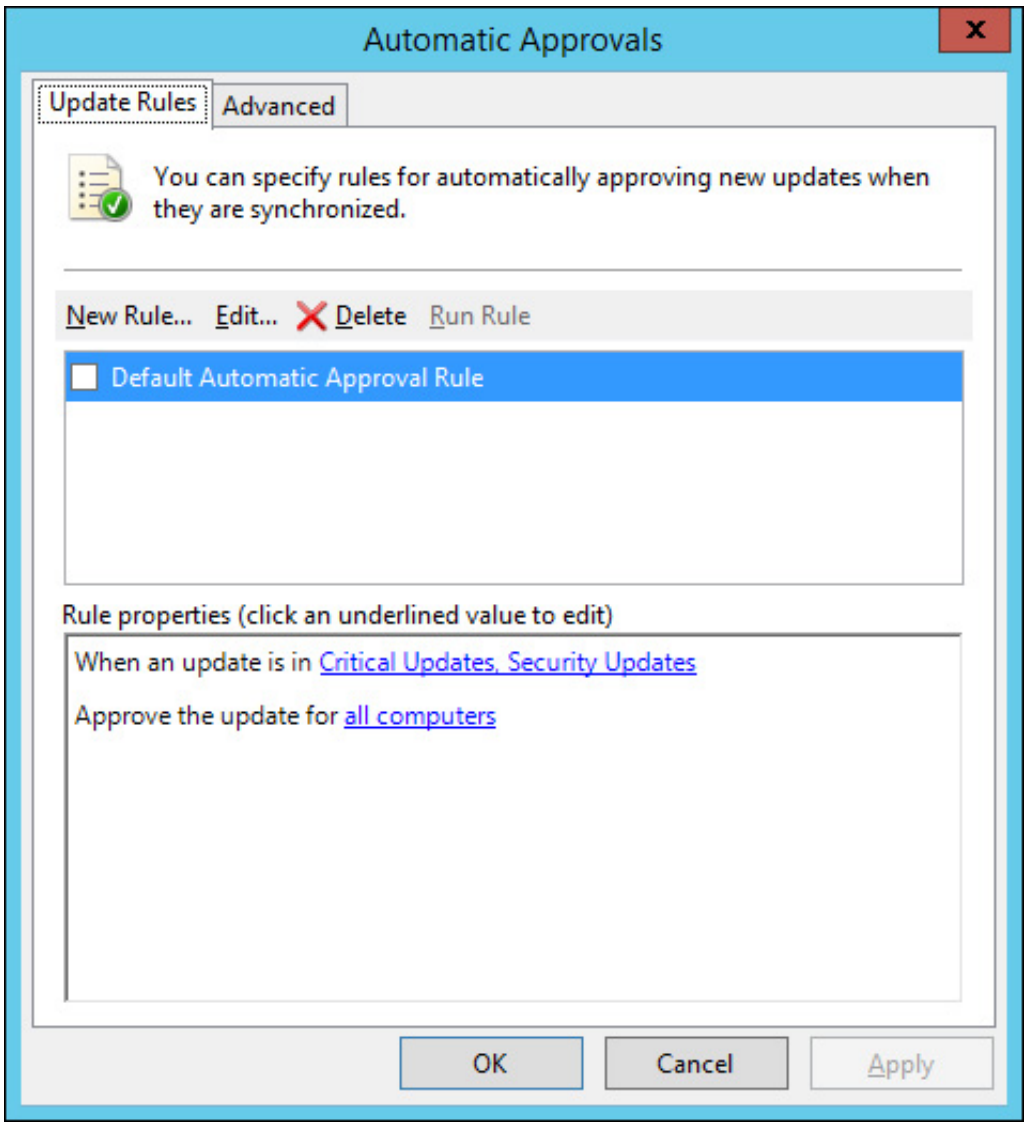

FIGURE 5-19 Automatic Approvals

3. On the Add Rule dialog box, select from the following options:
   - Update Classification
   - Update Product
   - Approval Deadline
   - Computer Groups
4. Figure 5-20 shows a rule that will automatically approve critical updates, security updates, update rollups, and updates for Windows Server 2012 R2 if a computer is a member of the Melbourne Infrastructure group, with an installation deadline of 7 days after the approval.

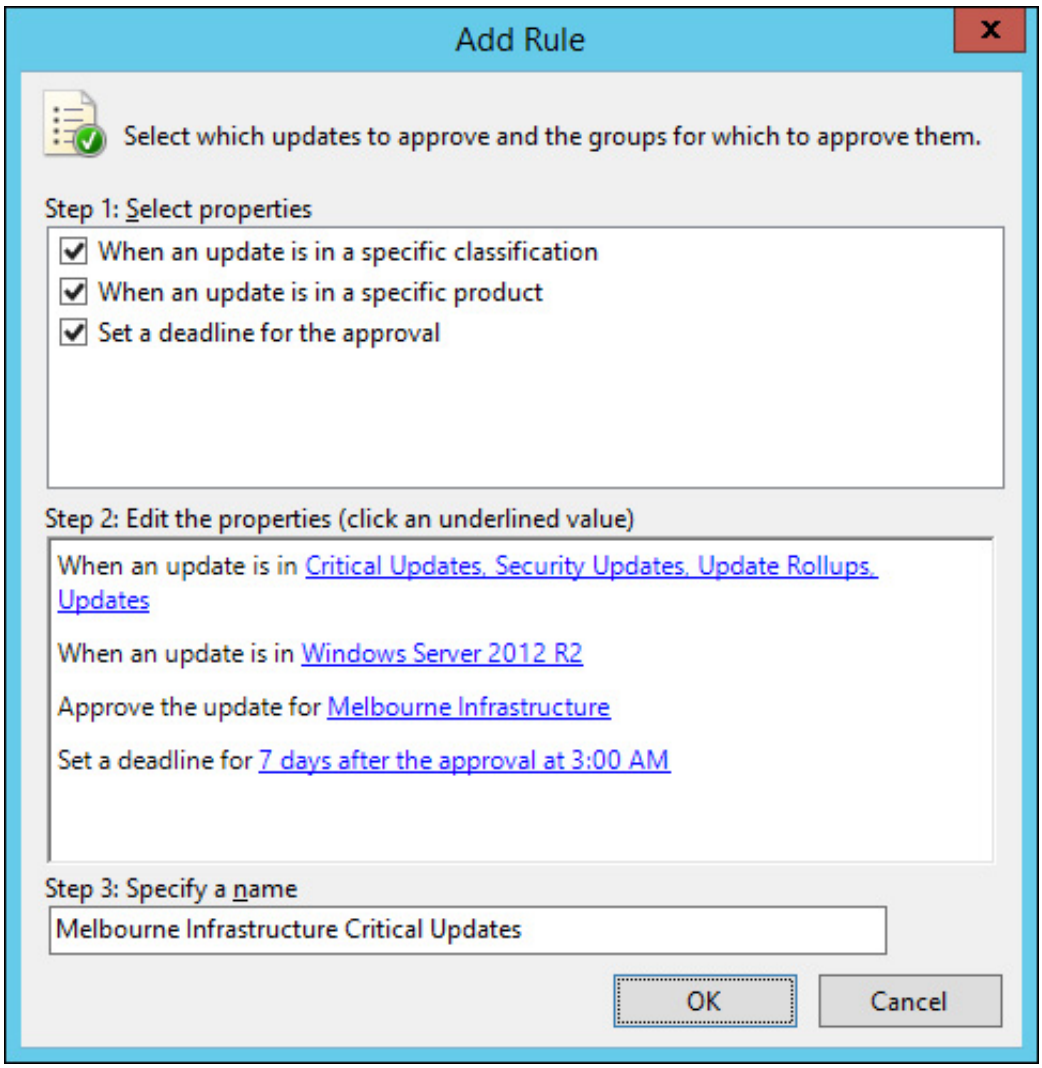

FIGURE 5-20 Add Rule

More Info: **Deploy WSUS Updates**

You can learn more about deploying updates at *http://technet.microsoft.com/en-us/library/hh852348.aspx*.

Verifying update deployment

You can verify update deployment and computer compliance either by viewing the properties of individual computers, or by viewing information on a per-update basis. Figure 5-21 shows that computer Mel-demoserver requires 59 updates and has 69 updates either installed or not applicable. It is important to note that the WSUS server doesn't scan a computer to determine what updates are installed. Instead, the client computer contacts the WSUS server and provides information about which updates have been installed. The WSUS server then uses this information to determine which updates need to be installed given the current configuration of the WSUS client.

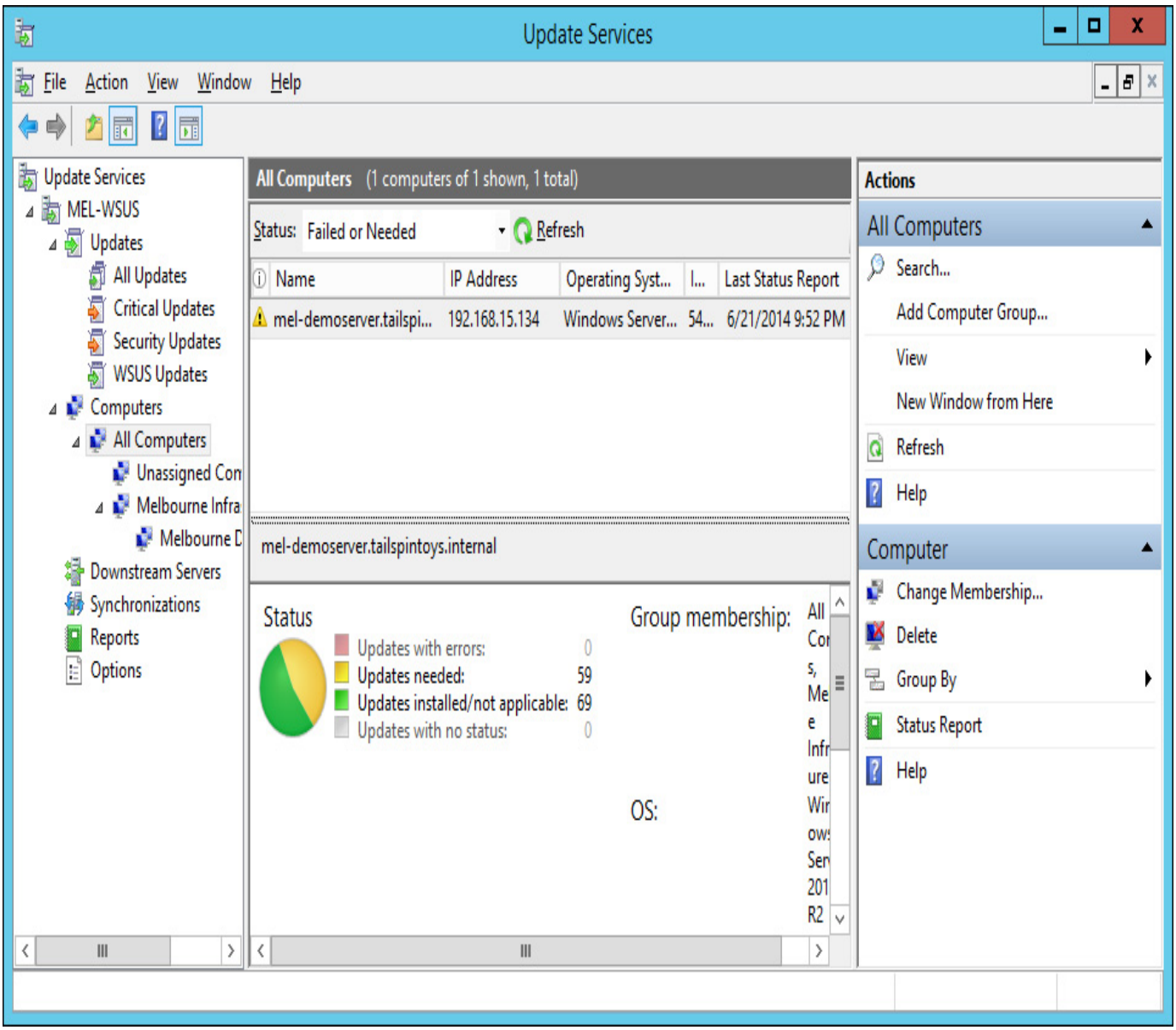

FIGURE 5-21 Update status

The WSUS server also provides the following reports, shown in Figure 5-22, that you can use to determine the update status of computers that report to the WSUS server:

- Update Status Summary
- Update Detailed Status
- Update Tabular Status
- Update Tabular Status For Approved Updates
- Computer Status Summary
- Computer Detailed Status
- Computer Tabular Status
- Computer Tabular Status For Approved Updates
- Synchronization Results

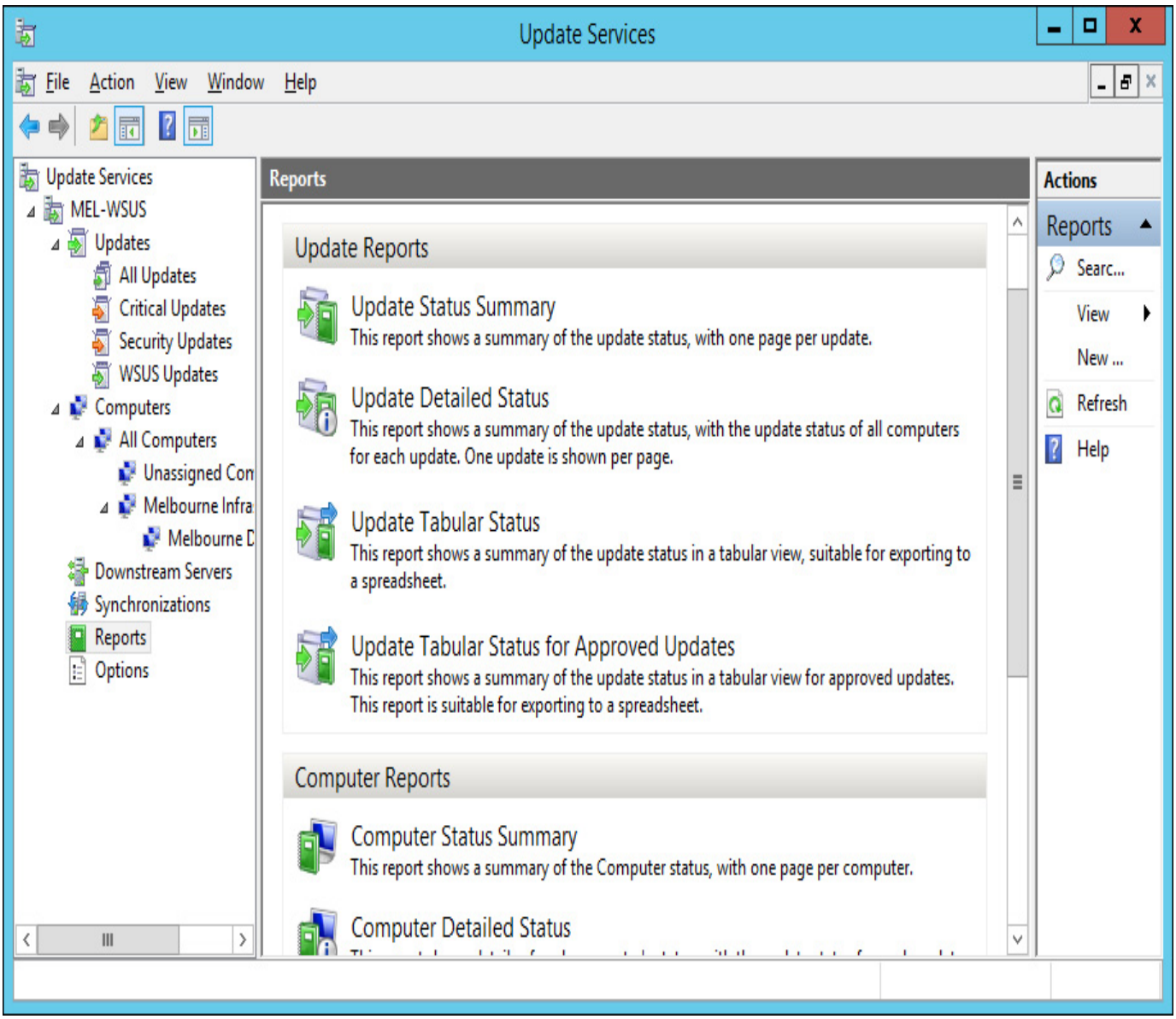

FIGURE 5-22 Report

Managing updates with Configuration Manager

WSUS provides basic update management functionality, but does not provide advanced functionality such as maintenance windows, configuration baselines, support for Network Access Protection, and support for Wake On LAN. You can integrate WSUS with System Center 2012 R2 Configuration Manager to provide advanced software update management functionality for computers in your private cloud environment. When you integrate WSUS with Configuration Manager, you perform update management tasks using the Configuration Manager console.

Integrating WSUS with Configuration Manager

Integrating WSUS with Configuration Manager involves installing and configuring a software update point and synchronizing the software update point's metadata with Configuration Manager. To deploy a software update point when WSUS has been deployed and configured on another computer, perform the following steps:

1. In the Administration workspace of the Configuration Manager console, select Servers And Site System Roles under the Site Configuration node.
2. On the Home tab of the ribbon, click Create Site System Server.
3. On the General page of the Create Site System Server Wizard, specify the name of the server that hosts WSUS, the site code, and the account used for deploying the site system. Figure 5-23 shows the server CBR-WSUS.tailspintoys.internal being configured for this role.

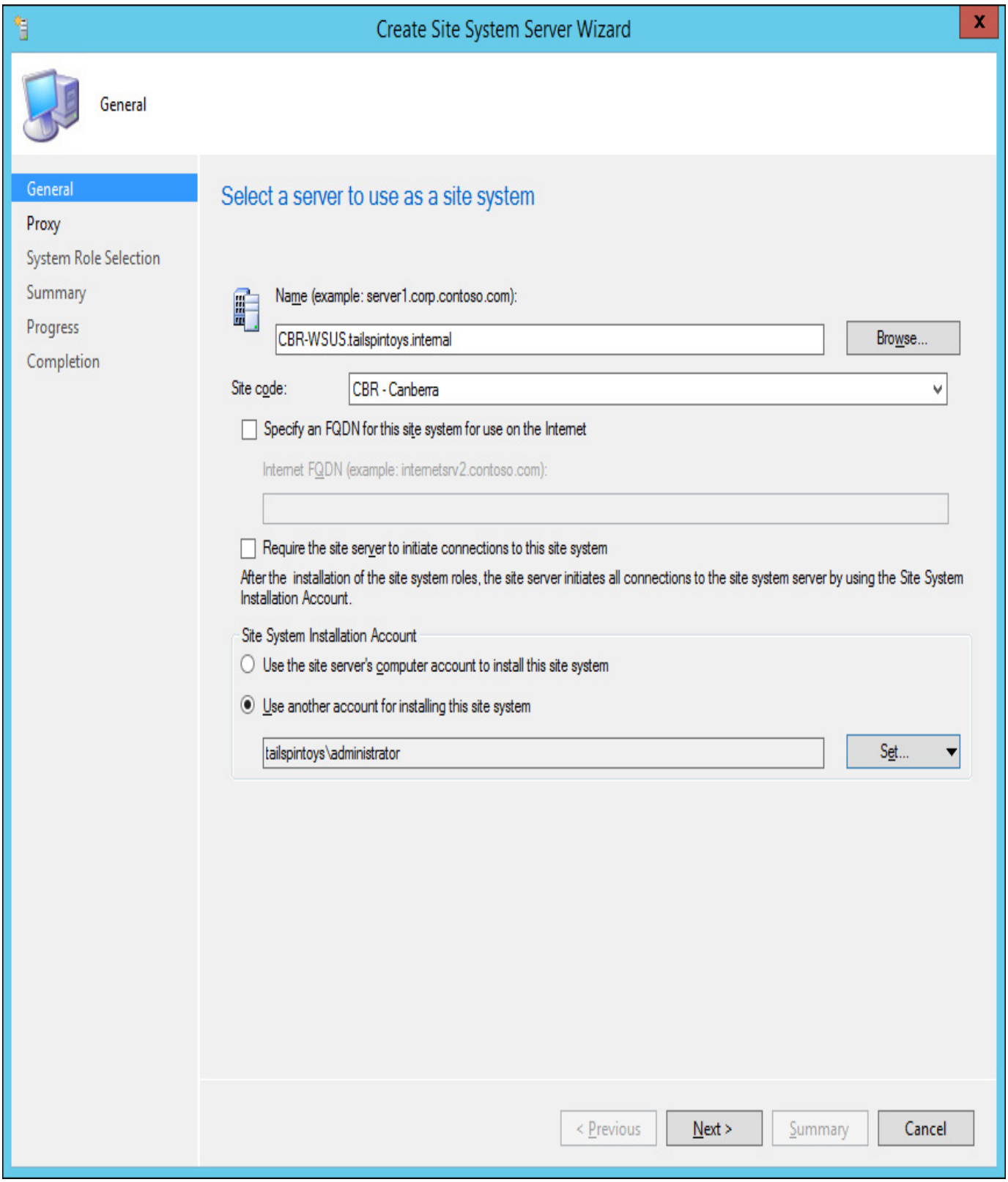

FIGURE 5-23 Create Site System Server Wizard

4. On the Proxy Server page, you can specify the details of any proxy server required to allow the computer that hosts the site server role the ability to connect to hosts on the Internet.
5. On the System Role Selection page, select Software Update Point, as shown in Figure 5-24.

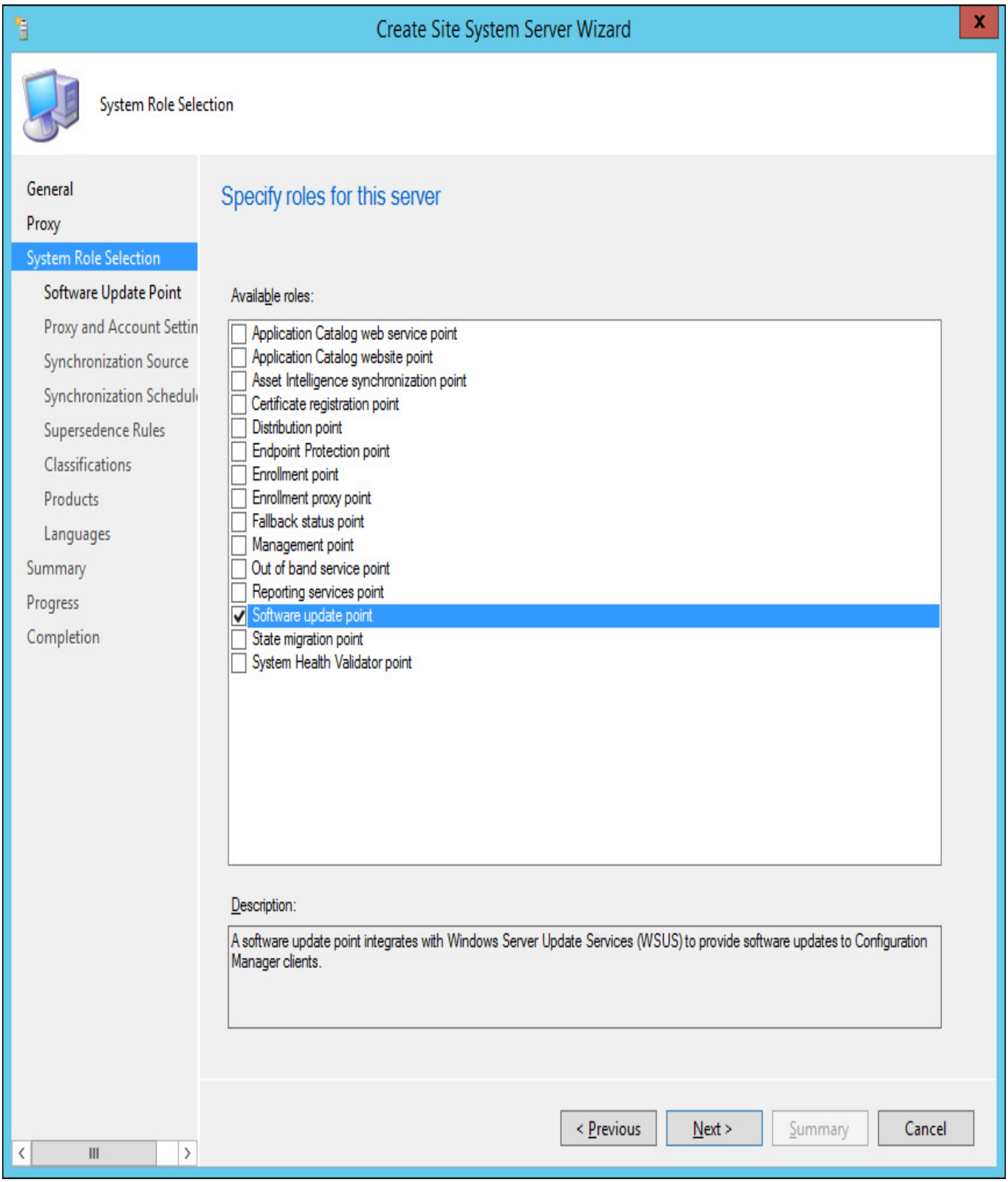

FIGURE 5-24 Software update point

6. On the Software Update Point page, specify whether WSUS will use port 80 and 443, or port 8530 and 8531. Ports 80 and 443 are the default for WSUS 3.0 SP2. Ports 8530 and 8531 are the default for WSUS on Windows Server 2012 and Windows Server 2012 R2. You can also specify whether connections will be limited to Internet, intranet, or both intranet and Internet clients. Figure 5-25 shows this page of the wizard.

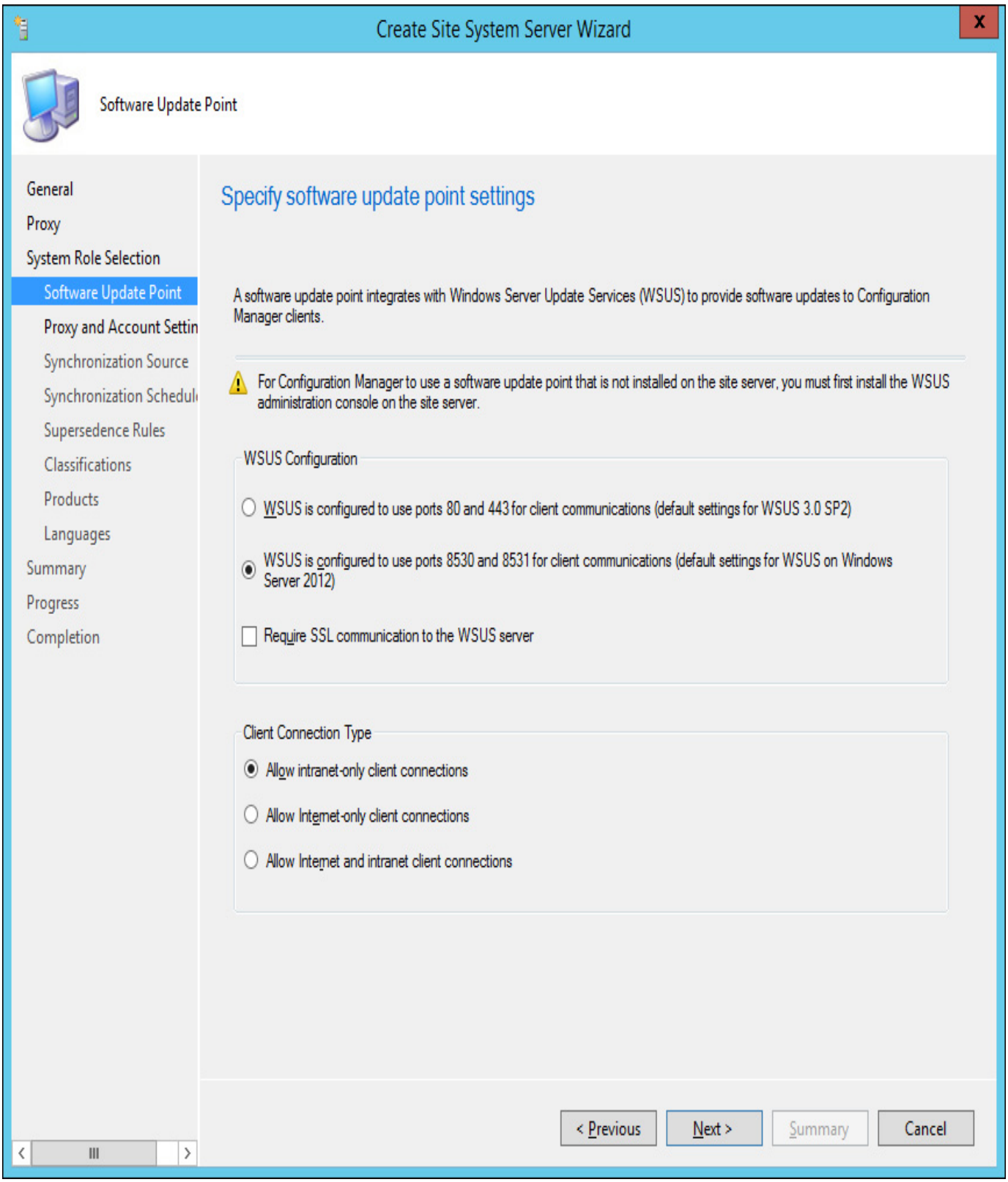

FIGURE 5-25 Software Update Point settings

7. On the Proxy And Account Settings page, specify the account that will be used to connect from the Configuration Manager site server to the WSUS server.
8. On the Synchronization Source page, specify whether the WSUS server will synchronize updates from Microsoft update, or from another WSUS server. You can also use this page to specify whether WSUS will continue to generate reports. If you are using Configuration Manager's more sophisticated reporting functionality, you do not need to enable WSUS reporting. Figure 5-26 shows the Synchronization Source set to Microsoft Update.

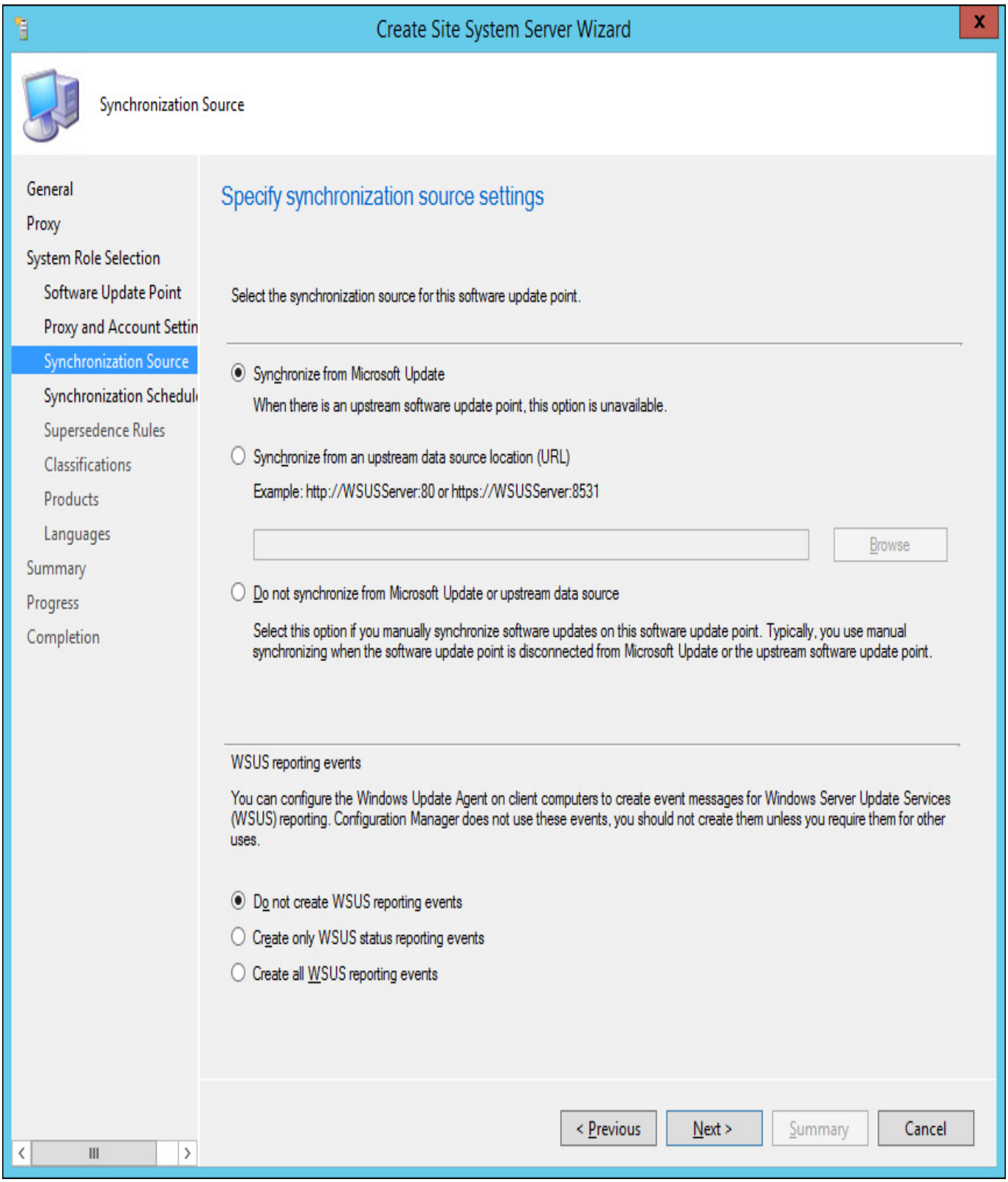

FIGURE 5-26 Synchronization Source

9. On the Synchronization Schedule page, specify how often synchronization should occur. You can also perform synchronization manually.
10. On the Supersedence Behavior page, specify how to treat superseded updates. You can configure superseded updates to expire immediately, or after a specific number of months.
11. On the Classifications page, shown in Figure 5-27, specify which updates Configuration Manager will use the WSUS server to obtain.

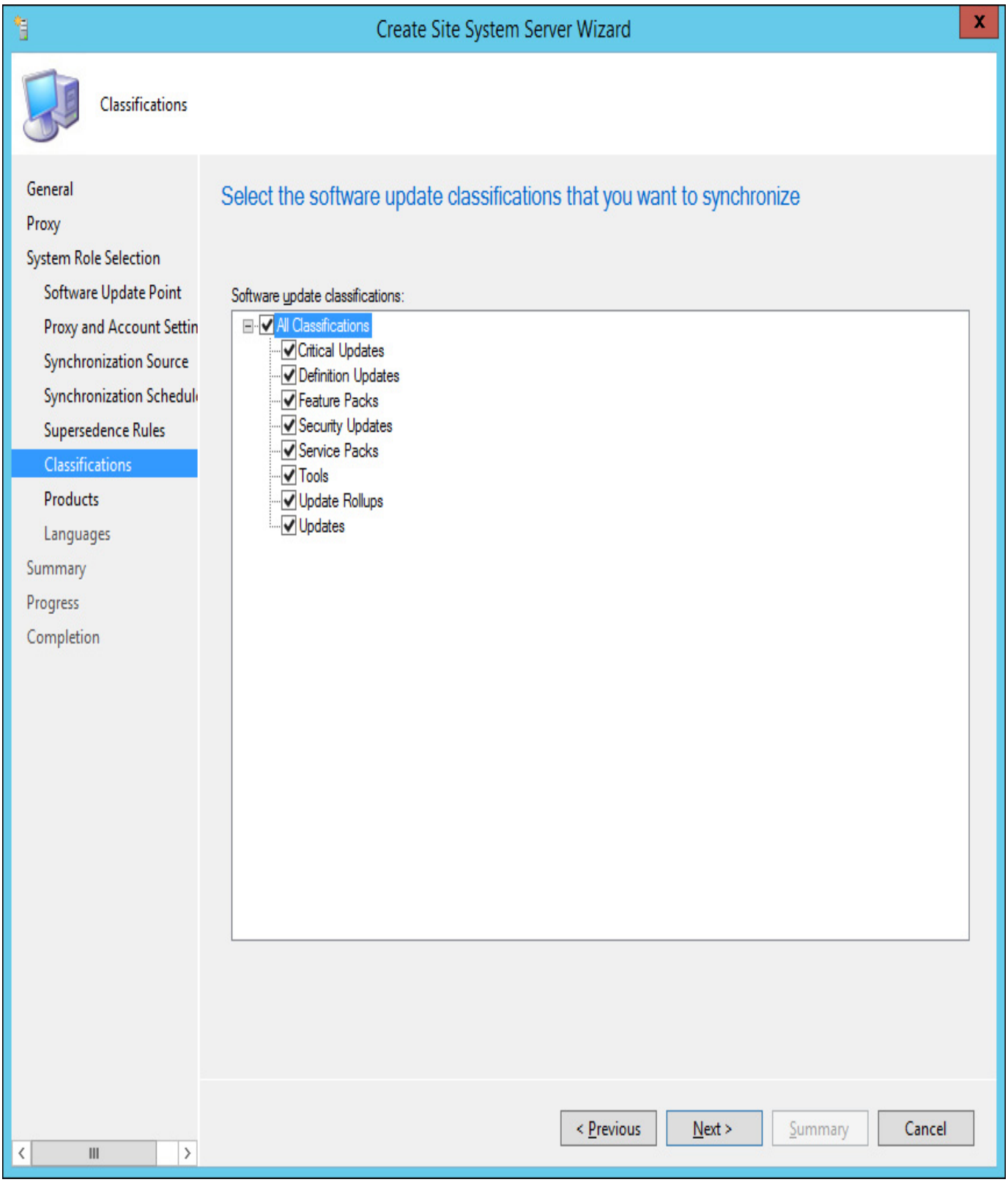

FIGURE 5-27 Update classifications

12. On the Products page, specify which product you wish to provide updates for.
13. On the Languages page, specify the product language versions that you want to support, and then complete the wizard.

Once you have configured the Software Update point, you can trigger a manual synchronization by performing the following steps:

1. In the Software Library workspace of the Configuration Manager console, click All Software Updates under Software Updates.
2. On the ribbon, click Synchronize Software Updates. You can view the status of the synchronization by checking the SMS_WSUS_SYNC_MANAGER segment in the Component Status node of the Monitoring workspace.

Software update groups

Software update groups allow you to collect together updates. You can add software updates to software update groups manually, or automatically configure new software updates to be added to a software update group through an automatic deployment rule. You can deploy software update groups to Configuration Manager collections. Configuration Manager collections are groups of configuration manager clients or users, though you can only deploy software updates to client collections. You can deploy software update groups to collections either manually, or automatically through an automatic deployment rule. When you deploy a software update group to a collection, any new updates that you add to the group are automatically deployed to the collection.

To add software updates to a new software update group, perform the following steps:

1. In the Software Library workspace of the Configuration Manager console, click All Software Updates under Software Updates.
2. Select the updates that you want to add to the new software update group, and then click Create Software Update Group on the ribbon.
3. Provide a meaningful name for the update group, and then click Create. Figure 5-28 shows the Create Software Update Group dialog box.

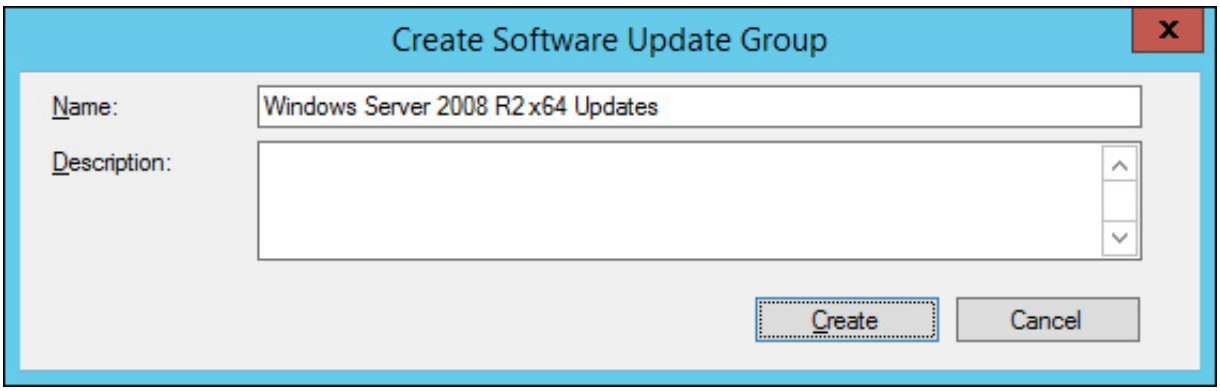

FIGURE 5-28 Update group

Once you have created the update group, you need to download the updates themselves, so that you can deploy them to clients. To download the constituent files of an upgrade group, select the update group, and then click Download. This will launch the Download Software Updates Wizard. To complete this wizard, perform the following steps:

1. On the Deployment Package page of the Download Software Updates Wizard, shown in Figure 5-29, choose either to use an existing deployment package, or to create a new deployment package. If you choose an existing deployment package, any updates that have been previously downloaded will not be downloaded again. If you choose to deploy a new deployment package, you'll need to provide the following information:
   - **Name** A unique name for the deployment package.
   - **Package Source** A unique shared folder location to host the software update source files. You need to create and specify this folder prior to clicking Next.

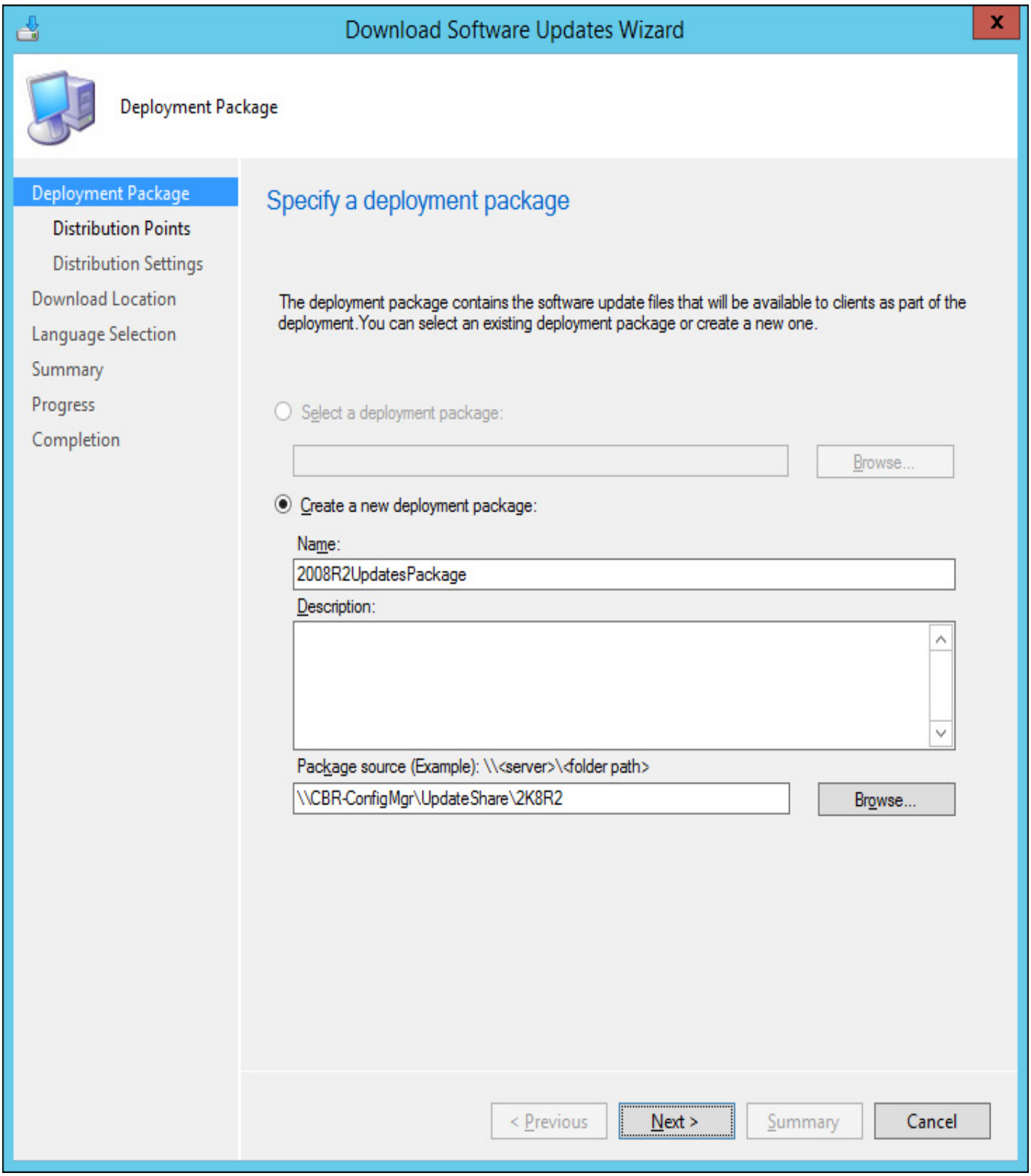

FIGURE 5-29 Deployment Package

2. On the Distribution Point page, choose the Configuration Manager distribution points that will host the software update files.
3. On the Distribution Settings page, shown in Figure 5-30, configure the following settings:
   - **Distribution Priority** This determines the priority when the package is sent to distribution points at child sites. Priority is only used if there is a backlog of packages being sent to distribution points.
   - **Distribute the content for this package to preferred distribution points** If you enable this option, content is automatically distributed to preferred distribution points.
   - **Prestaged distribution point settings** Use this option to specify whether you want content to be automatically downloaded when a deployment package is assigned to a distribution point, whether to only download changed content to a distribution point, or whether you will manually copy content to a distribution point.

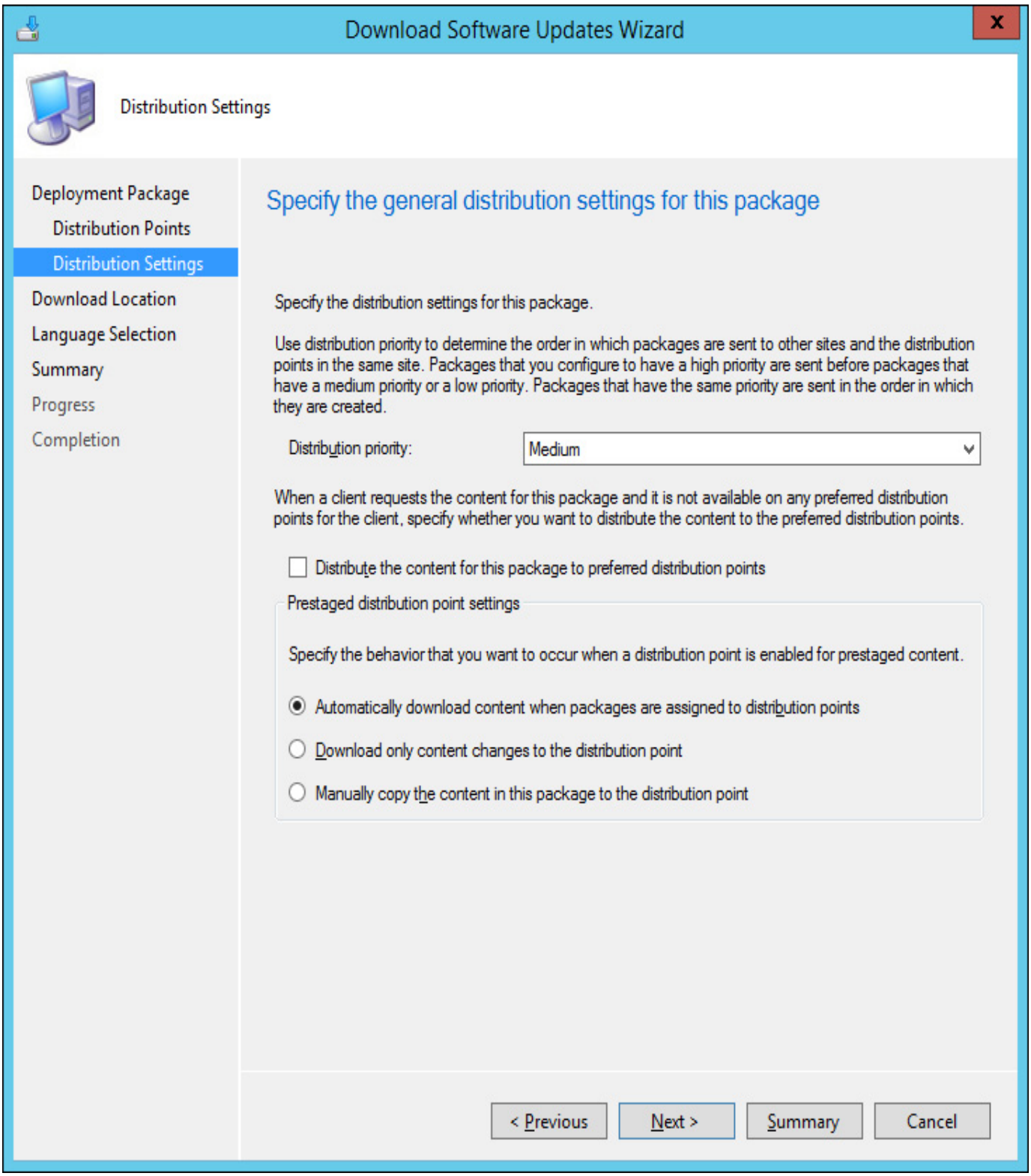

FIGURE 5-30 Distribution Settings

4. On the Download Location page, shown in Figure 5-31, choose how Configuration Manager will obtain software update source files. Choose between having Configuration Manager download software updates from the Internet, or from a location on the local network.

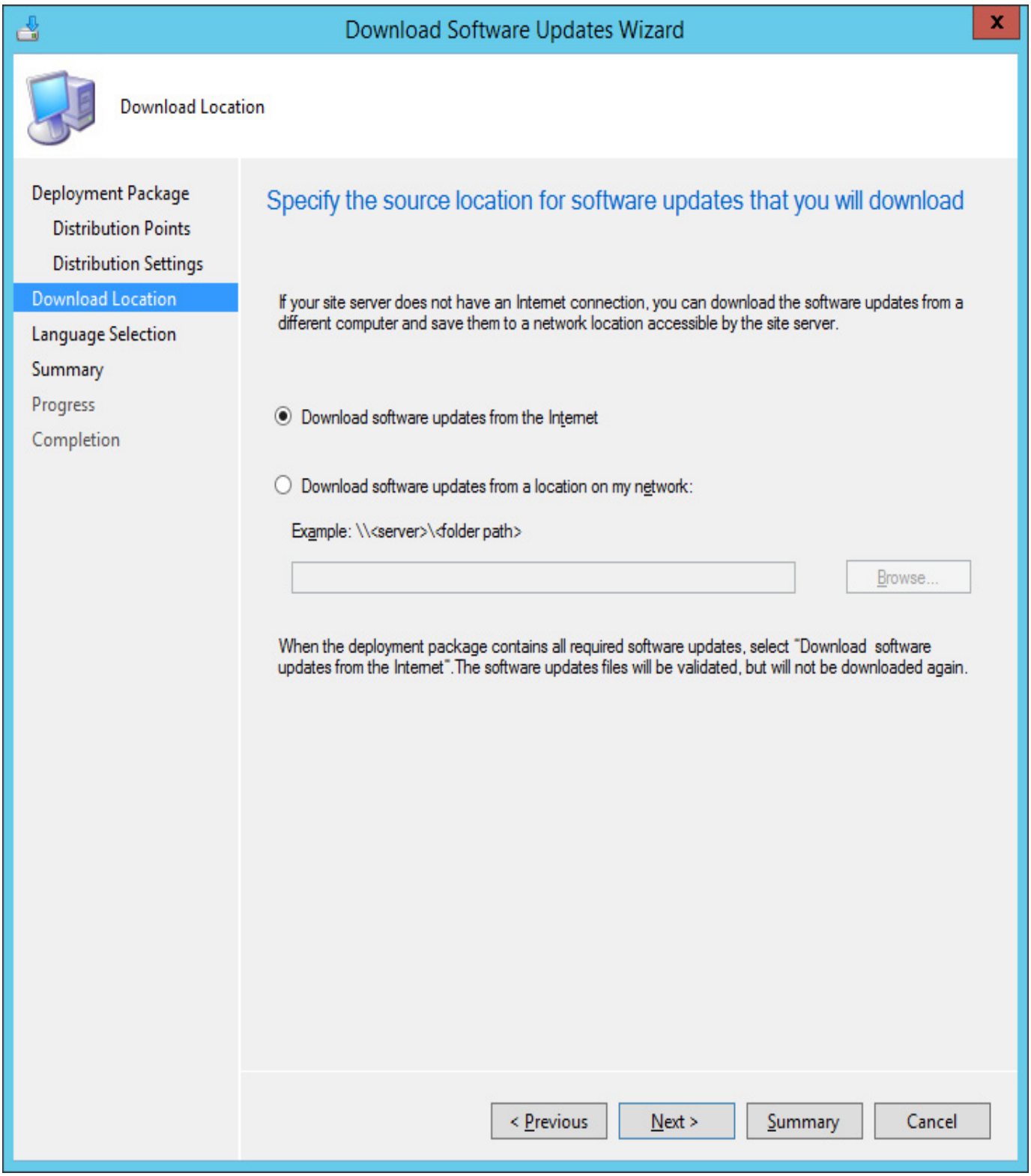

FIGURE 5-31 Download Location

5. Select which language the update files will be downloaded in. Most organizations will only need to download updates for the language version of the software that they use

Deploy software updates

Once software updates have been obtained, you need to deploy them to Configuration Manager clients. The clients that you will deploy the updates to need to be part of a Configuration Manager collection. You can configure maintenance windows on a per-collection basis. Maintenance windows allow you to specify the time of day that operations such as update installation occur.

To deploy a software update group package to a Configuration Manager collection, perform the following steps:

1. In the Software Library workspace of the Configuration Manager console, click Software Update Groups under Software Updates, and then select the software update group that you

want to deploy.

2. On the ribbon, click Deploy. This will launch the Deploy Software Updates Wizard.
3. On the General page of the Deploy Software Updates Wizard, shown in Figure 5-32, provide the following information:

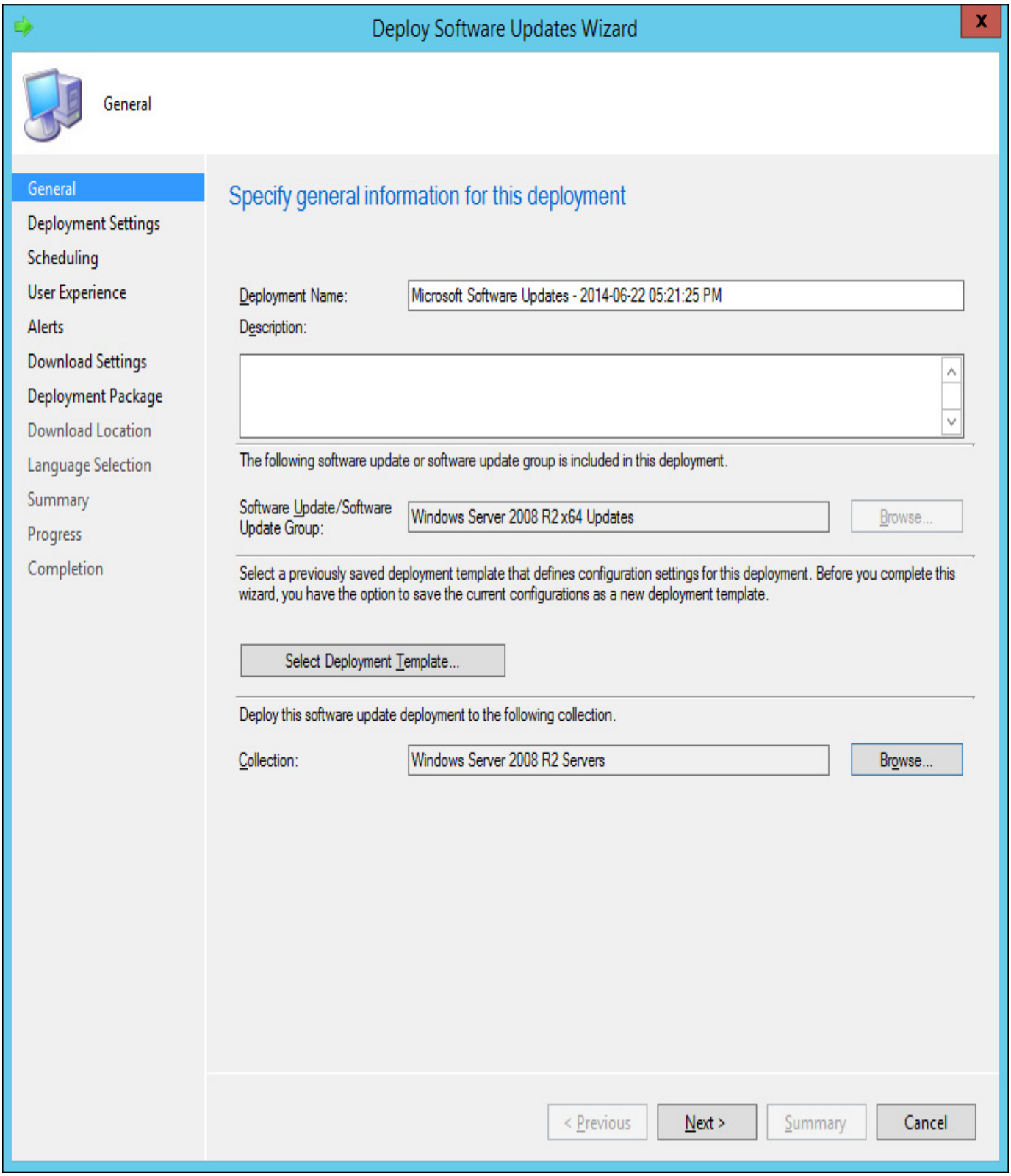

FIGURE 5-32 Deploy Software Updates

- **Name** The name of the deployment.
- **Collection** The collection to which you want to deploy the software update group package.
- **Deployment Template** These templates allow you to save commonly used properties. Rather than configuring similar settings each time you use the wizard, you can instead save those settings as a deployment template, and select that template when you run the wizard.
- **Software Update/Software Update Group** This setting will be pre-populated with the

details of the software update group you are intending to deploy.

4. On the Deployment Settings page, provide the following information:
   - **Type of deployment** Here you select between Required and Available. When you select Required, software updates install automatically on clients before the configured installation deadline.
   - **Use Wake-on-LAN to wake clients for required deployments** If you have configured, and your clients support Wake-on-LAN, special packets will be sent to client computers that are in a low power state to wake them for update installation. This option is only available for the Required deployment type.
   - **Detail level** This configures the level of detail for state messages reported back to Configuration Manager by clients.
5. On the Scheduling page, configure the following information:
   - **Schedule Evaluation** This setting determines whether the deadline time is calculated using UTC, or the computer's local time.
   - **Software Available Time** Use this setting to specify whether the updates will become available at a particular time, or that the client will be aware of them when it next polls the Configuration Manager server.
   - **Installation Deadline** Allows you to specify a deadline for update installation. You can also choose for updates to be installed as soon as possible.
6. On the User Experience page, specify the type of notification users will receive about software update download and installation. You also configure what happens when the deadline is reached, and what happens if the computer requires a restart to complete installation.
7. On the Alerts page, specify how Configuration Manager and Operations Manager will generate alerts related to this deployment. This option is only available if the deployment type is set to Required.
8. On the Download Settings page, shown in Figure 5-33, you configure whether the clients will download the software locally and then install them if connected to a slow network, whether to use BranchCache when obtaining content, and whether to use the Microsoft Update servers to obtain updates if a distribution point is not available.

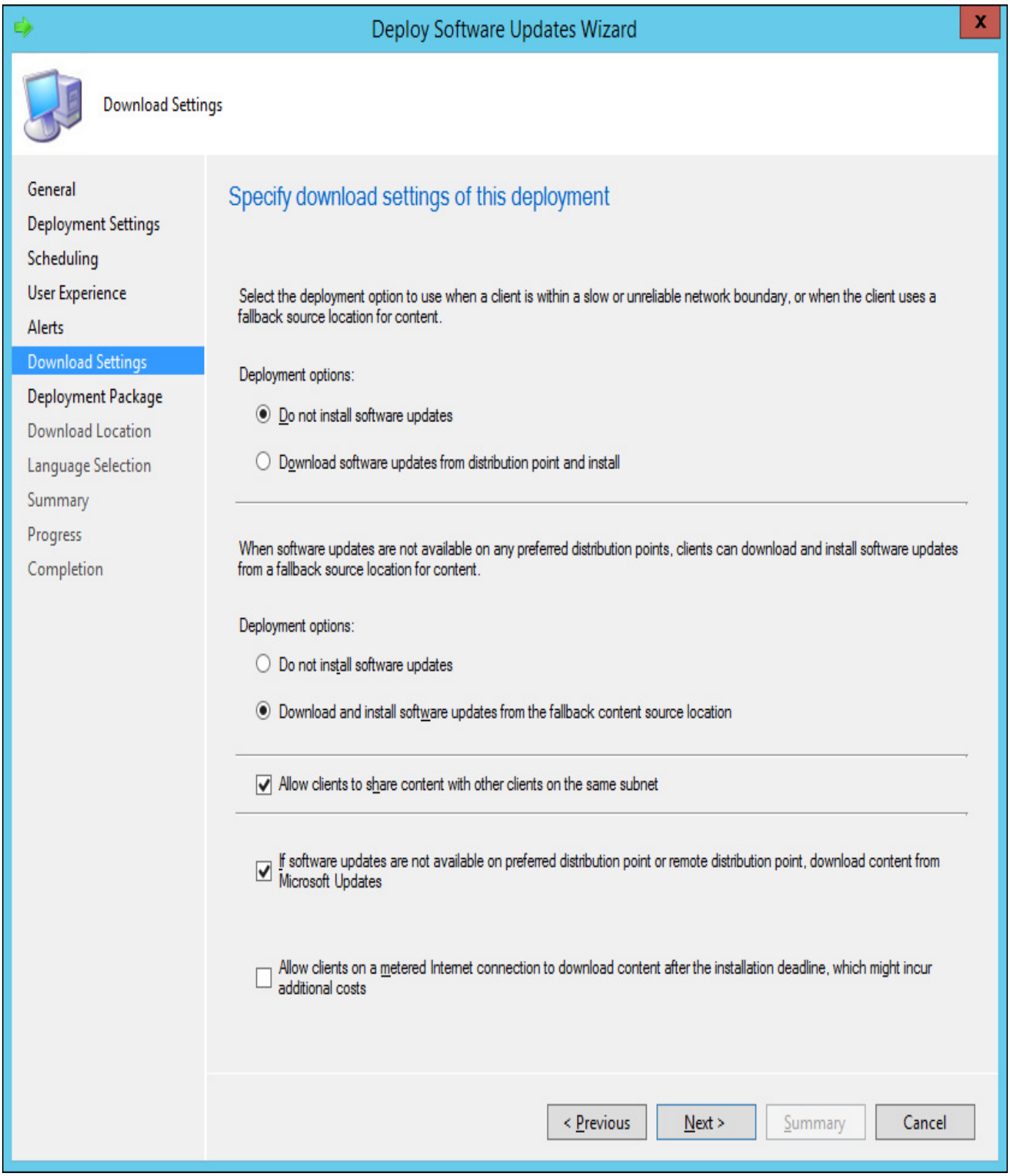

FIGURE 5-33 Download settings

9. On the Deployment Package page, shown in Figure 5-34, select the deployment package that contains the updates you want to deploy.

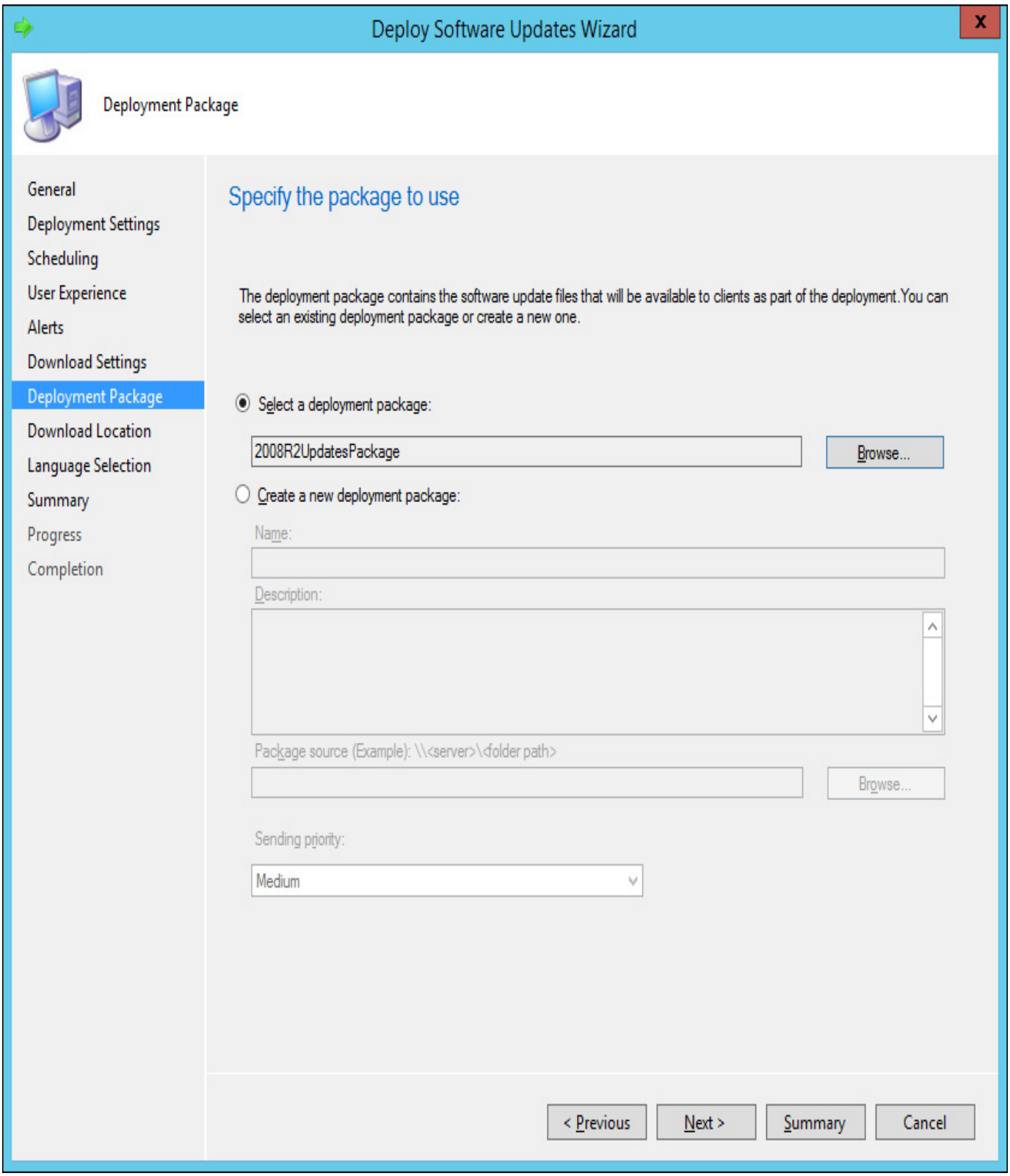

FIGURE 5-34 Select deployment package

10. On the Download Location page, select whether updates will be downloaded from the Internet or over the local network. Download only occurs for updates that are not already present in the deployment package.
11. On the Language selection page, ensure that the product language used in your organization is selected.
12. On the Summary page, you get the chance to save this information as a template, so you don't have to go through the process of configuring all of these deployment settings in the future.

More Info: **Managing Software Updates with Configuration Manager**

You can learn more about managing software updates with Configuration Manager at *http://technet.microsoft.com/en-us/library/gg712304.aspx*.

Integrating WSUS with VMM

You can integrate WSUS with VMM as a way of centrally managing updates for your organization's virtualization servers and VMM infrastructure servers. Integrating WSUS with VMM allows you to:

- Collect updates together in baselines
- Determine update compliance.
- Remediate update compliance.
- Automatically evacuate VMs off of host cluster nodes that require a reboot to install updates.

Configuring WSUS with VMM

While it's possible to deploy the WSUS role on the computer that hosts VMM, Microsoft recommends that WSUS be deployed on a separate computer. You should run the WSUS Configuration Wizard to perform preliminary WSUS configuration, and perform a synchronization prior to integrating with VMM. You can run the WSUS Configuration Wizard and perform a synchronization using the default settings.

To integrate WSUS with VMM, perform the following steps:

1. In the Fabric workspace of the VMM console, click the Update Server Node under Infrastructure, as shown in Figure 5-35.

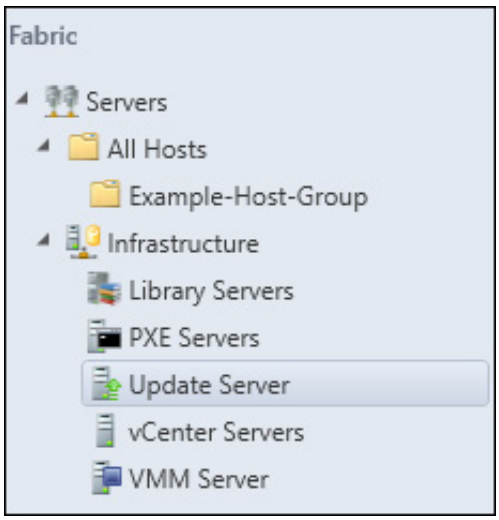

FIGURE 5-35 Update Server

2. On the Ribbon, click Add Resources, and then click Update Server. This will launch the Add Windows Server Update Services Server dialog box.
3. In the Add Windows Server Update Services Server dialog box, provide the following information, as shown in Figure 5-36, and then click Add.
   - **Computer Name** The FQDN of the WSUS server.
   - **TCP Port** The WSUS server's TCP port. By default, this is port 8530 (or port 8531 if using SSL) when you deploy WSUS on computers running Windows Server 2012 or Windows Server 2012 R2.
   - **Credentials** An account with local Administrator privileges on the WSUS server. You can also use a Run As account for this task.

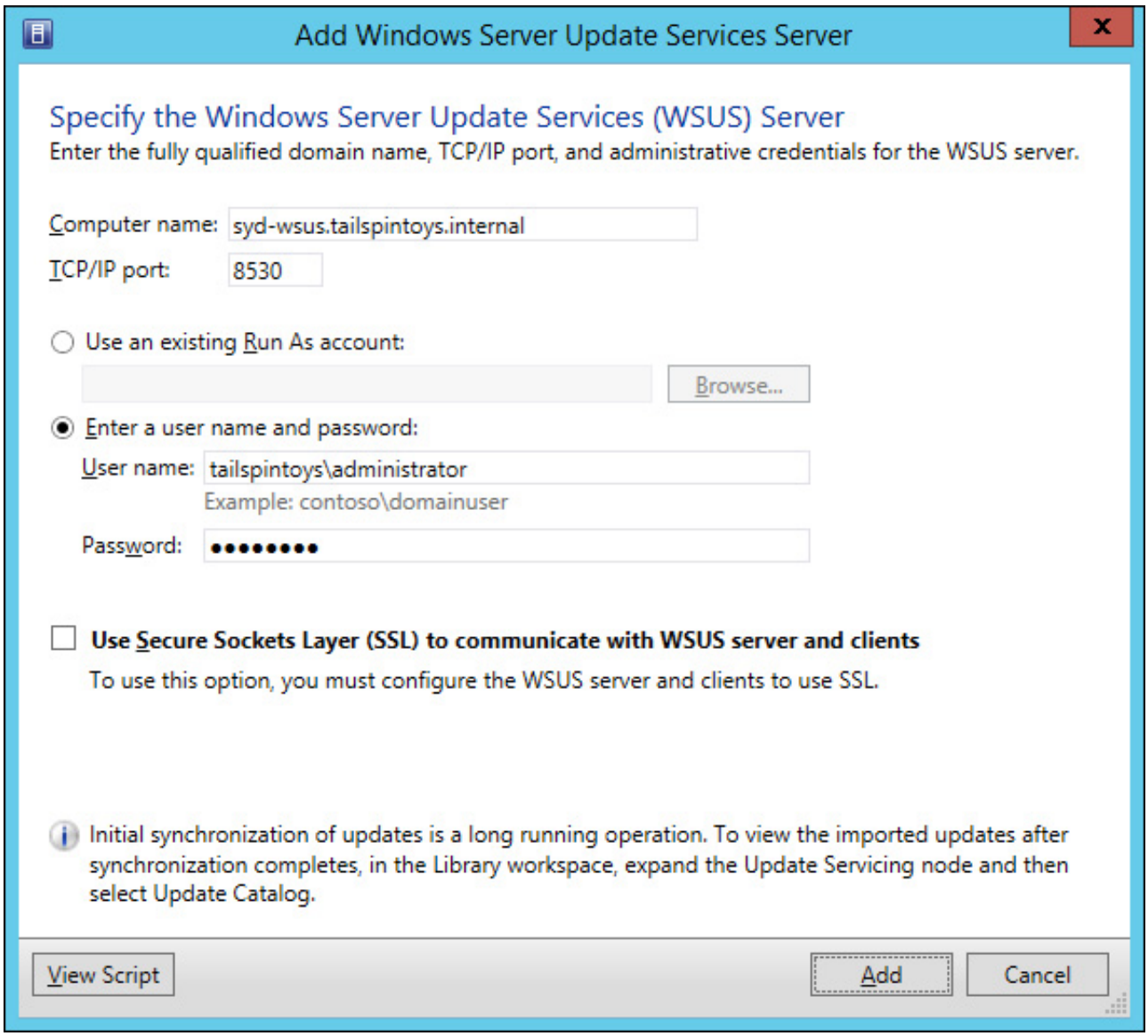

FIGURE 5-36 Add Update Server

4. Once the installation completes, verify that the update server is listed when the Update Server node is selected. The Agent Status is set to Responding, and Synchronization Result is listed as Succeeded, as shown in Figure 5-37.

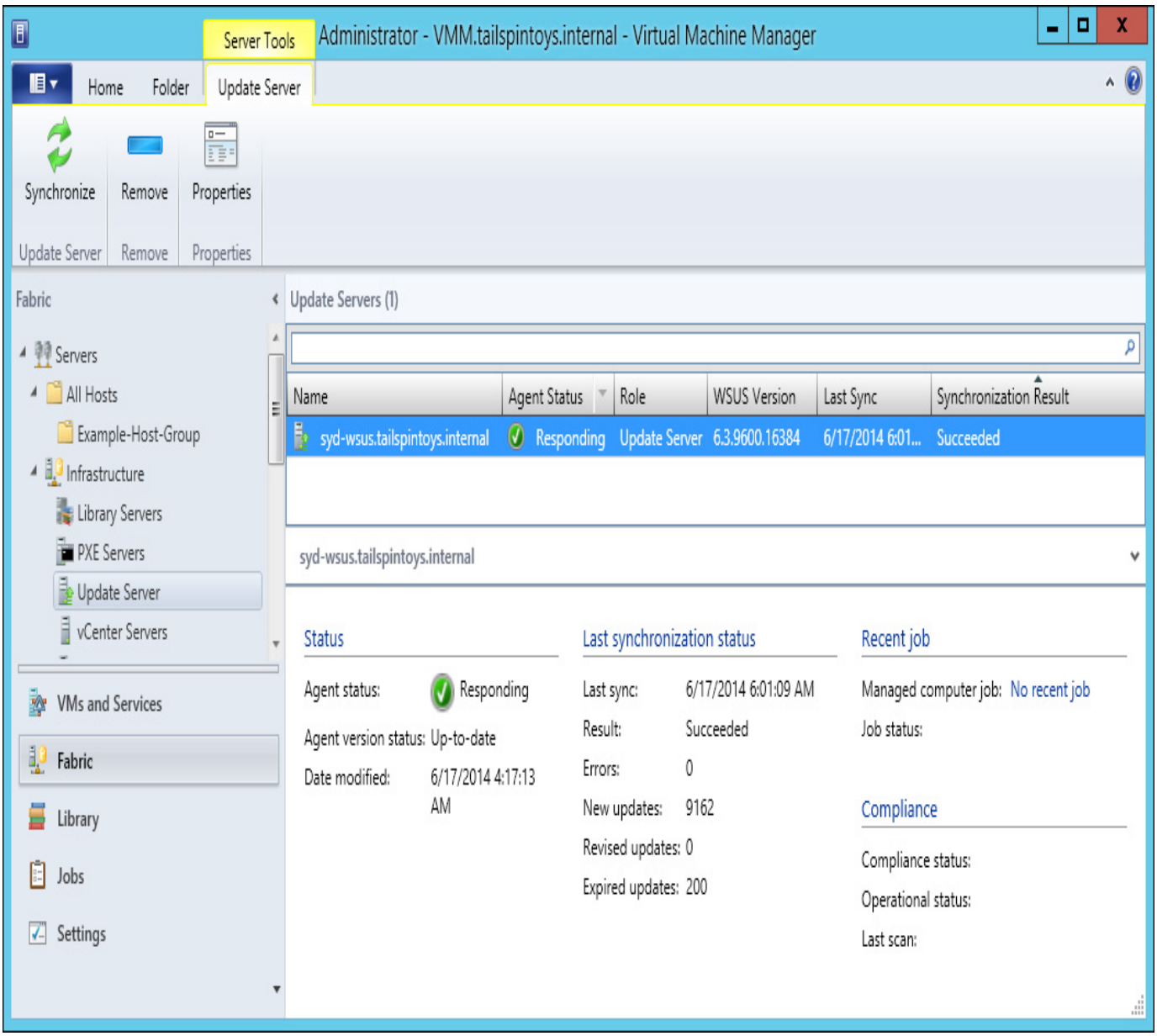

FIGURE 5-37 Update Server

5. To check which updates are available, in the Library workspace, select Update Catalog under Update Catalog And Baselines, and verify that updates are listed, as shown in Figure 5-38.

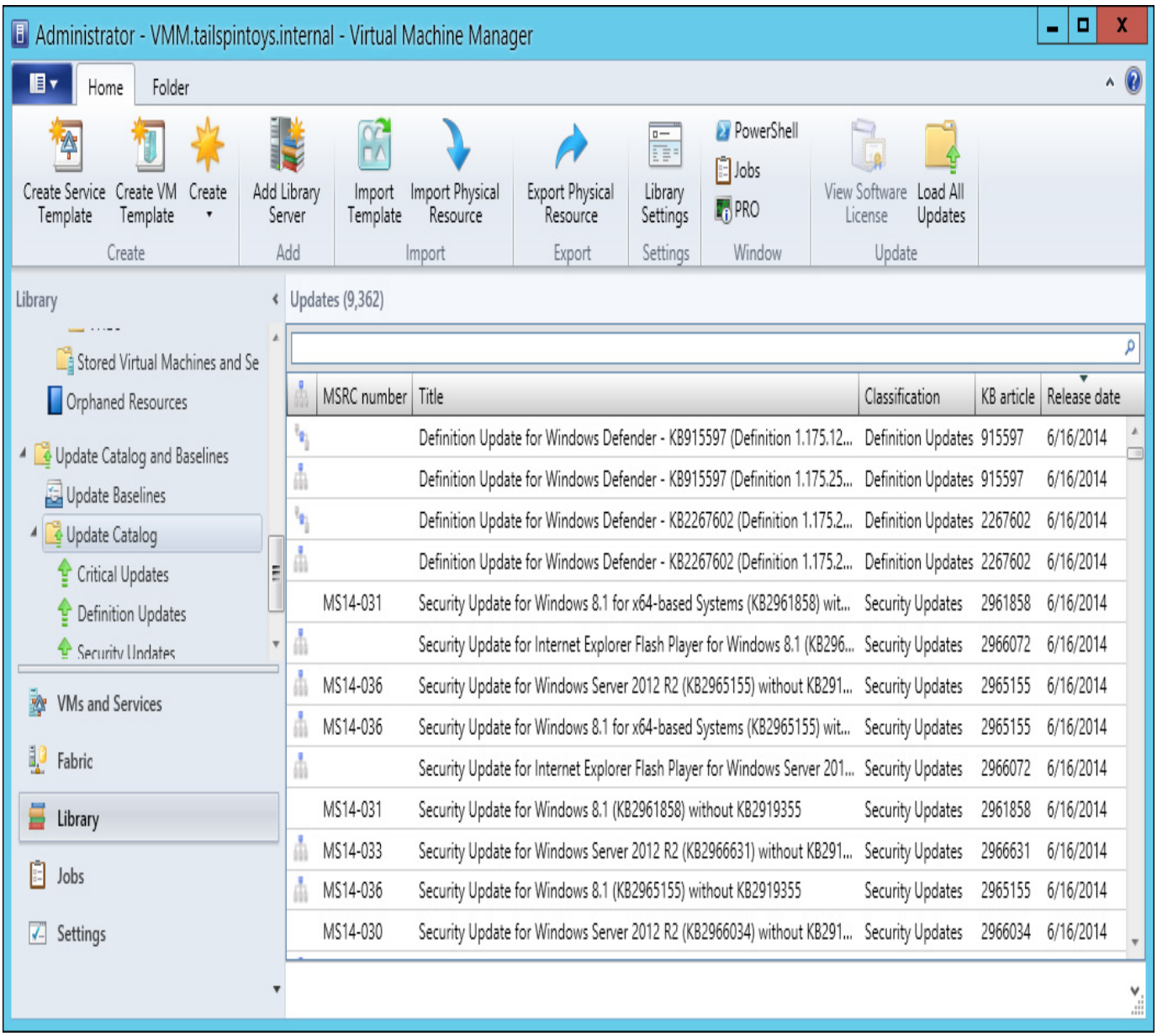

FIGURE 5-38 Update Catalog

After the initial synchronization is performed to gather the current list of available updates, VMM will not perform subsequent synchronizations automatically. This means that you need to either perform them manually, or configure a scheduled task using the Start-SCUpdateServerSynchronization Windows PowerShell cmdlet. To trigger a synchronization using the VMM console, perform the following steps:

1. In the Fabric workspace of the VMM console, select Update Server under the Servers\Infrastructure node.
2. Select the WSUS server that you want VMM to synchronize.
3. On the ribbon, click the Synchronize icon.

To trigger synchronization from the Virtual Machine Manager Command Shell, issue the following command, where WSUSServerName is the name of the WSUS server.

Click here to view code image

```
SCUpdateServerSynchronization WSUSServerName
```

More Info: **Integrating WSUS with VMM**

You can learn more about integrating WSUS with VMM at *http://technet.microsoft.com/en-us/library/gg675099.aspx*.

Update baselines

An update baseline is a collection of software updates. You can use update baselines as a way of assessing computers and applications to determine whether or not they are up-to-date. A computer that has all of the updates that are in an update baseline collection installed is said to be compliant. A computer that does not have all of the updates that are in an update baseline collection installed is said to be non-compliant.

More Info: **Update Baselines**

You can learn more about update baselines at *http://technet.microsoft.com/en-us/library/gg675110.aspx*.

You assign baselines to computers performing the following VMM roles:

- Host group
- Individual hosts
- Library servers
- PXE servers
- Update server
- VMM Management server

Figure 5-39 shows the Assignment Scope page of the Update Baseline Wizard.

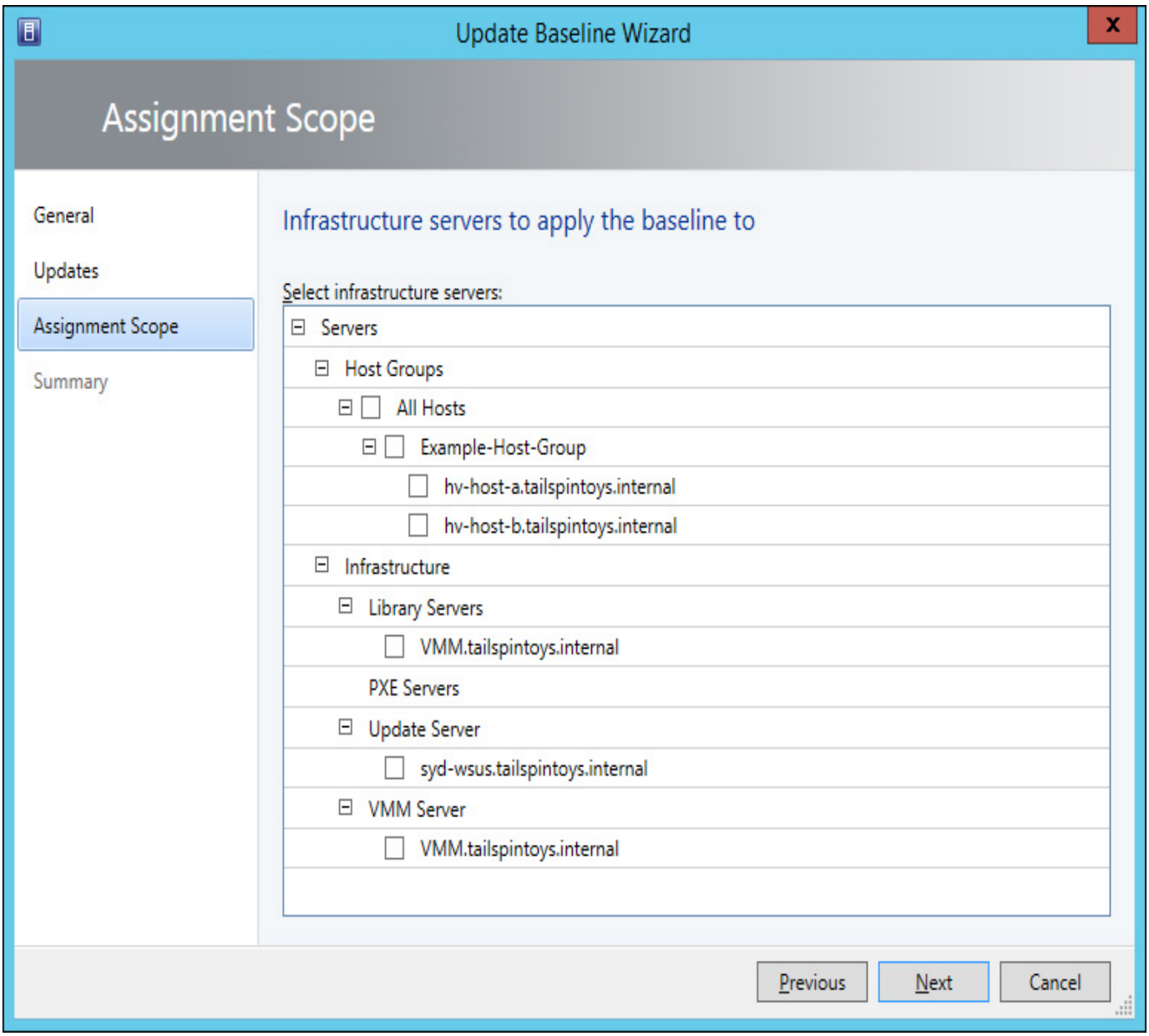

FIGURE 5-39 Assignment Scope

Assigning an update baseline does the following:

- When you assign a baseline to a host group, the baseline will apply to all stand-alone hosts and host clusters that are members of the group. The baseline also applies to any stand-alone costs and host clusters that are members of child host groups.
- When you move a host or host cluster between host groups, the host or host cluster will use the update baseline associated with its new host group.
- If you assign a baseline to a host or a host cluster directly, the host or host cluster will use that update baseline when moved between host groups.

To create a new update baseline, perform the following steps:

1. In the Library workspace of the VMM console, click Update Baselines under Update Catalog And Baselines.
2. On the ribbon, click Create, and then click Baseline. This will launch the Update Baseline Wizard.
3. On the General page of the Update Baseline Wizard, provide a name and description for the baseline.
4. On the Updates page of the Update Baseline Wizard, click Add. This will launch the Add Updates To Baseline dialog box. You use this dialog box to add updates to the baseline. Figure 5-40 shows a security update for Windows Server 2012 R2 selected for addition to the baseline. Select all of the updates that you want to have in the baseline, and click Add.

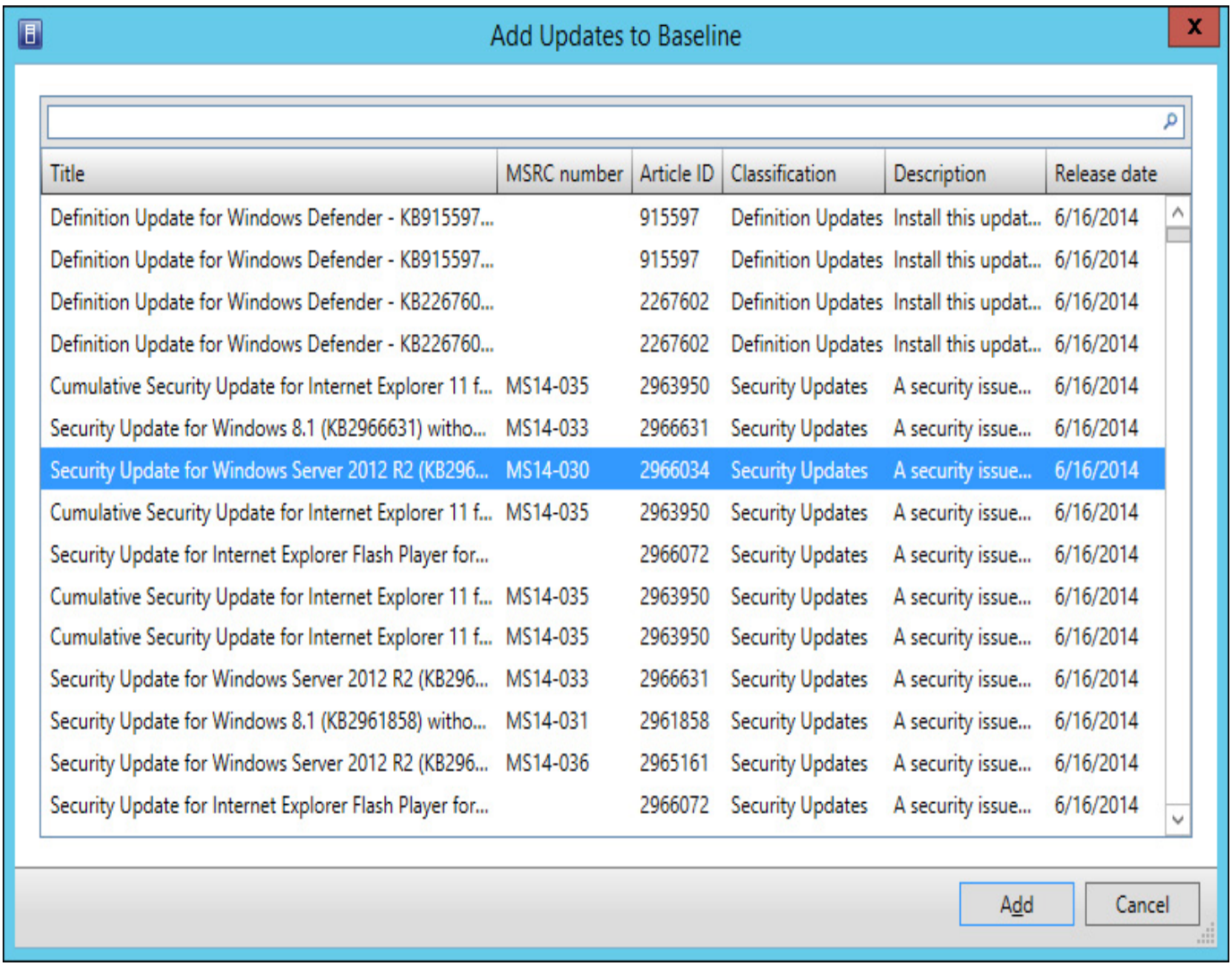

FIGURE 5-40 Add Updates To Baseline

5. On the Updates page of the Update Baseline Wizard, shown in Figure 5-41, review the list of updates in the baseline, and then click Next.

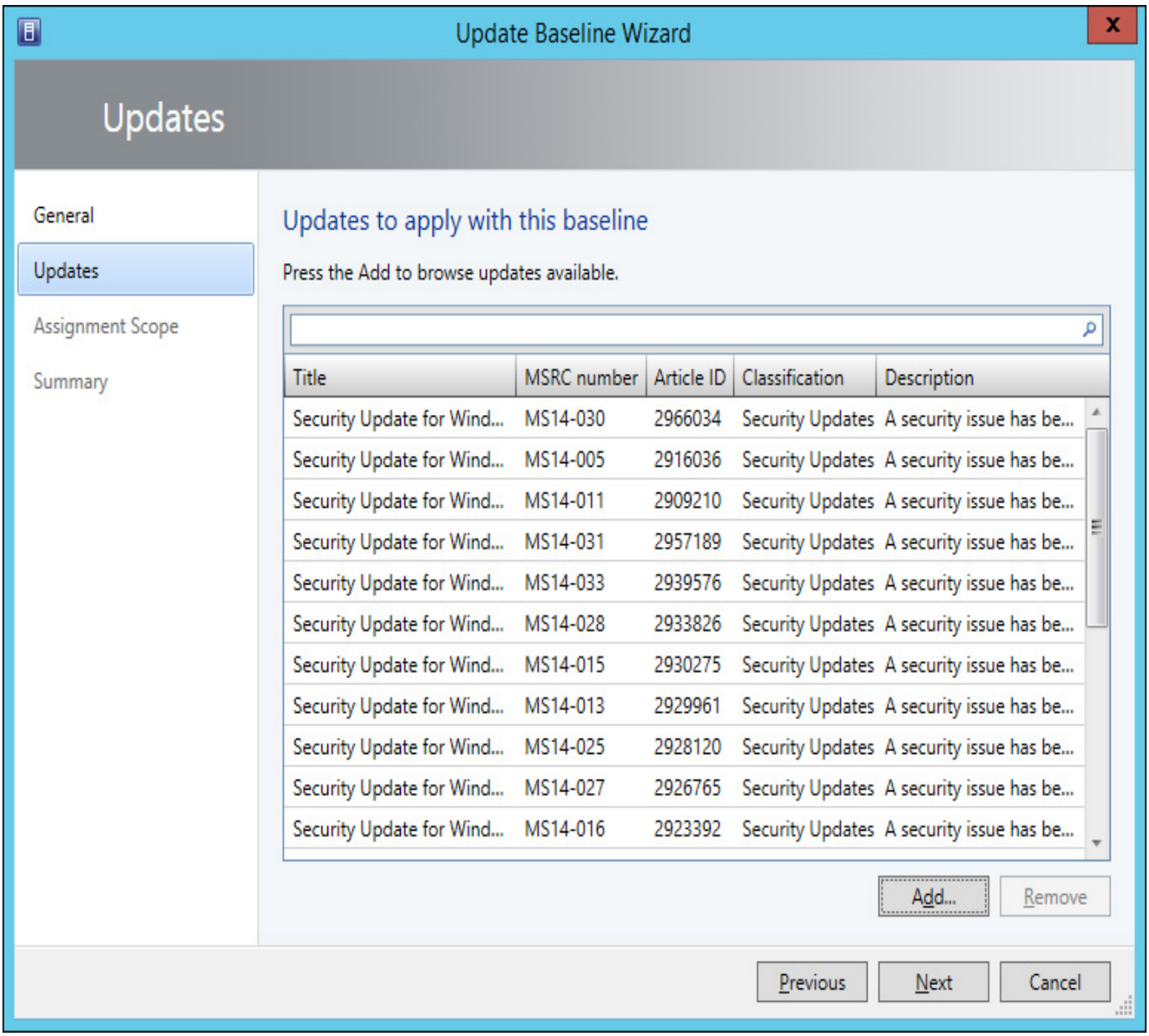

FIGURE 5-41 Updates

6. On the Assignment Scope page, select the servers, host clusters, and host groups to which you wish to assign the baseline. You don't have to assign the baseline at this time. You can do it after you have created the baseline.
7. Complete the wizard to create the update baseline.

To assign computers to a baseline, edit the properties of the baseline and select the host groups, hosts, or infrastructure server to which you want the baseline to apply. Figure 5-42 shows the TailspinToys Baseline update baseline being assigned to the Example-Host-Group host group.

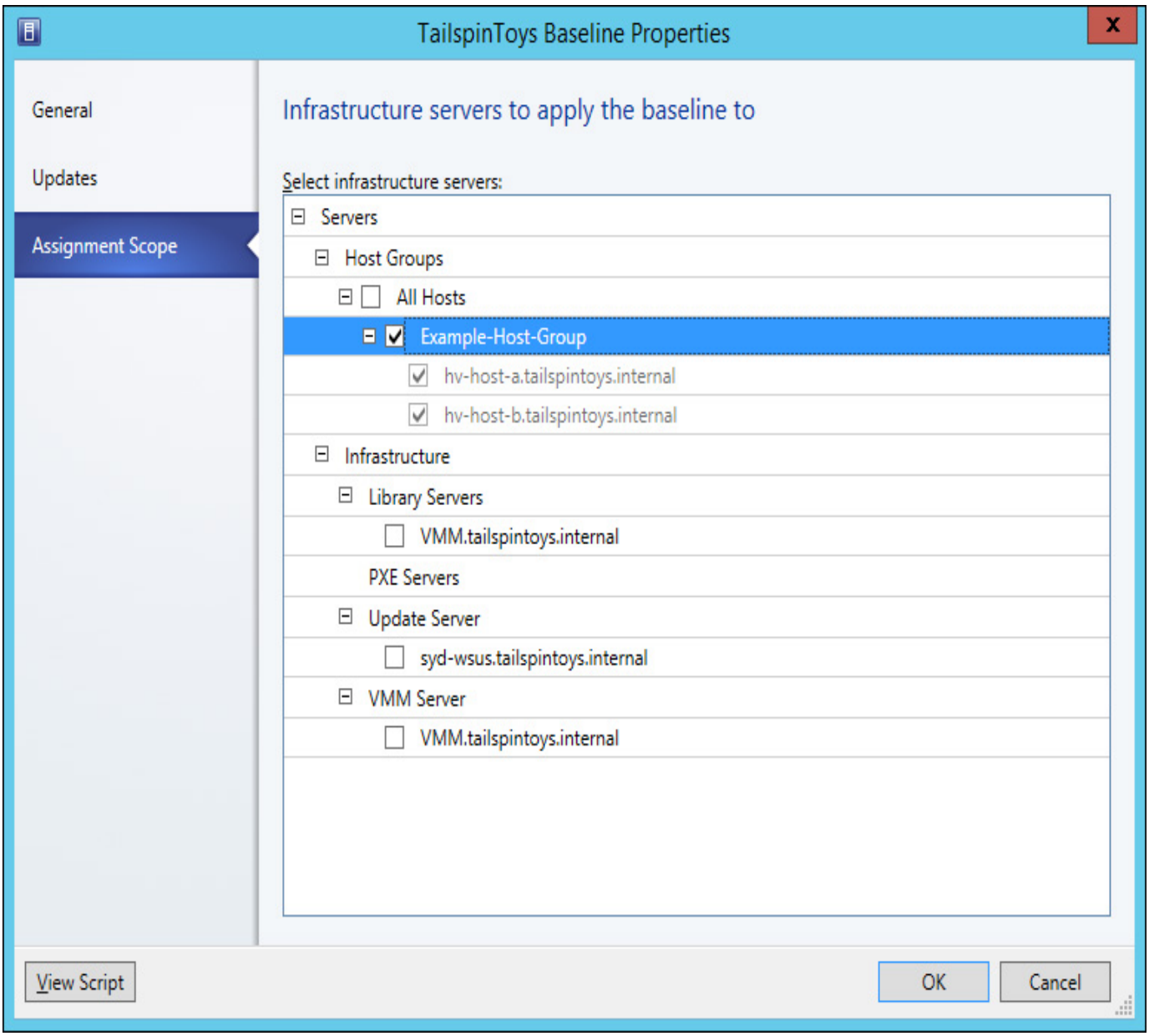

FIGURE 5-42 Assign

Update compliance

After assigning an update baseline, you can perform a scan to determine the compliance status of the computers subject to the baseline. A compliance scan checks whether each update in the baseline is applicable to the computer and, if the update is applicable, whether that update is installed. After a compliance scan, each update will have one of the following statuses:

- Compliant
- Non Compliant
- Error
- Pending Reboot
- Unknown

The unknown status often applies when hosts are moved between host groups, when updates are added or removed from baselines, or when computers are added to the scope of the baseline. Viewing compliance properties will provide additional information.

To scan a computer to determine whether or not it is compliant, perform the following steps:

1. In the Fabric workspace of the VMM console, select the server on which you want to perform the compliance check.
2. On the Home tab of the ribbon, click Scan.
3. On the Home tab of the ribbon, click Compliance Properties to view the compliance state of the

computer. Figure 5-43 shows the compliance state of Hv-host-a.tailspintoys.internal against the TailspinToys Baseline.

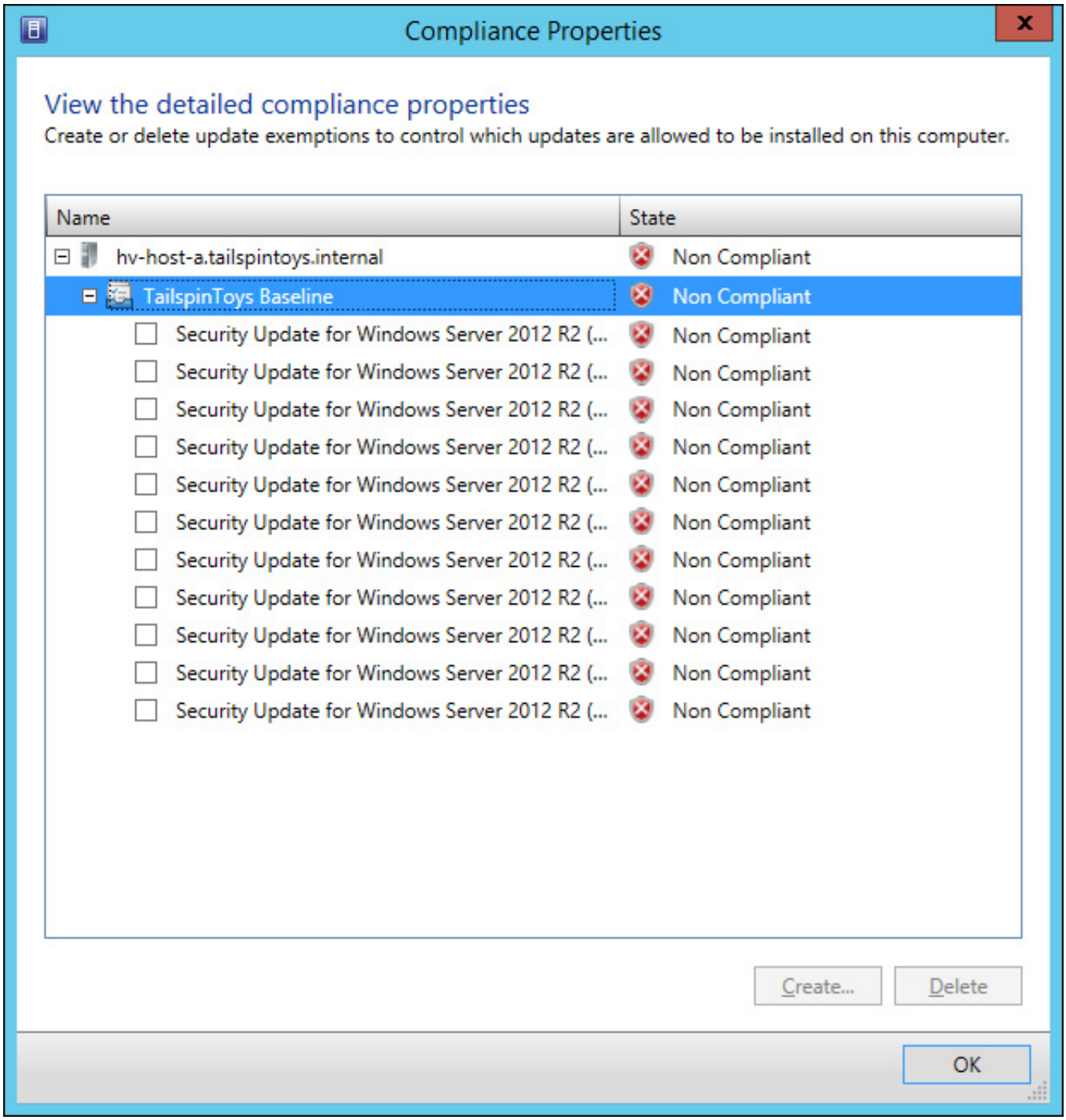

FIGURE 5-43 Compliance Properties

You can use the Compliance Properties dialog box to exempt a particular computer from a specific update. Figure 5-44 shows two updates exempted from a particular baseline for host Hv-host-a.tailspintoys.internal.

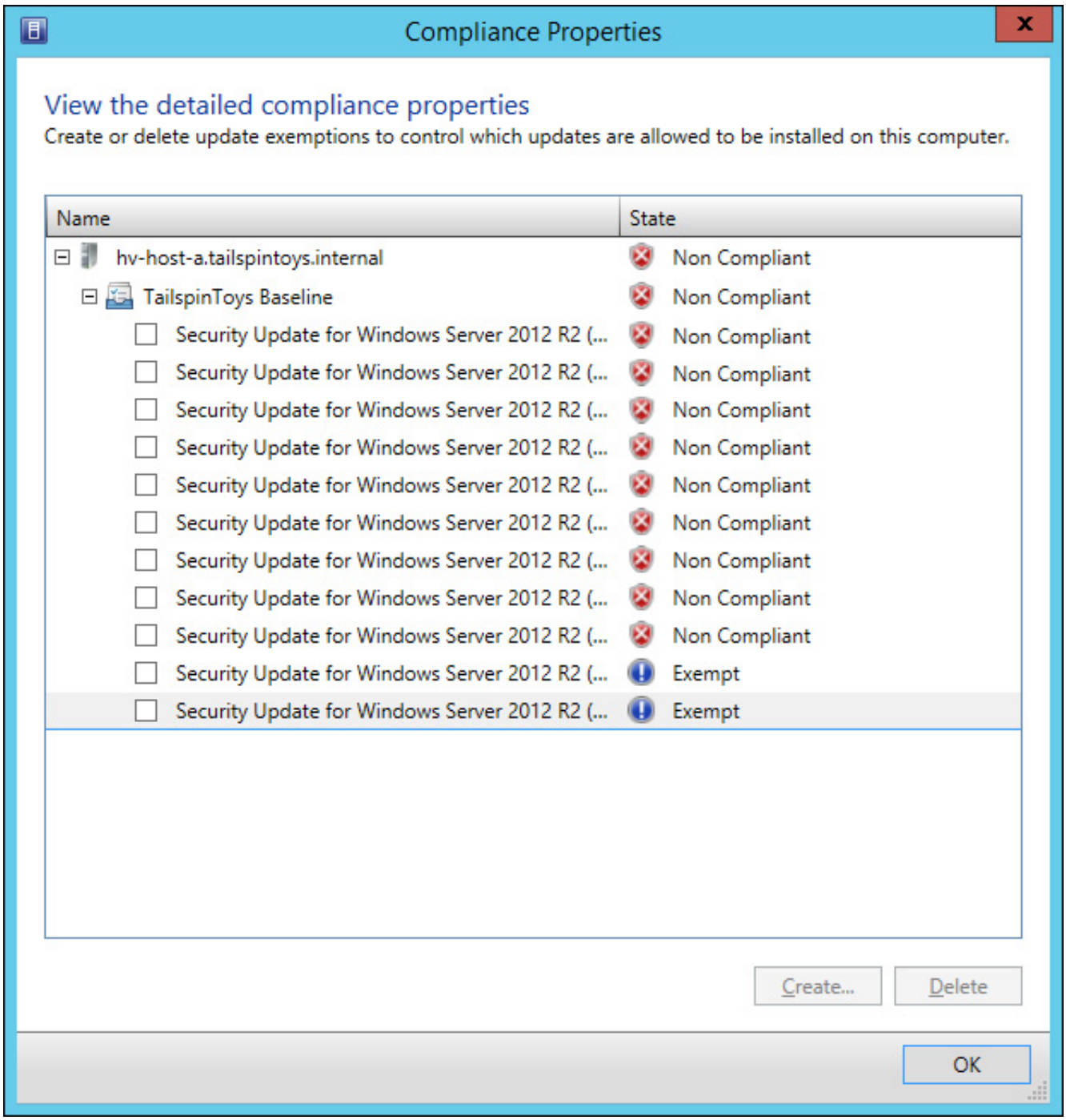

FIGURE 5-44 Exemption

To create an exemption, select those updates you want to exempt from the baseline, and click Create. This launches the Create Exemption dialog box. When using this dialog box, provide notes that explain why the computer or computers in question have been exempted from the updates being applied, as shown in Figure 5-45.

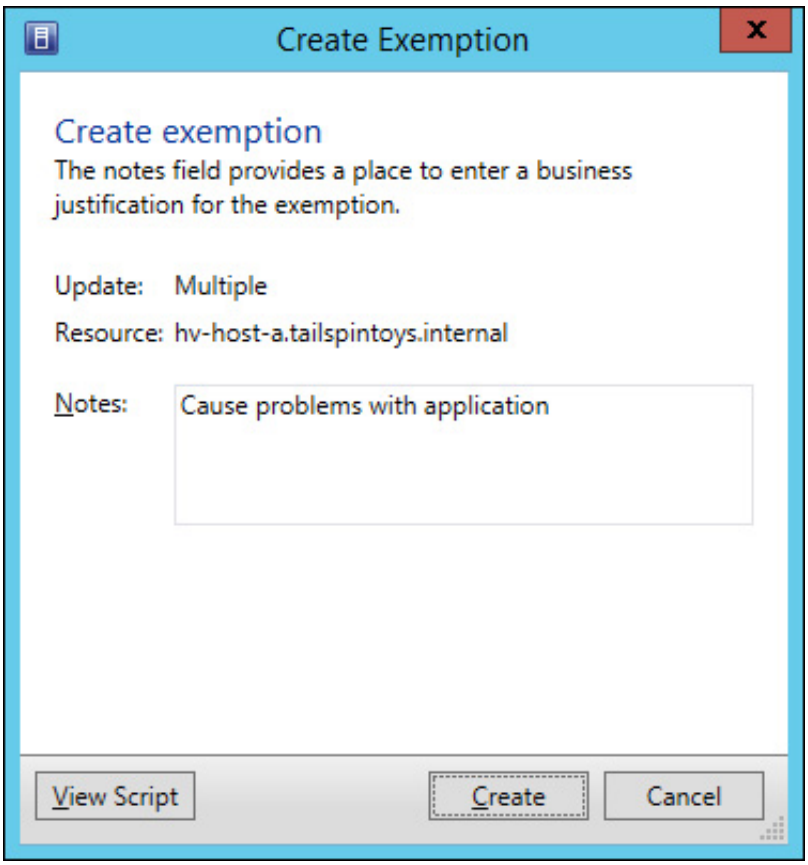

FIGURE 5-45 Create Exemption

More Info: **Update Compliance**

You can learn more about VMM update compliance at http://technet.microsoft.com/en-us/library/gg675093.aspx.

Update remediation

Remediating a computer applies updates that are relevant but have yet to be applied to a computer. To remediate a computer, select the update baseline under the computer Compliance view in the Fabric workspace, as shown in Figure 5-46, and then click Remediate on the ribbon.

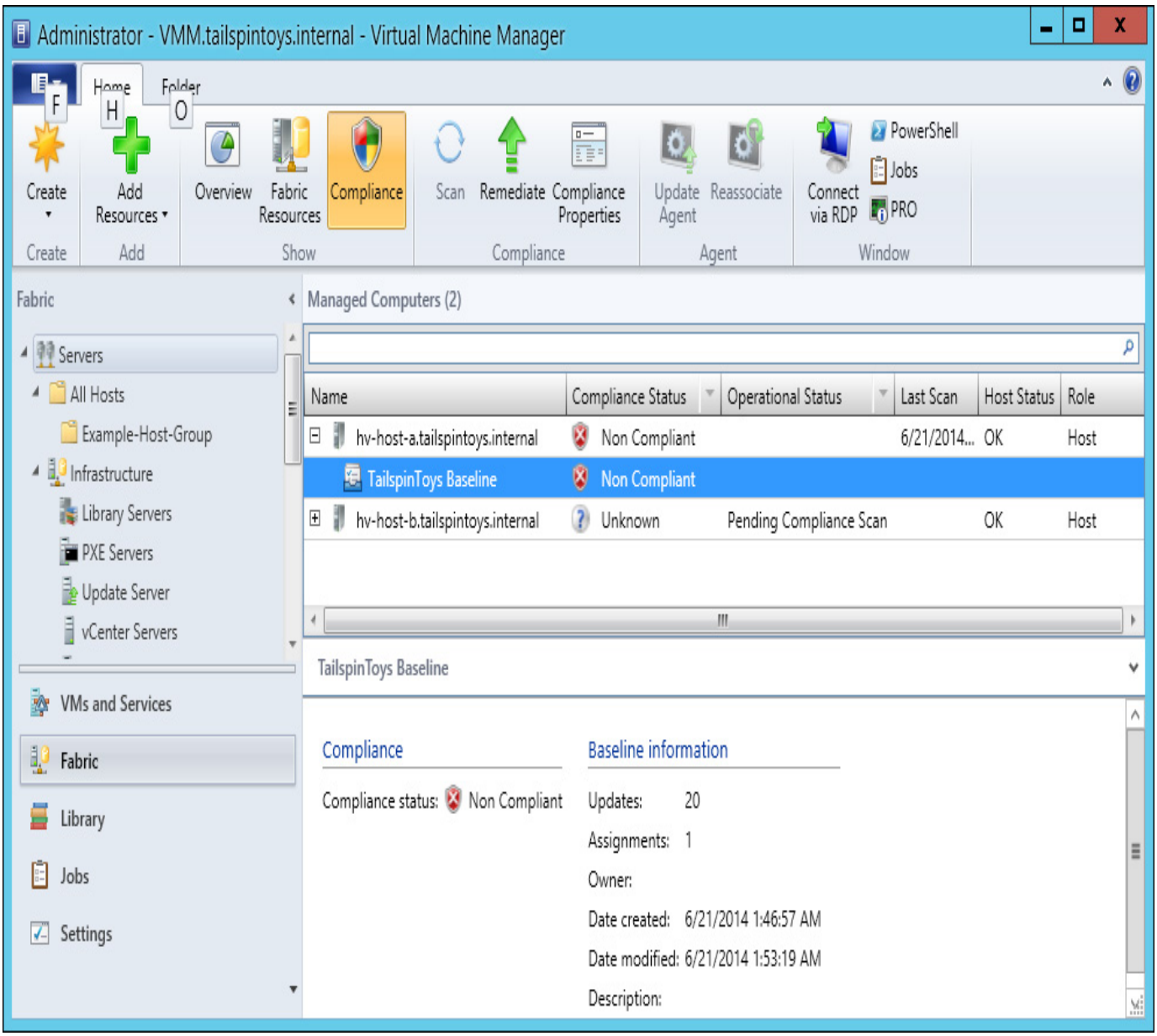

FIGURE 5-46 Non Compliant

On the Update Remediation dialog box, shown in Figure 5-47, select whether to restart servers to complete update installation. If you are applying updates to Hyper-V cluster nodes, you can also select whether virtual machines will be evacuated from the node, or placed into a saved state.

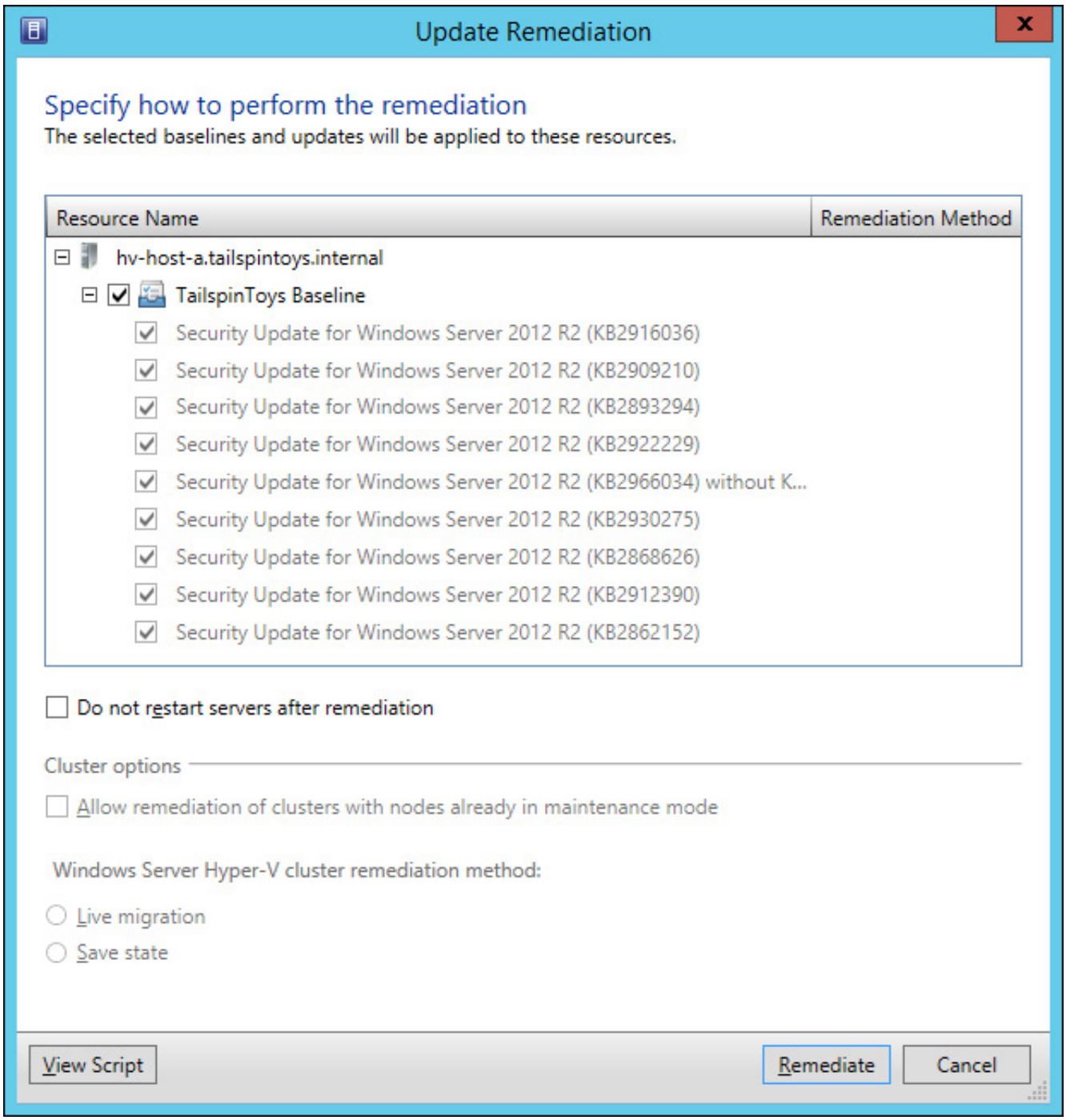

FIGURE 5-47 Update Remediation

More Info: **Update Remediation**

You can learn more about VMM update remediation at *http://technet.microsoft.com/en-us/library/gg675081.aspx*.

Updating offline VMs

Prior to the release of System Center 2012 R2 Virtual Machine Manager, administrators used the Virtual Machine Servicing Tool (VMST) to apply software updates to offline VMM virtual machines. Since the release of System Center 2012 R2 Virtual Machine Manager, the recommended method of updating offline virtual machines is to use a service management automation runbook that is available on Microsoft's website. The service management automation runbook performs the following tasks:

1. Locate all images stored in the VMM library.
2. Mount each virtual machine hard disk image on the VMM server.
3. Locate updates that are made available through WSUS.
4. Perform a check to determine if the update is applicable.

5. Perform a check to determine whether the update has been applied.
6. Apply updates to the mounted virtual hard disk image.
7. Commit the changes to the virtual hard disk and dismount.

More Info: **Update Offline VMs**

You can learn more about updating offline VMs at *http://blogs.technet.com/b/privatecloud/archive/2013/12/07/orchestrated-vm-patching.aspx*.

Exam Tip

Remember that while VMM manages updates for virtualization hosts and VMM servers, it does not manage updates for virtual machines.

***Thought experiment*: WSUS at Fabrikam**

You are in the process of deploying WSUS at a medium sized enterprise that will be deploying Configuration Manager and VMM to manage software updates within the next 12 months. You have created several computer groups and automatic deployment rules to allow for automatic update approval. You want to ensure that client computers at Fabrikam automatically contact the WSUS server rather than the Microsoft Update servers. You also want to ensure that WSUS computer group membership occurs through Group Policy.

1. Which Group Policy do you need to configure so that servers know the location of the WSUS server?
2. Which Group Policy do you need to configure to assign computers to WSUS computer groups?

Objective summary

- WSUS is a Windows Server server role that allows you to manage and centralize the deployment of updates.
- You can configure automatic approval rules that allow updates to be automatically approved based on update classification, product being updated, and the computers being updated.
- You can integrate WSUS with Configuration Manager. When you do this, you create software update groups that contain multiple updates and then deploy these updates to Configuration Manager computer collections.
- You can perform compliance checks to determine whether updates have been deployed on specific Configuration Manager clients.
- You can integrate WSUS with VMM. This allows you to manage the updates for your virtualization hosts as well as your VMM infrastructure.
- With VMM, you collect updates into baselines. You can then assess hosts against the baseline and remediate any hosts that are missing updates.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You are using Configuration Manager with WSUS to manage software updates in your

environment. You have performed and updated synchronization and located five updates that you want to deploy to a collection of computers running the Windows Server 2012 R2 operating system. Which of the following steps should you take before performing deployment?

A. Create a software update group.

B. Create an Update baseline.

C. Download the updates and create a deployment package.

D. Create an automatic approval rule.

2. You have integrated VMM with WSUS. You want to check whether several virtualization hosts have several recently released updates installed. Which of the following steps should you take to accomplish this goal?

A. Add the updates to an update baseline.

B. Add the updates to a Software Update Group.

C. Assign the update baseline to the virtualization hosts and assess compliance.

D. Assign the software update group to the virtualization hosts and assess compliance.

3. You have deployed System Center 2012 R2 Virtual Machine Manager. Which of the following tools can you use to automatically apply software updates to VM images stored in the VMM library?

A. Virtual Machine Servicing Tool

B. Service management automation runbook

C. WSUS

D. Configuration Manager

Objective 5.3: Implement backup and recovery

Although it is likely that the fabric upon which you are running your private cloud is highly redundant, with VMs hosted on failover clusters that use redundant storage and network resources, it's still important to ensure that you regularly back up important workloads. This is because while redundant resources minimize the chance that you'll lose important data to hardware failure, it's still possible to lose data due to data corruption, malware, or an administrator making an unforced error.

This section covers the following topics:

- Understanding Data Protection Manager
- Deploying DPM agents
- Configuring DPM storage
- Creating DPM protection groups
- Performing recovery
- Integrating Microsoft Azure Online Backup
- Using DPM Orchestrator integration pack

Understanding Data Protection Manager

System Center 2012 R2 Data Protection Manager (DPM) is Microsoft's data protection and recovery solution. You can use DPM to backup and recover workloads including Exchange, SQL Server, SharePoint, Windows server role services and features, and virtual machine running under Hyper-V. DPM supports backup to disk, to take, and to Microsoft Azure.

When discussing DPM, it's important to understand the following terms:

- A recovery point objective (RPO) is the point in time to which you want to recover data. For example, you might need to recover a database to a specific RPO that represents the state it was in 45 minutes ago.
- A recovery time objective (RTO) is the amount of time you have to recover to the RPO. This is

the amount of time it would take to recover the database to the state it was in 45 minutes ago.

Deploying DPM agents

DPM requires that an agent be installed if it is going to be configured to protect a computer. The agent identifies which data on the computer can be protected, tracks changes that occur to that data, and manages the process of forwarding protected data from the protected computer to the DPM server. You need to configure any firewall on the DPM server to allow inbound TCP port 135 traffic, as well as allowing traffic to the DPM service (msdpm.exe) and the protection agent (dpmra.exe).

To deploy the DPM agents, perform the following steps:

1. In the Management workspace of the DPM console, click Install. This will launch the Protection Agent Installation Wizard. On the Select Agent Deployment method, shown in Figure 5-48, choose Install Agents, or Attach Agents. You select Attach Agents for computers that already have the agent software installed, for example those that have the DPM agent as part of their installation image, or for computers that might be on the perimeter network.

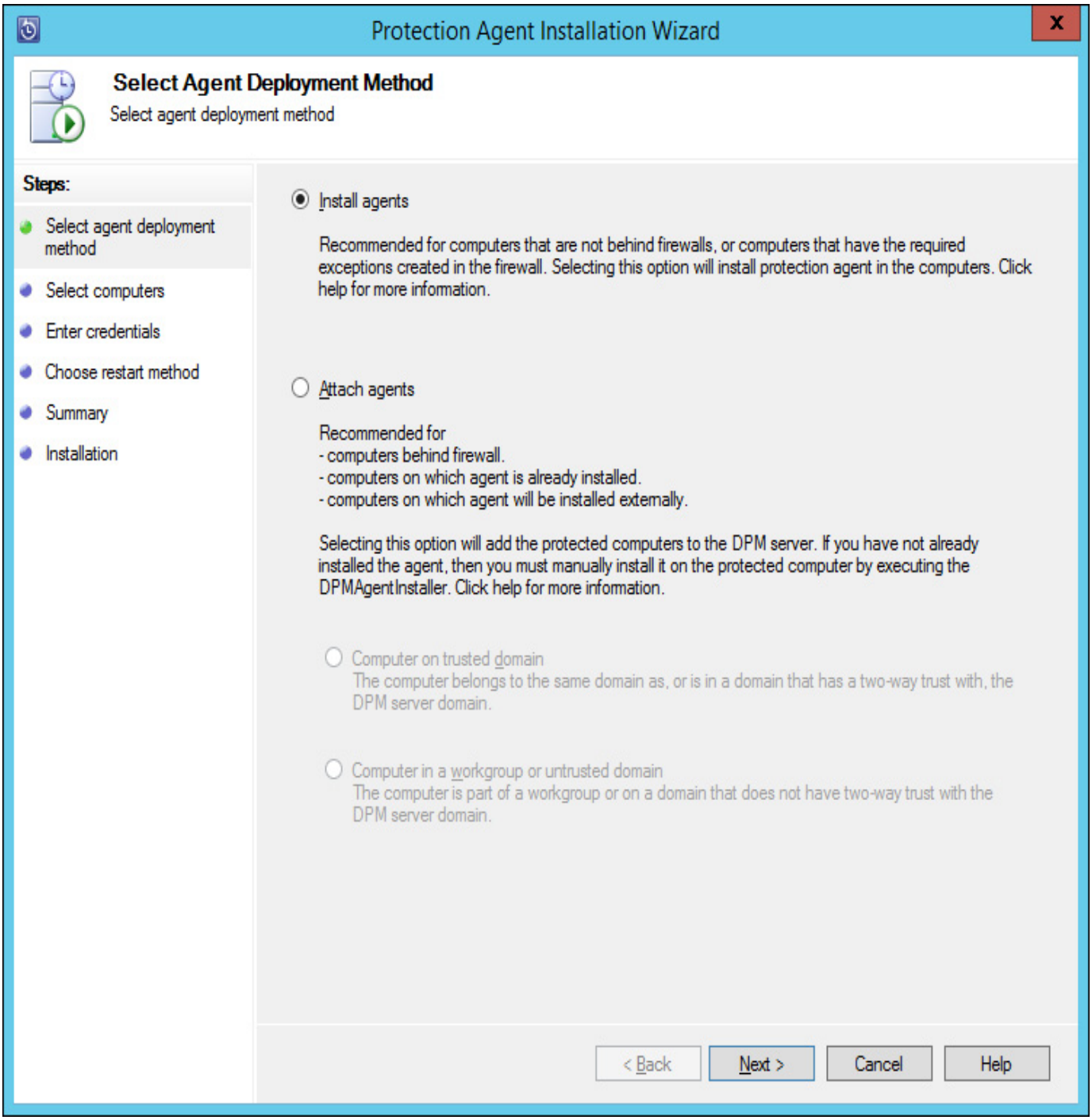

FIGURE 5-48 Install DPM agent

2. On the Select Computers page, either select computers that are in the same domain as the DPM server, which are presented in a list, as shown in Figure 5-49, or enter the FQDN of the

computer.

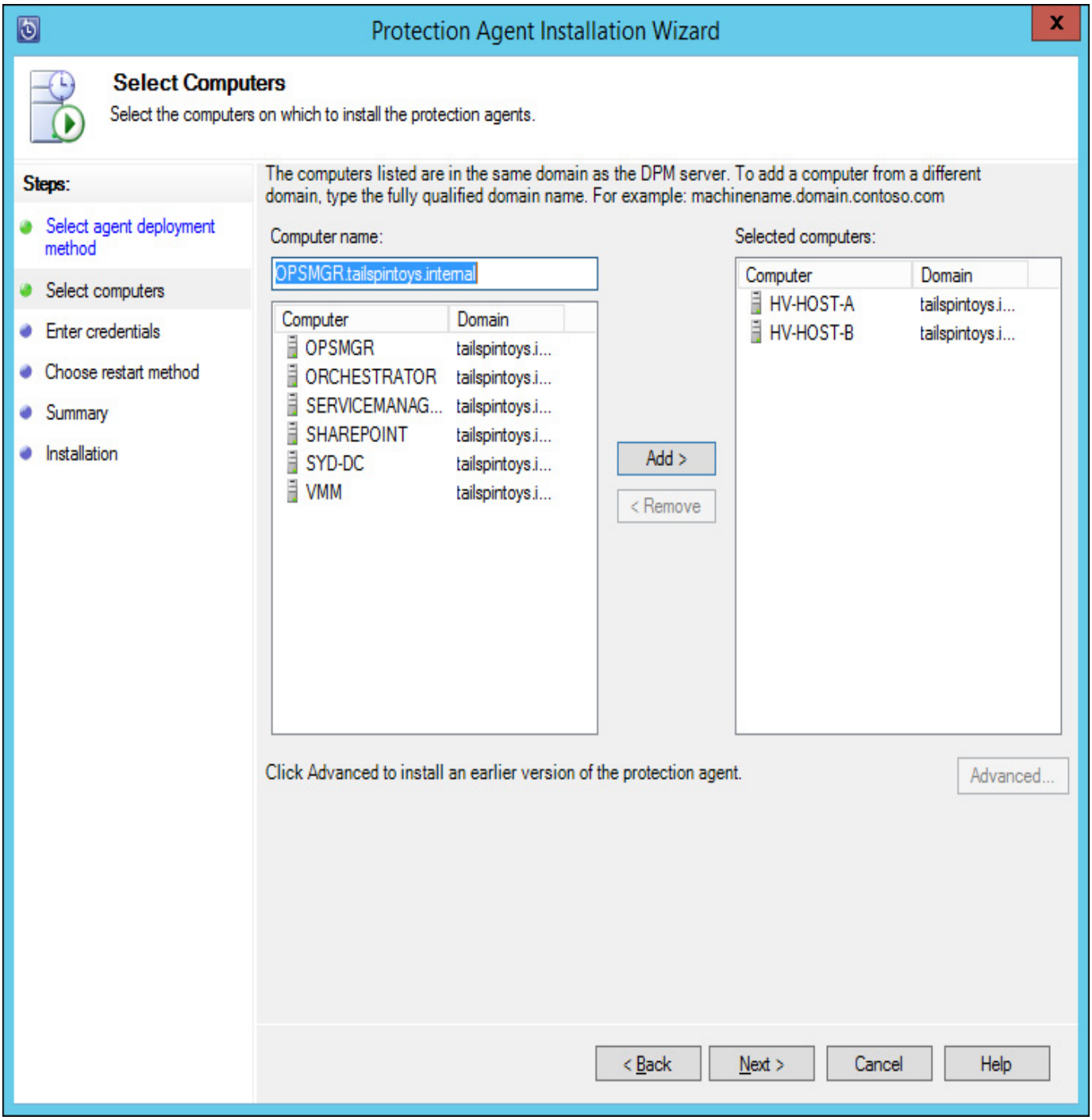

FIGURE 5-49 Select Computers

3. On the Credentials page, specify the credentials of an account that has local administrator access on the computers on which you want to deploy the DPM agent.
4. On the Choose Restart Method page, select whether restart will occur automatically or manually. Restart is only required on computers running the Windows Server 2003 or Windows Server 2003 R2 operating systems.
5. To complete the wizard, click Install. This will deploy the agent.

Figure 5-50 shows the DPM agent installed on HV-HOST-A and HV-HOST-B.

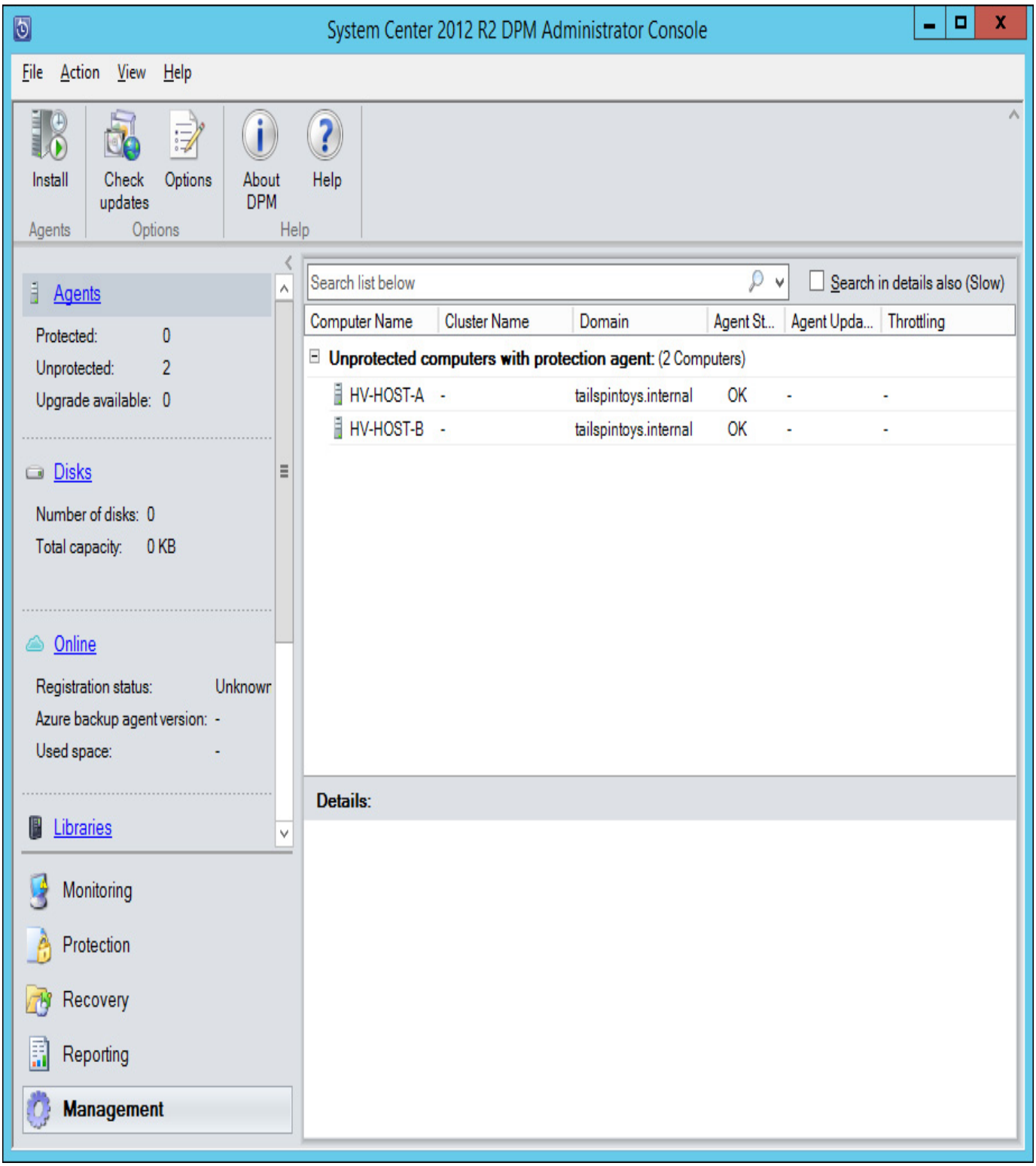

FIGURE 5-50 Agents

More Info: **DPM Agent Deployment**

You can learn more about deploying the DPM agent at *http://technet.microsoft.com/en-us/library/hh758075.aspx*.

Configuring DPM storage

DPM uses disk as the primary short-term storage location, whilst allowing long-term storage using tape. A DPM storage pool is a collection of disks that DPM uses to store replicas and recovery points for protected data. DPM requires at least one disk in the storage pool before it can begin protecting data. Additional disks can be added to the storage pool as necessary.

To add a disk to the DPM storage pool, perform the following steps:

1. In the Management workspace of the DPM console, click Disks.

2. On the ribbon, click Add. This will launch the Add Disks To Storage Pool dialog box. The disks must be online and initialized before you can add them to the DPM storage pool. Figure 5-51 shows two disks being added to the storage pool.

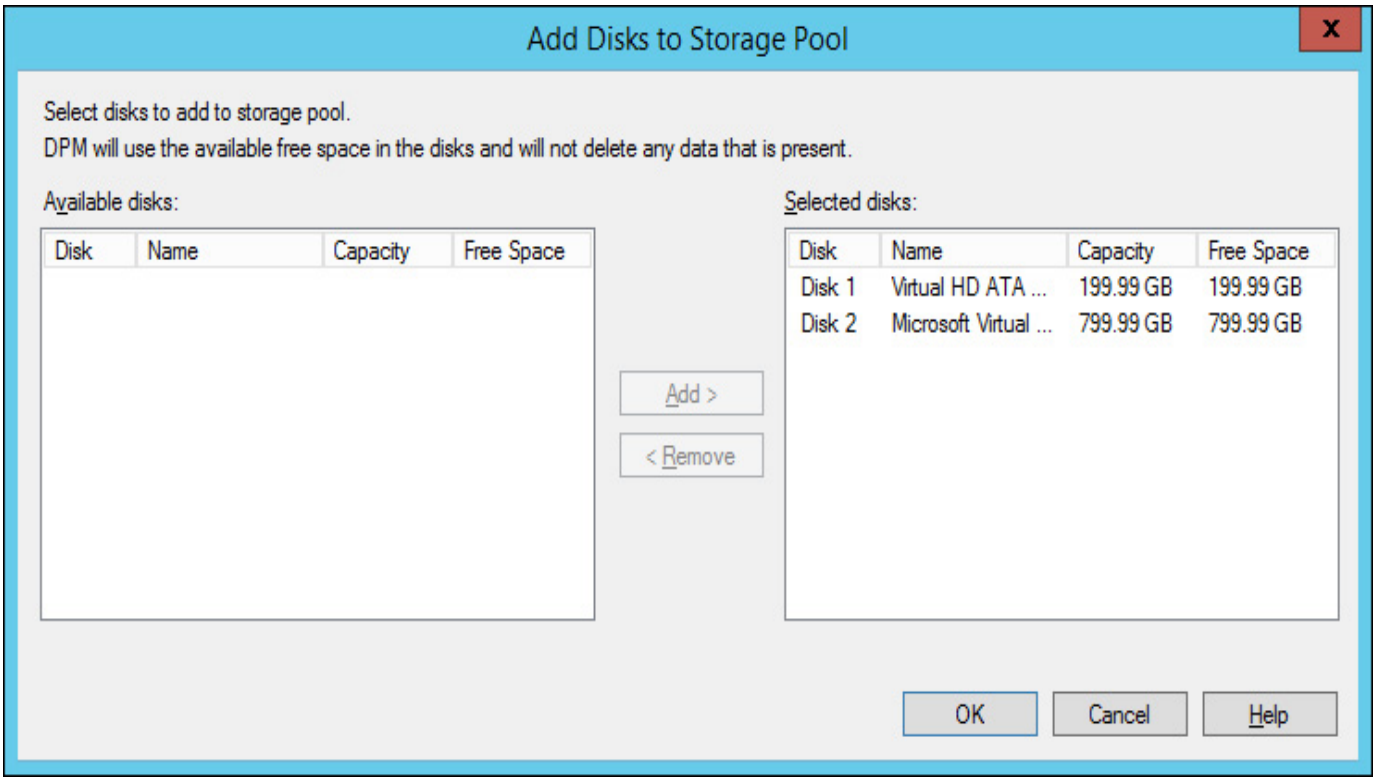

FIGURE 5-51 Adding disks to storage pool

3. Click OK to add the disks to the storage pool. DPM will convert any disk you add to dynamic, and convert any volumes to simple volumes. Best practice is to allocate new, unformatted, empty disks to the storage pool, and allow DPM to manage and prepare them. Figure 5-52 shows two disks added to the DPM storage pool.

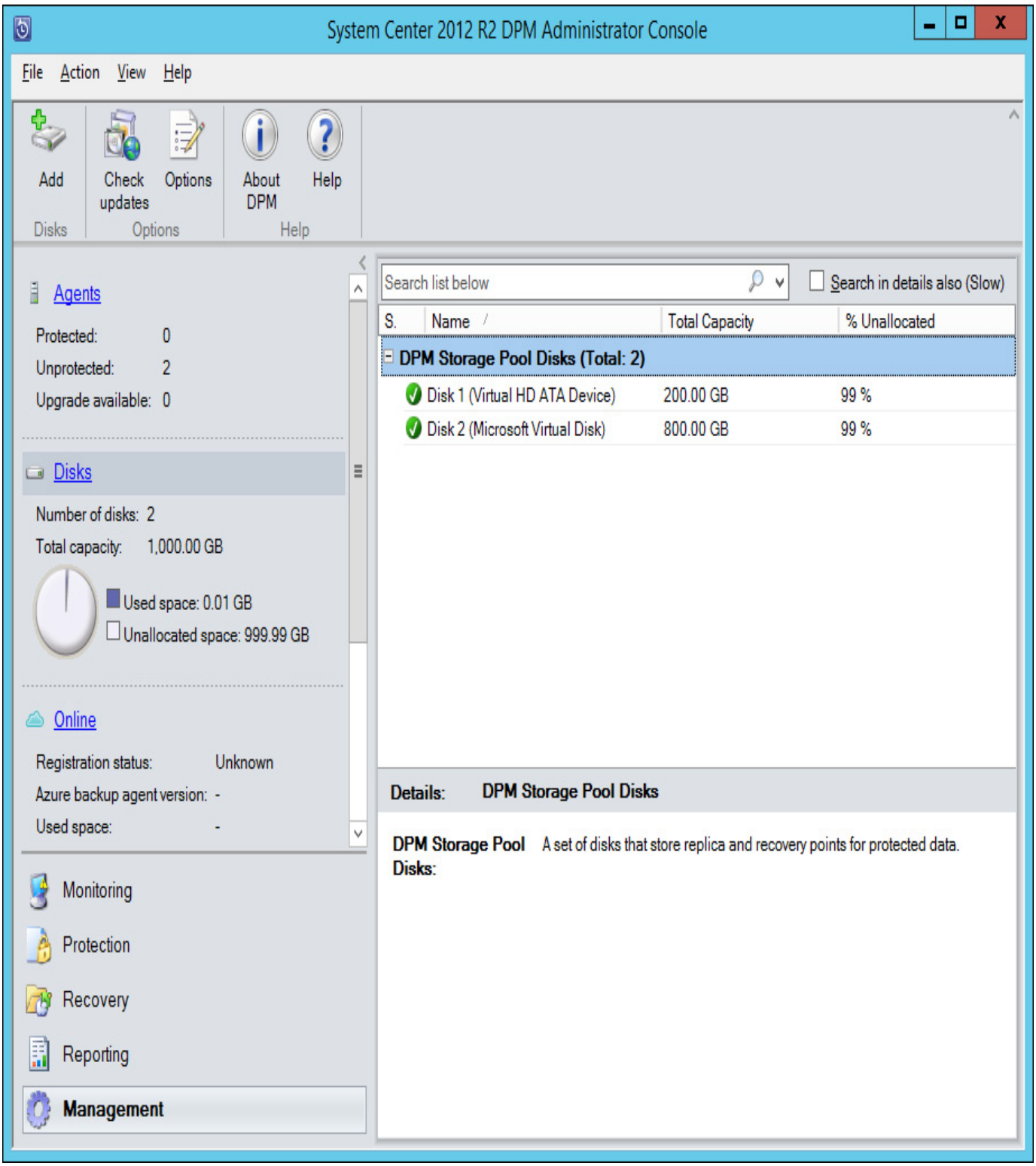

FIGURE 5-52 Storage pool disks

More Info: **DPM Storage**

You can learn more about configuring DPM storage at *http://technet.microsoft.com/en-us/library/hh758039.aspx*.

Creating DPM protection groups

Protection groups are collections of data sources (also known as workloads) that have a common protection configuration. Members of a protection group share the following:

- Backup targets (disk, tape, or Microsoft Azure)
- Protection schedule
- Recovery point schedule

■ Performance options (compression and consistency checks)

To create a protection group, perform the following steps:

1. In the Protection workspace of the DPM console, click New.
2. On the Select Protection Group Type page of the Create New Protection Group Wizard, shown in Figure 5-53, select Servers. You can also configure DPM to protect clients.

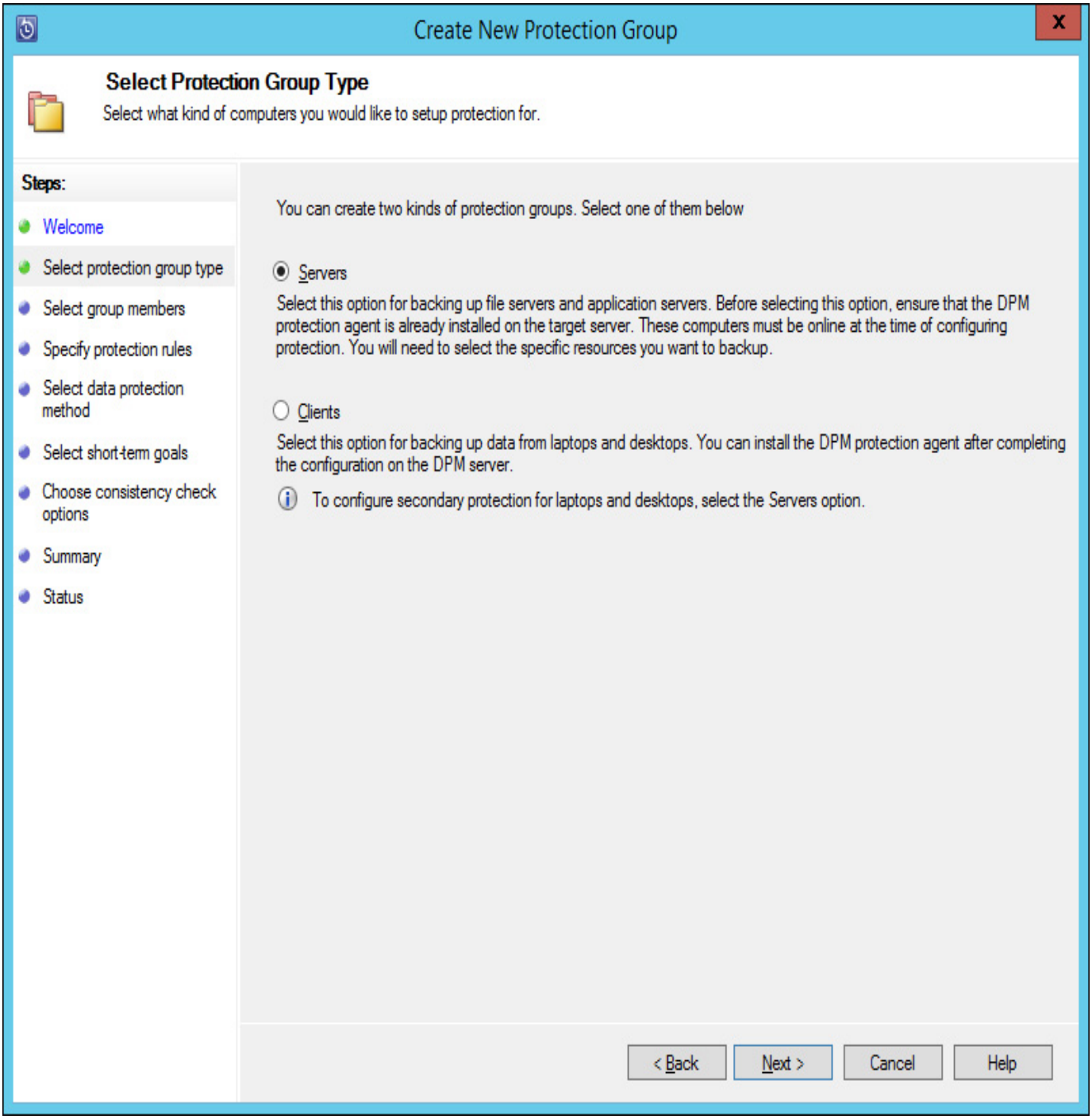

FIGURE 5-53 Servers protection group

3. On the Select Group Members page, specify which data you want to protect. For example, Figure 5-54 shows the selection of an online Hyper-V virtual machine named Live-Hyper-V-VM. When configuring protection group members, you specify what you will protect, from individual files and folders, through to VMs, databases, and even entire servers.

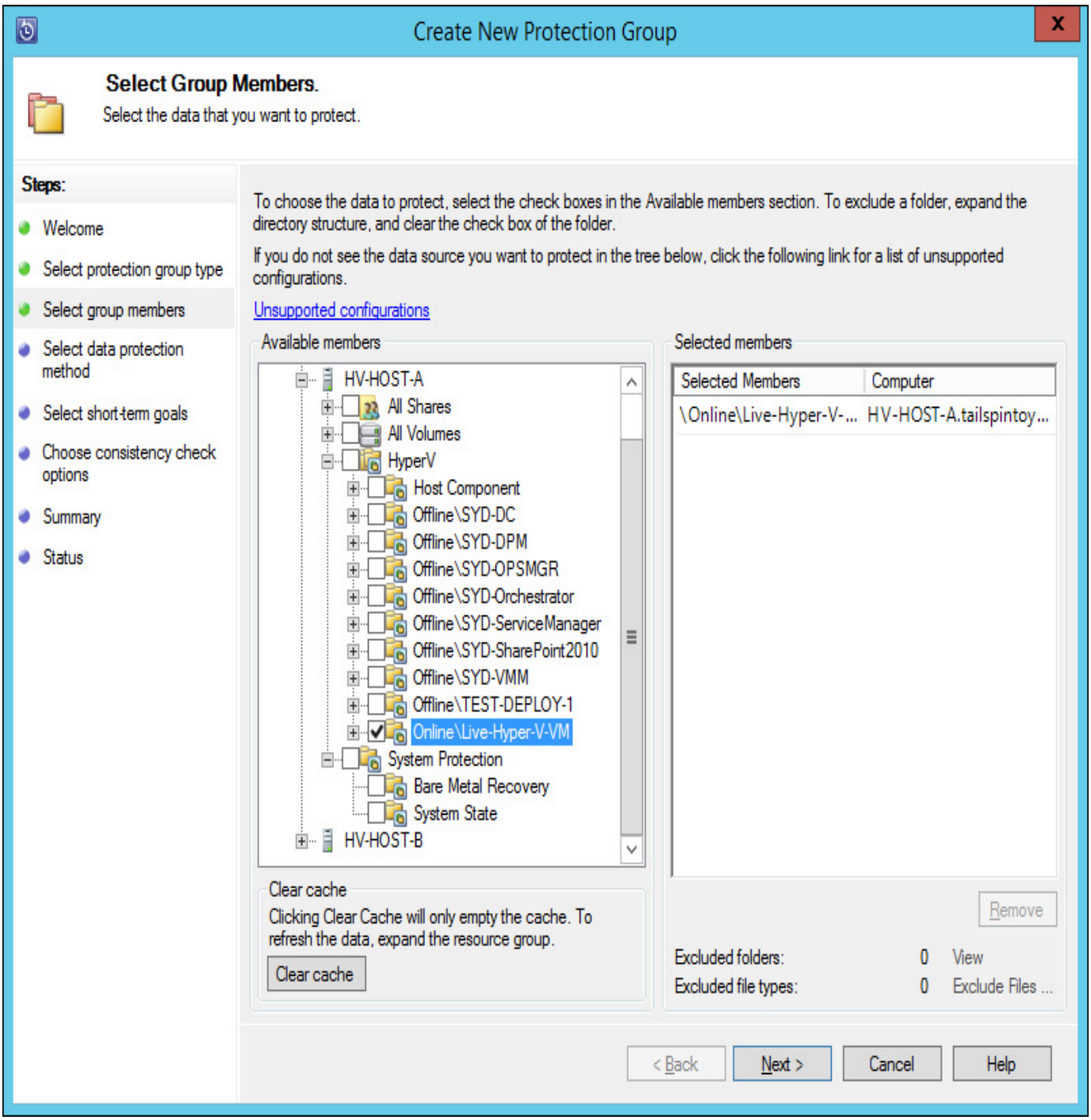

FIGURE 5-54 Select Group Members

4. On the Select Data Protection Method page, provide a protection group name, and then specify the protection methods. You can choose to have short-term protection using Disk, online protection using Microsoft Azure, and long-term protection using tape. The Azure and Tape options are only available if they have previously been configured. Figure 5-55 shows the selection of short-term protection using Disk.

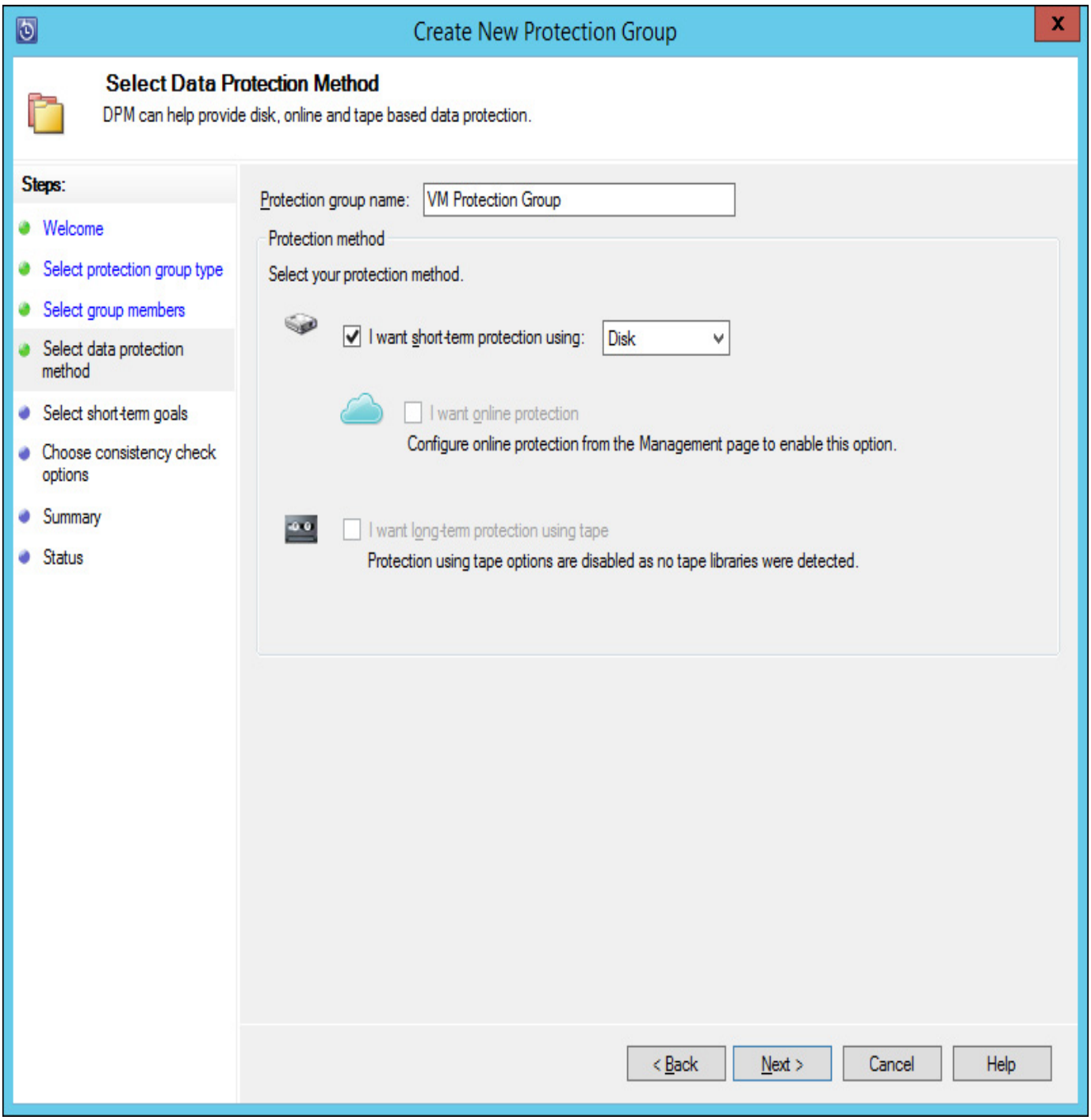

FIGURE 5-55 Select Data Protection Method

5. On the Specify Short Term Goals page, select the Retention Range and how often an Express Full Backup is taken. Figure 5-56 shows recovery points created every half an hour with a Retention Range of 3 days.

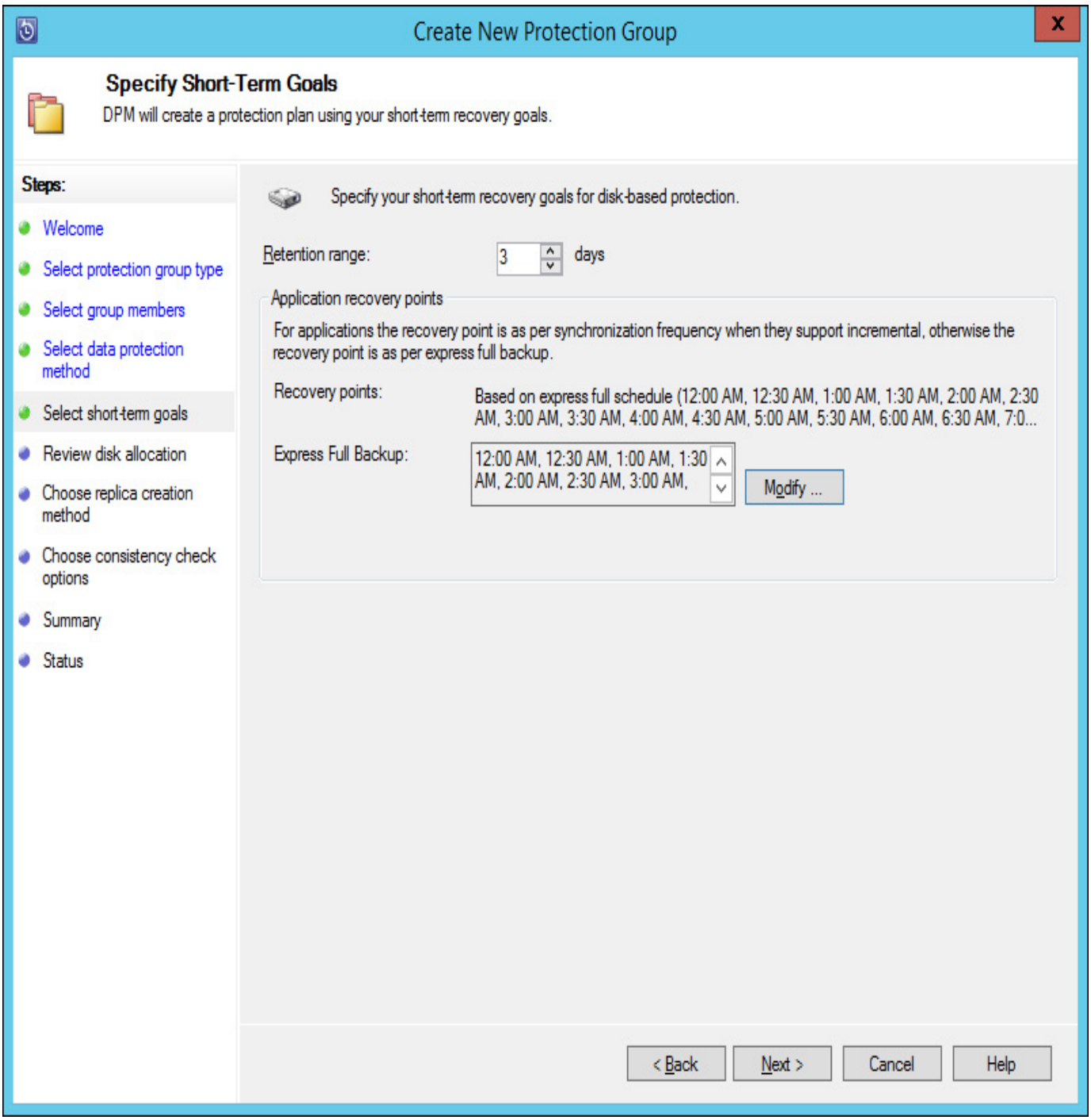

FIGURE 5-56 Select short-term goals

6. The Review Disk Allocation page allows you to view the allocation of storage in the storage pool. You also have the option to grow volumes as required. Figure 5-57 shows the Review Disk Allocation page.

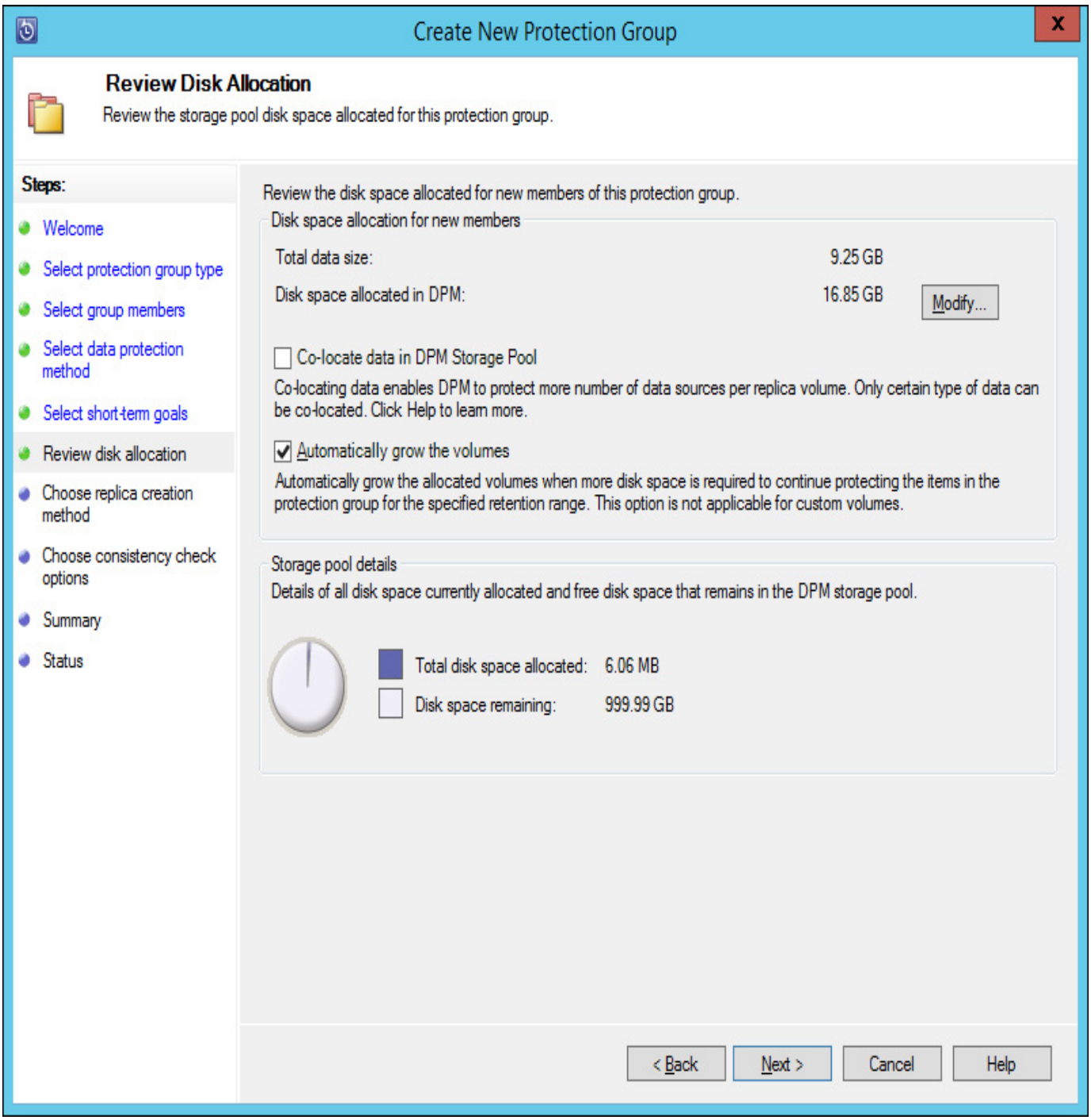

FIGURE 5-57 Review Disk Allocation

7. On the Choose Replica Creation Method page, select how the first replica should be created. Options include creating the replica immediately, creating the replica at a scheduled point in the future, or creating a replica manually using removable media.
8. On the Consistency Check Options page, shown in Figure 5-58, configure how often a consistency check is run to verify the integrity of the protected data.

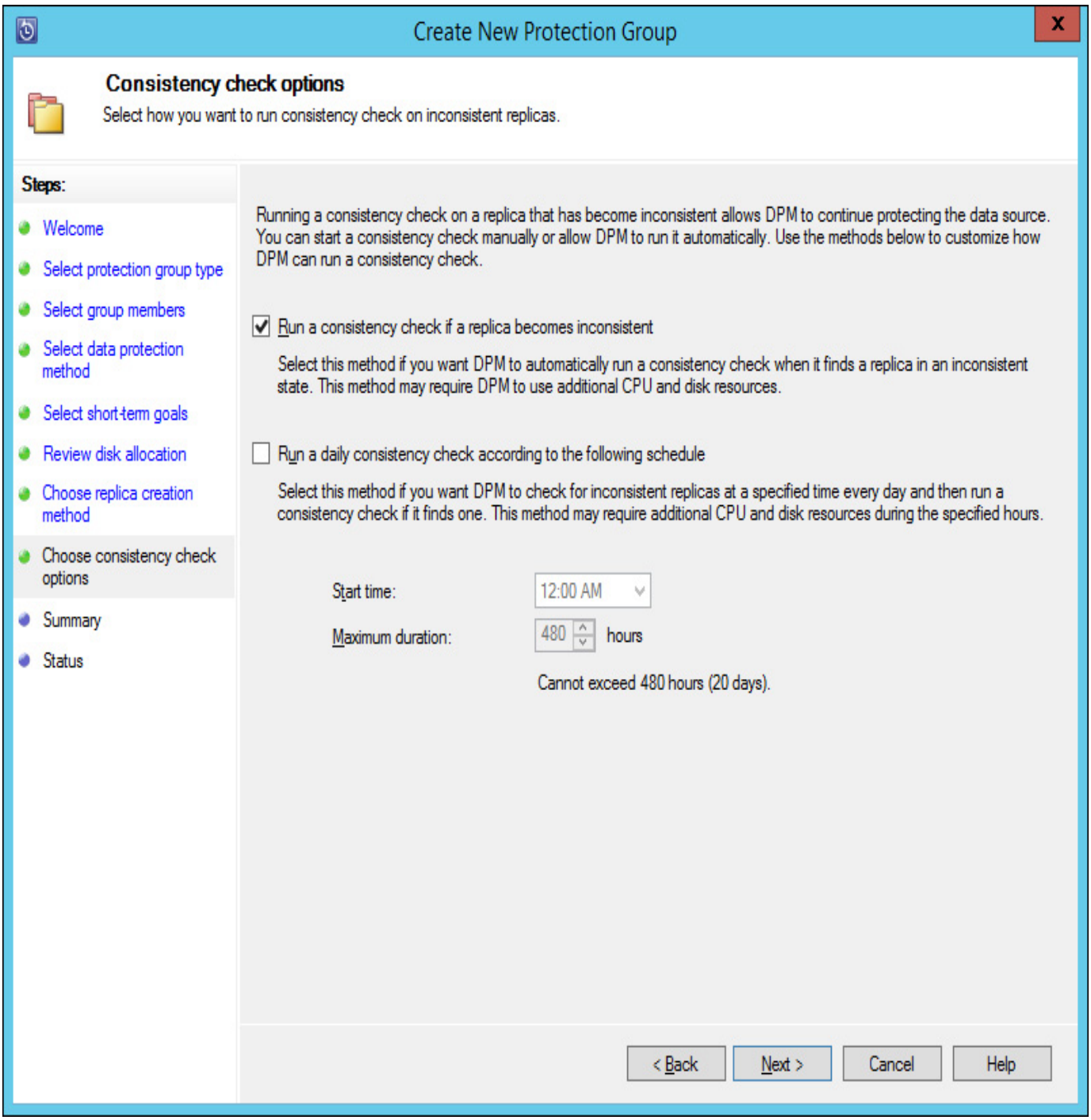

FIGURE 5-58 Consistency check options

9. Complete the wizard to finish creating the new protection group. Figure 5-59 shows the protection group that protects the online VM with an OK protection state.

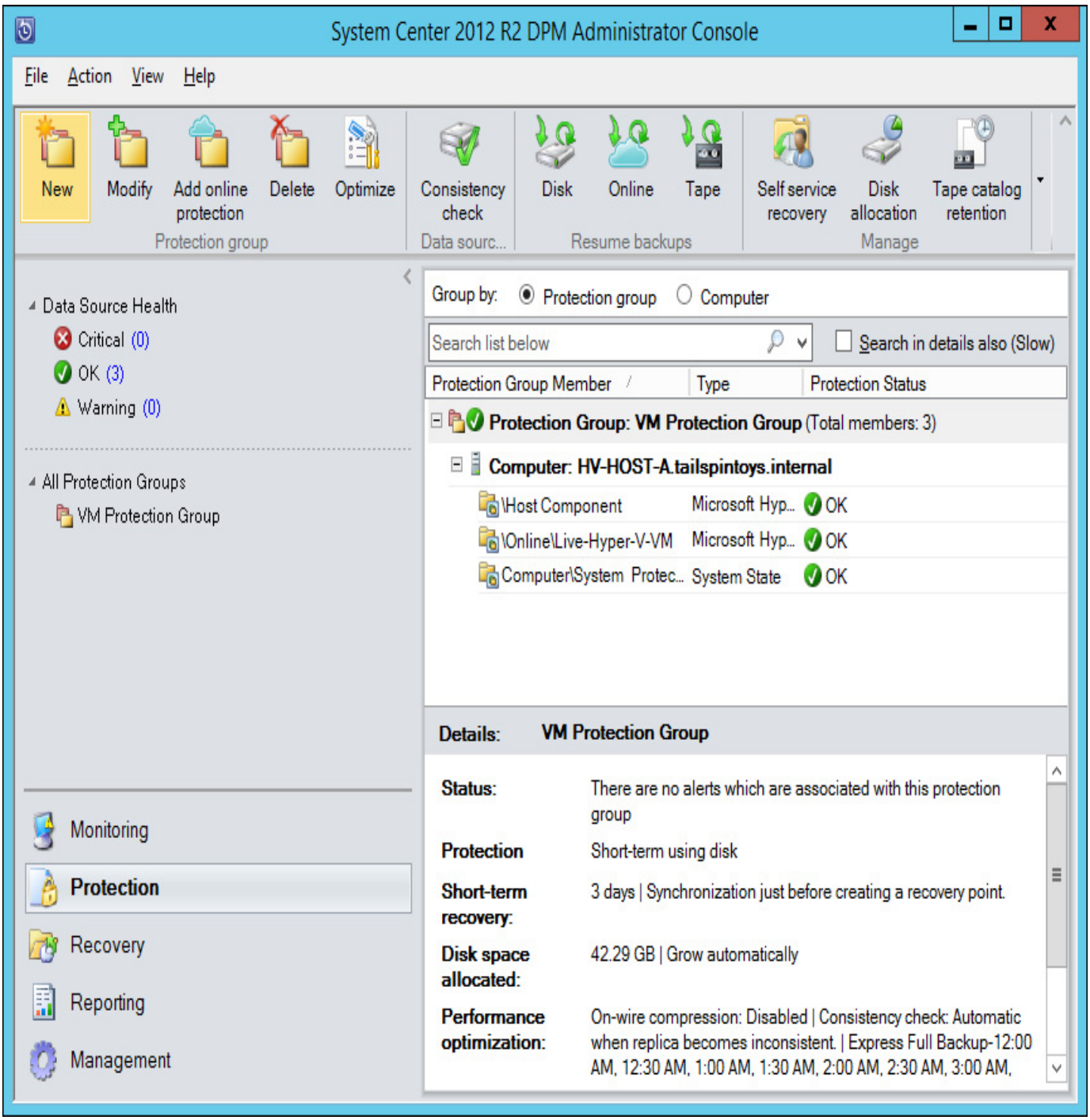

FIGURE 5-59 Protection workspace

More Info: **DPM Protection Groups**

You can learn more about configuring DPM protection groups at *http://technet.microsoft.com/en-us/library/jj628070.aspx*.

Performing recovery

You can use DPM to recover data from any available recovery point. A recovery point, also termed a backup snapshot, is a consistent point-in-time copy of a DPM-protected item, be that a file, folder, database, virtual machine, or an entire computer. The type of data being protected determines your options when it comes to performing recovery. For example, you can recover a SQL Server database to another SQL Server as long as the destination SQL Server has the DPM agent installed. Similarly, you can recover Exchange mailbox databases or Hyper-V virtual machines if they are properly protected to a separate host, as long as the destination host is running the same version of Exchange, SQL, or Hyper-V, and has the DPM agent installed. You also have the option of performing recovery to an alternate location. For example, you might want to only recover a specific file from a protected VM. Rather than restore the entire VM, you can restore the protected file to an accessible file share or local disk.

To recover the contents of protected VM, perform the following steps:

1. In the Recovery workspace of the DPM console, select the item and the recovery point that you wish to restore. Figure 5-60 shows the selection of the 7.00 AM recovery point of the Live-Hyper-V-VM virtual machine. When you have located the recovery point that you wish to restore, click Recover on the ribbon.

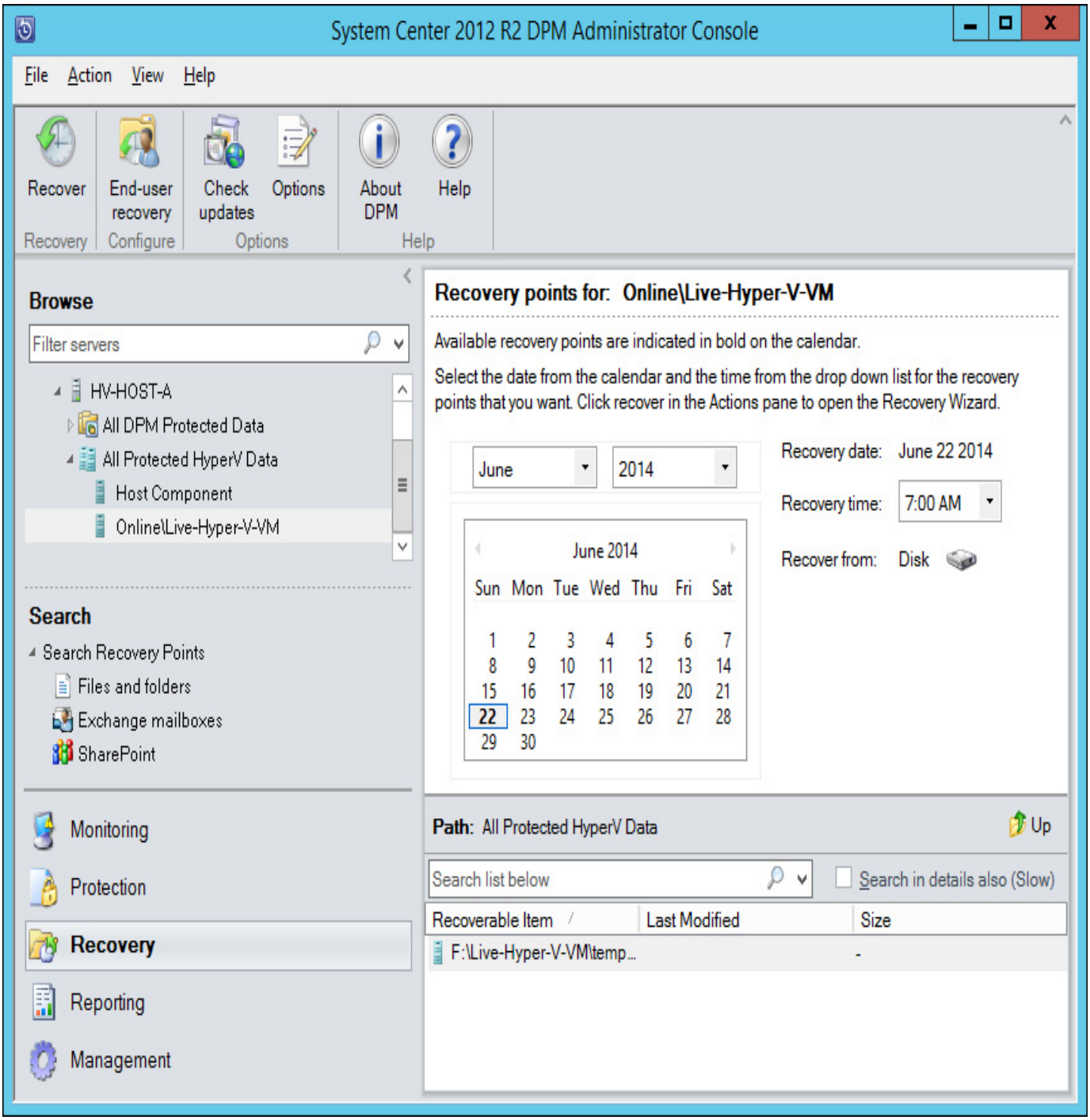

FIGURE 5-60 Recovery workspace

2. On the Select Recovery Type page of the Select Recovery Wizard, select Copy To A Network Folder. If the DPM server has the Hyper-V role installed, you could perform a recovery directly to another server running Hyper-V.
3. On the Specify Destination page, specify the location of a shared folder that will host the recovered files. The destination location must have the DPM agent installed.
4. On the Specify Recovery Options page, select whether you want to apply the security settings of the destination computer or the security settings of the recovery point. You can also configure bandwidth throttling, SAN recovery, and email notification. Figure 5-61 shows the Specify Recovery Options page.

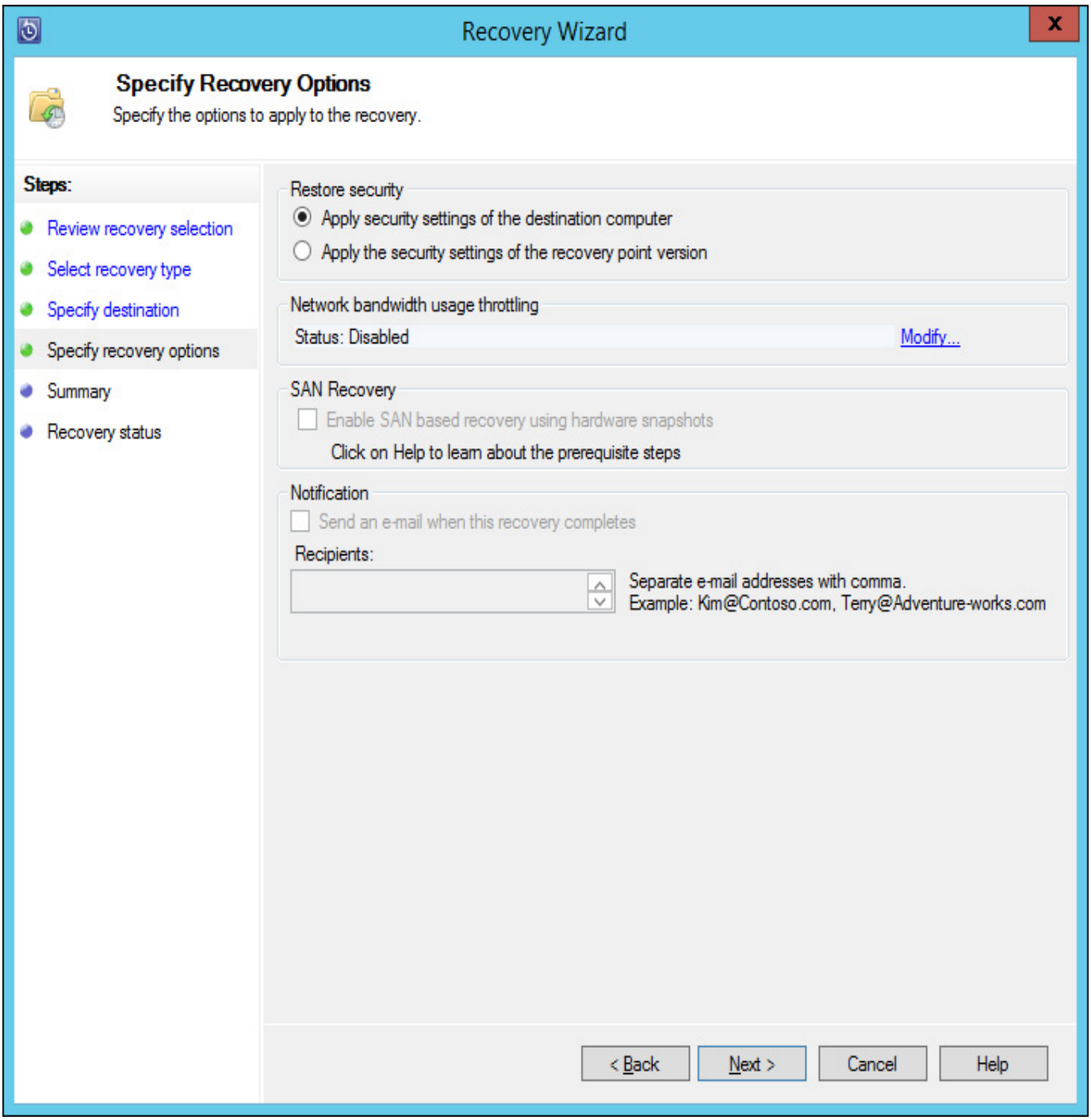

FIGURE 5-61 Specify Recovery Options

5. Complete the wizard by clicking Recover.

More Info: **Recovery Options**

You can learn more about DPM recovery options at *http://technet.microsoft.com/en-us/library/jj628056.aspx*.

Integrating Microsoft Azure Online Backup

Microsoft Azure Online Backup is Microsoft's cloud-based subscription backup service. Microsoft Azure Online Backup can be integrated with DPM, providing a secure off-site data storage and recovery location. Microsoft Azure can store data from DPM for 120 days if you synchronize data every 24 hours, and 60 days if you synchronize data every 12 hours. Your Azure subscription will be charged based on the amount of data stored in the backup vault, but you will not be charged for the bandwidth consumed transferring the data.

To configure DPM to work with Microsoft Azure Online Backup, you need to have performed the following steps:

- Have created a Microsoft Azure account.
- Have created a backup vault within the Microsoft Azure account. Backup vaults allow you to store backup data. Figure 5-62 shows the creation of a backup vault named ExampleVault.

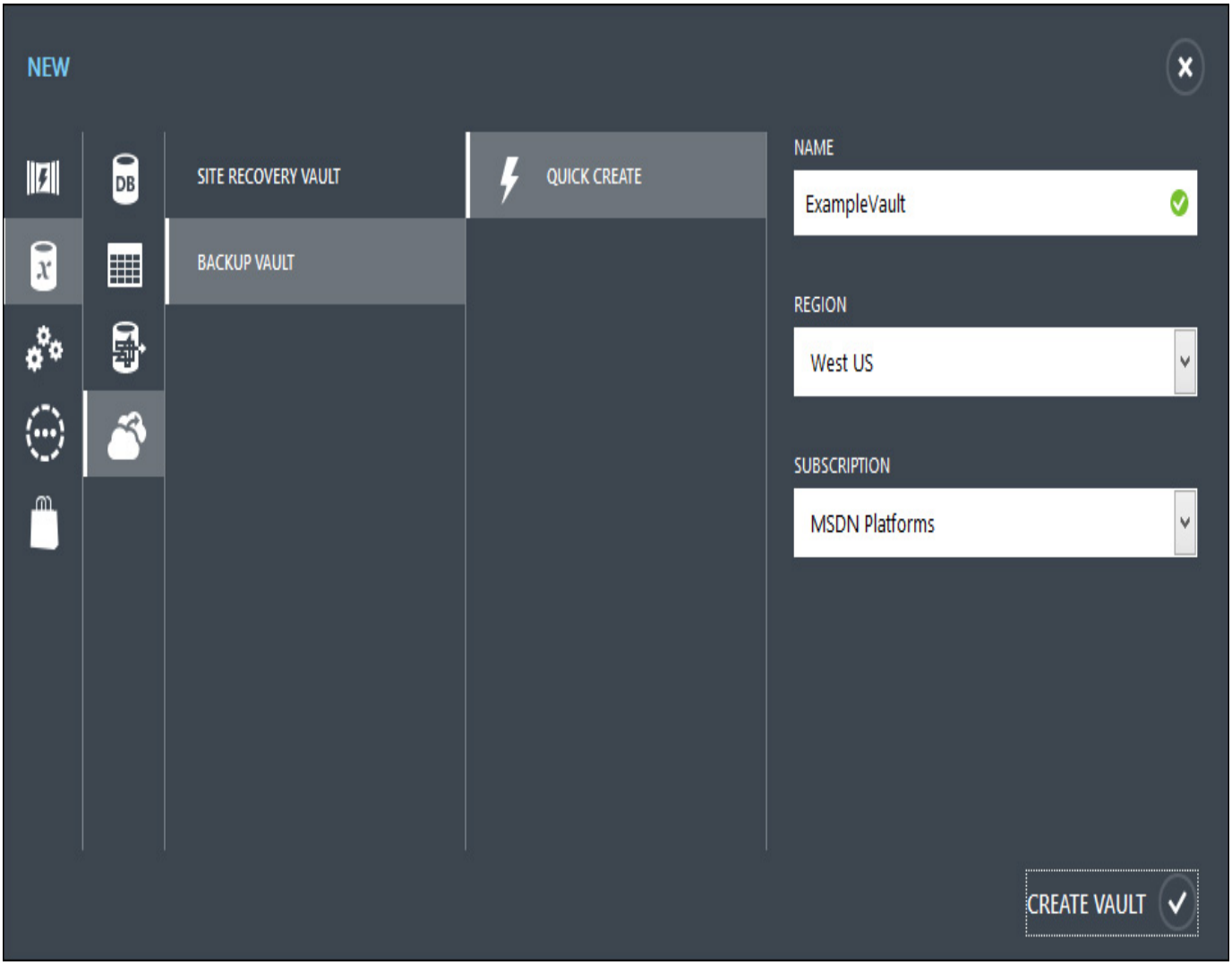

FIGURE 5-62 Create backup vault

- Upload a specially-created certificate that will identify the server to the backup vault, and secure the backup process. You can create this certificate with the makecert.exe utility, generate it using an internal certificate authority, or obtain it from a trusted third party CA.
- Download and install the Microsoft Azure Backup agent to the DPM server. This agent works for both Microsoft Azure Backup, a stand-alone server-based backup solution, and when installed on a System Center 2012 R2 DPM server, integrates with DPM, allowing protected data to be stored in the cloud.

To create a self-signed certificate, download the makecert.exe utility from Microsoft's website and run the following command.

Click here to view code image

```
.\makecert.exe -r -pe -n CN=SYD-DPM -ss my -sr localmachine -eku
1.3.6.1.5.5.7.3.2 -len
2048 -e 01/01/2018 SYD-DPM.cer
```

You replace SYD-DPM with the name of the computer for which you are creating the certificate, and where 01/01/2018 is an appropriate certificate expiry date. Once you've created the certificate, upload it to Microsoft Azure, as shown in Figure 5-63.

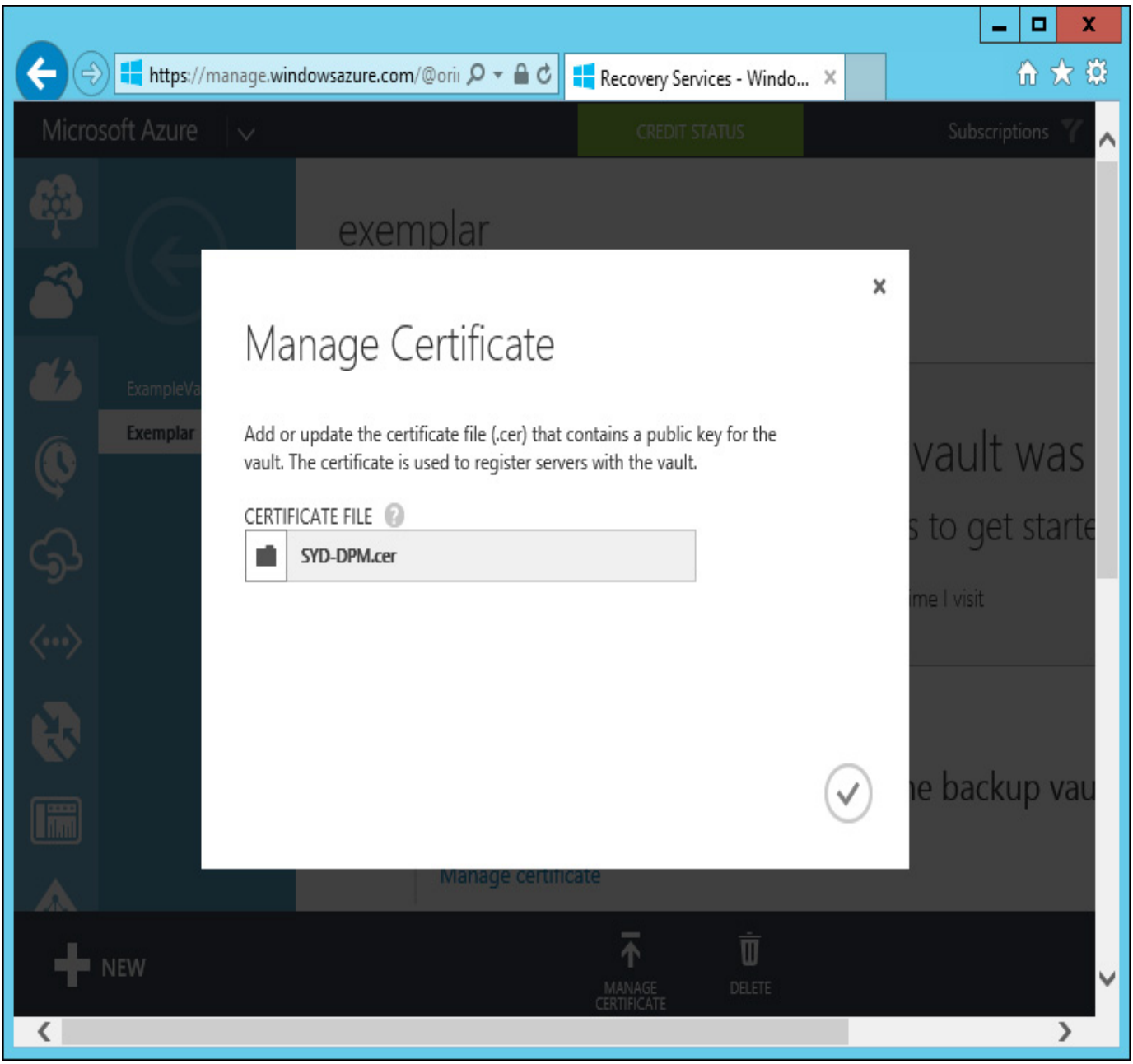

FIGURE 5-63 Manage Certificate

Once the certificate is uploaded, you download the agent and install it on the DPM server, as shown in Figure 5-64.

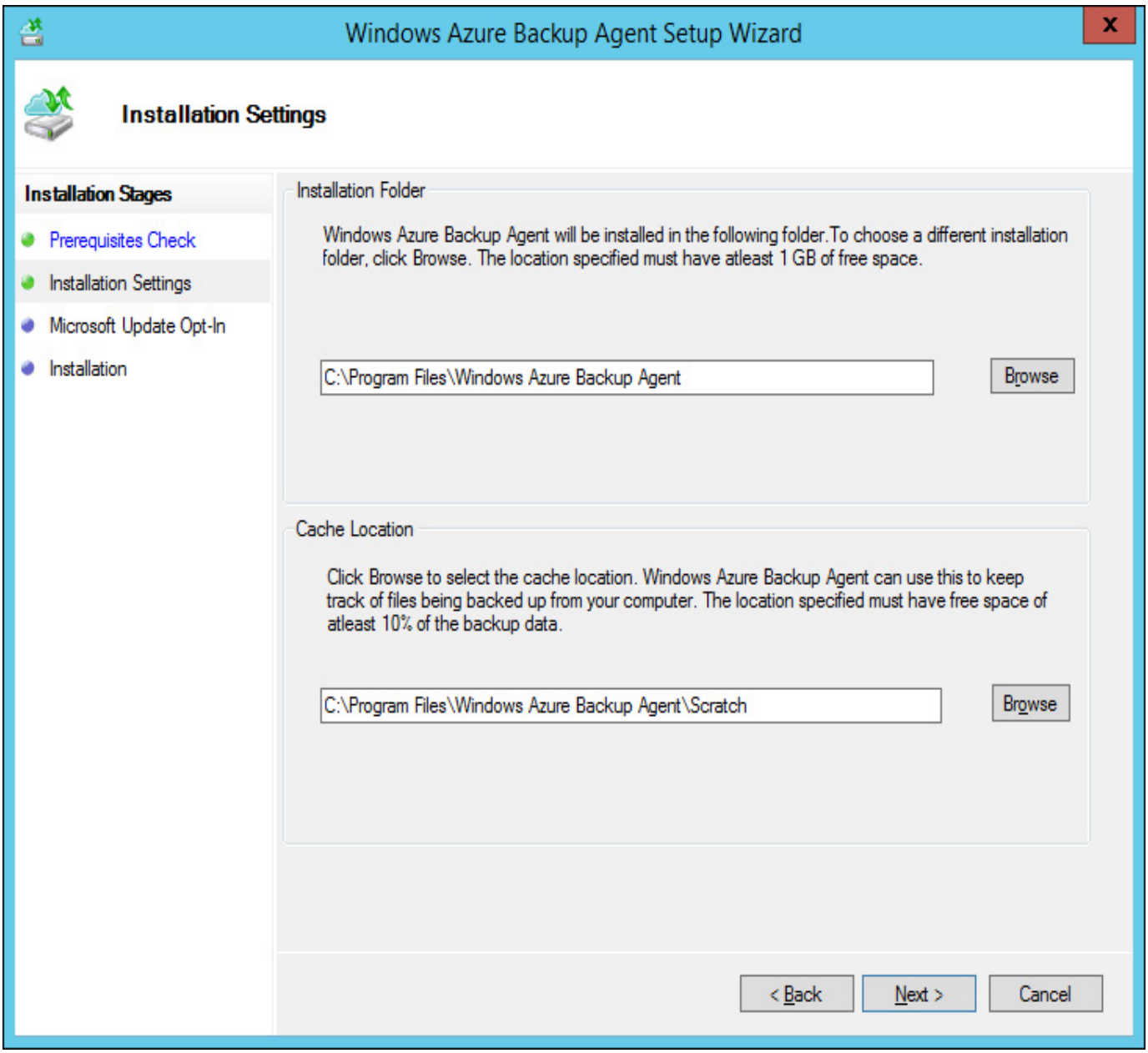

FIGURE 5-64 Windows Azure Backup Agent Setup

Once the agent is installed, you'll need to register the DPM server with Microsoft Azure. To register the DPM server with Microsoft Azure, perform the following steps:

1. In the Management node of the DPM console, click Online. In the ribbon, click Register. This will launch the Register Server Wizard.
2. On the Backup Vault page of the Register Server Wizard, select the management certificate that you uploaded to Microsoft Azure, and then select the name of the backup vault, as shown in Figure 5-65.

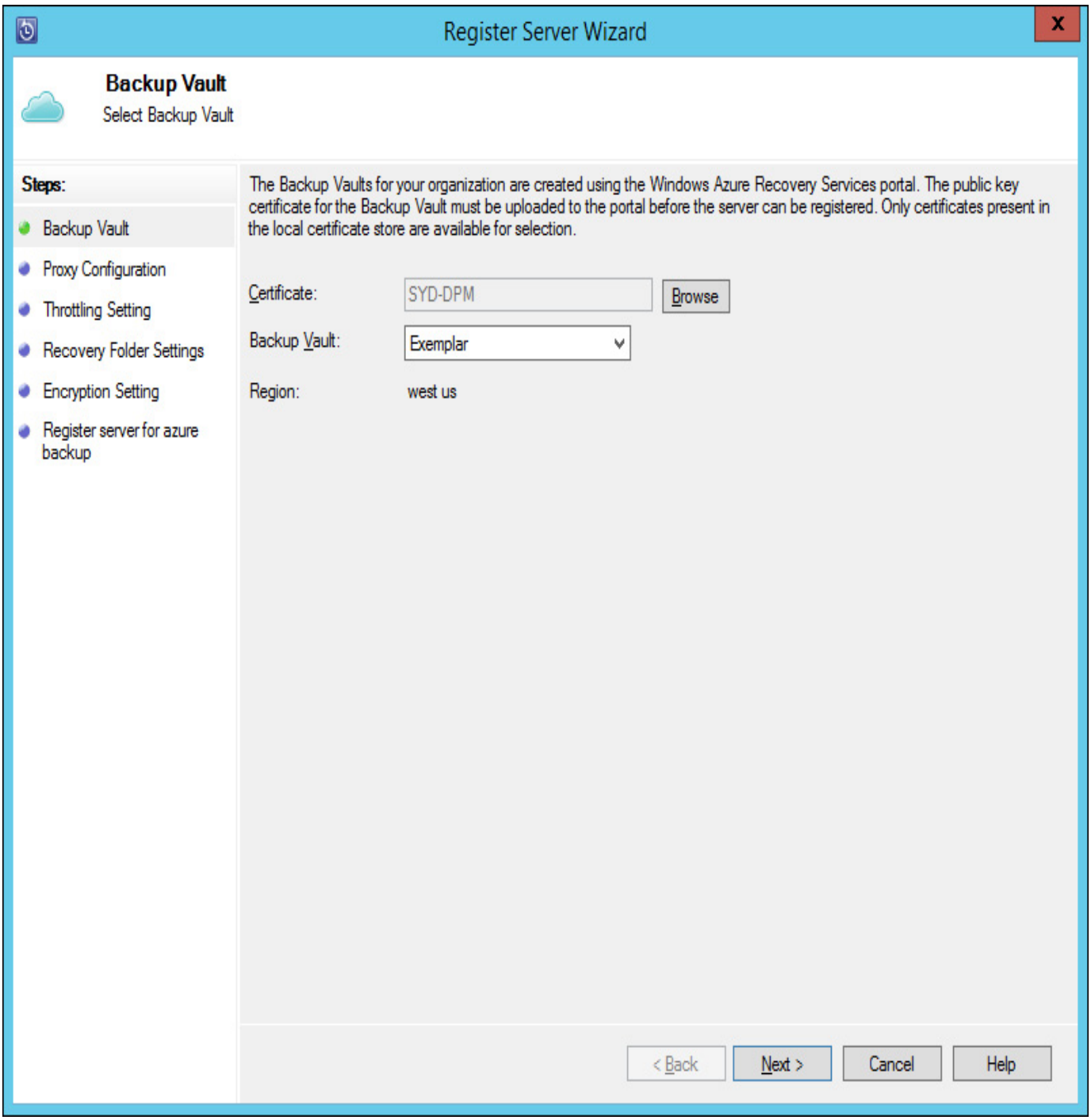

FIGURE 5-65 Backup vault

3. On the Proxy Configuration page, configure any proxy server settings that are required for the DPM server to make a connection to Microsoft Azure.
4. On the Throttling Setting page, shown in Figure 5-66, specify any bandwidth throttling settings that should apply when protected data is being transferred to Microsoft Azure. You can configure throttling settings for work hours and non-work hours.

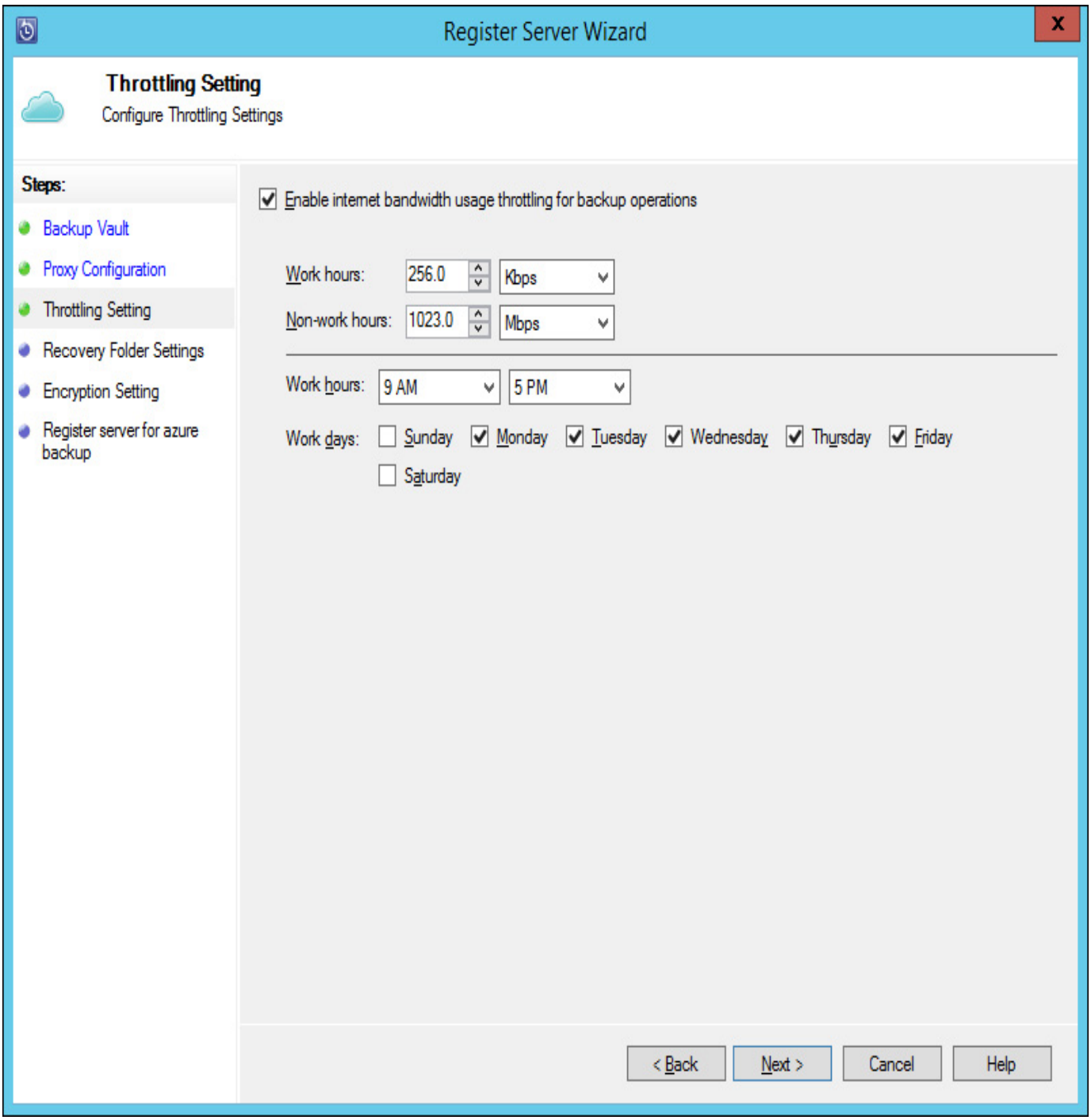

FIGURE 5-66 Throttling Setting

5. On the Recovery Folder Settings page, specify a location that the DPM server can use as temporary storage space before being transferred to the final recovery location. This location needs to have enough storage space to store this temporary data.
6. On the Encryption Settings page, provide a 16 character long passphrase. This passphrase will be used to encrypt backed up data. You need this passphrase to recover data from Microsoft Azure when recovering using a difference instance of DPM. The Encryption Setting page of the wizard is shown in Figure 5-67.

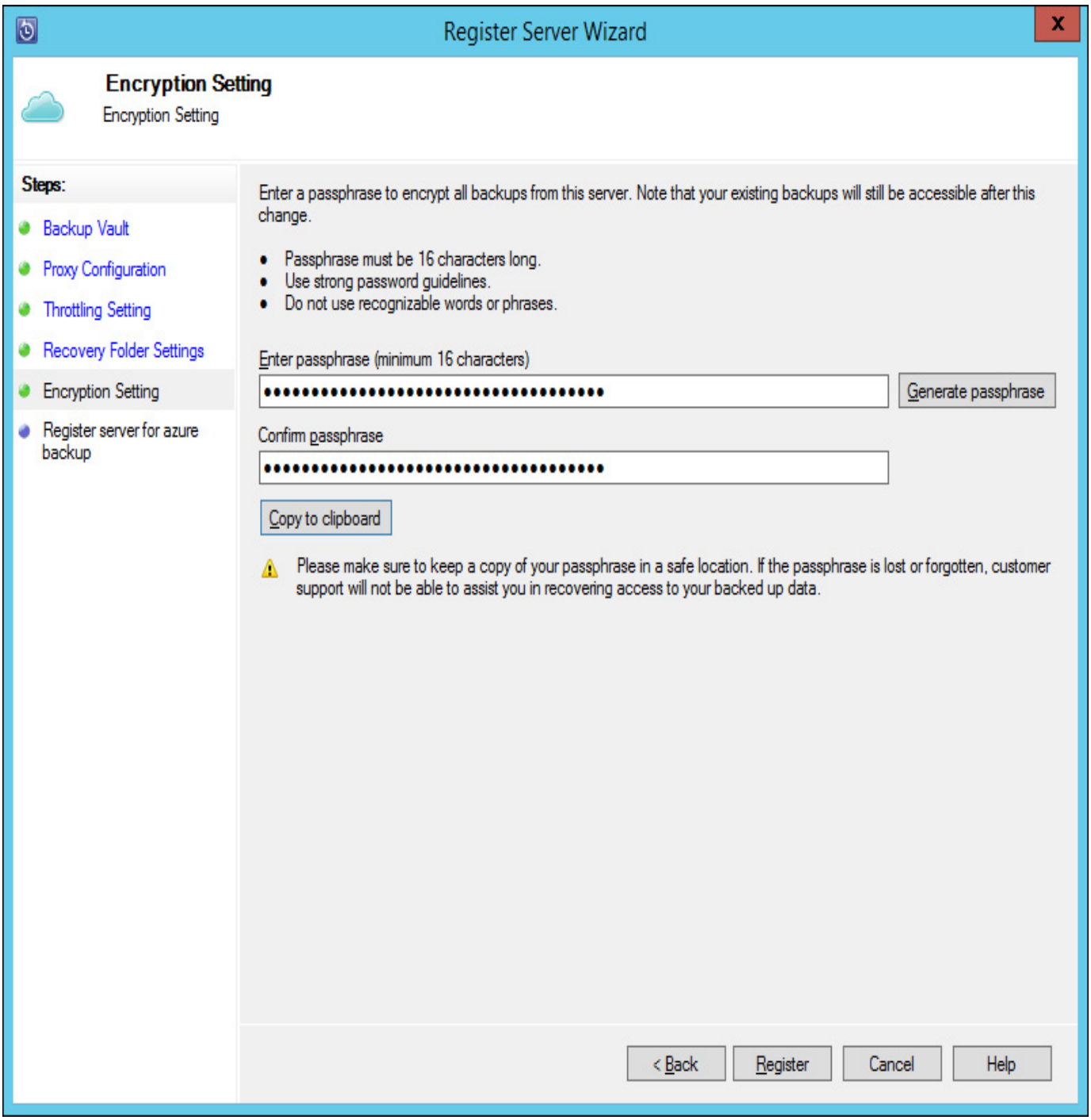

FIGURE 5-67 Encryption Setting

Once you have registered the DPM server with Microsoft Azure, you will be able to select the online protection option when creating or modifying a protection group, as shown in Figure 5-68.

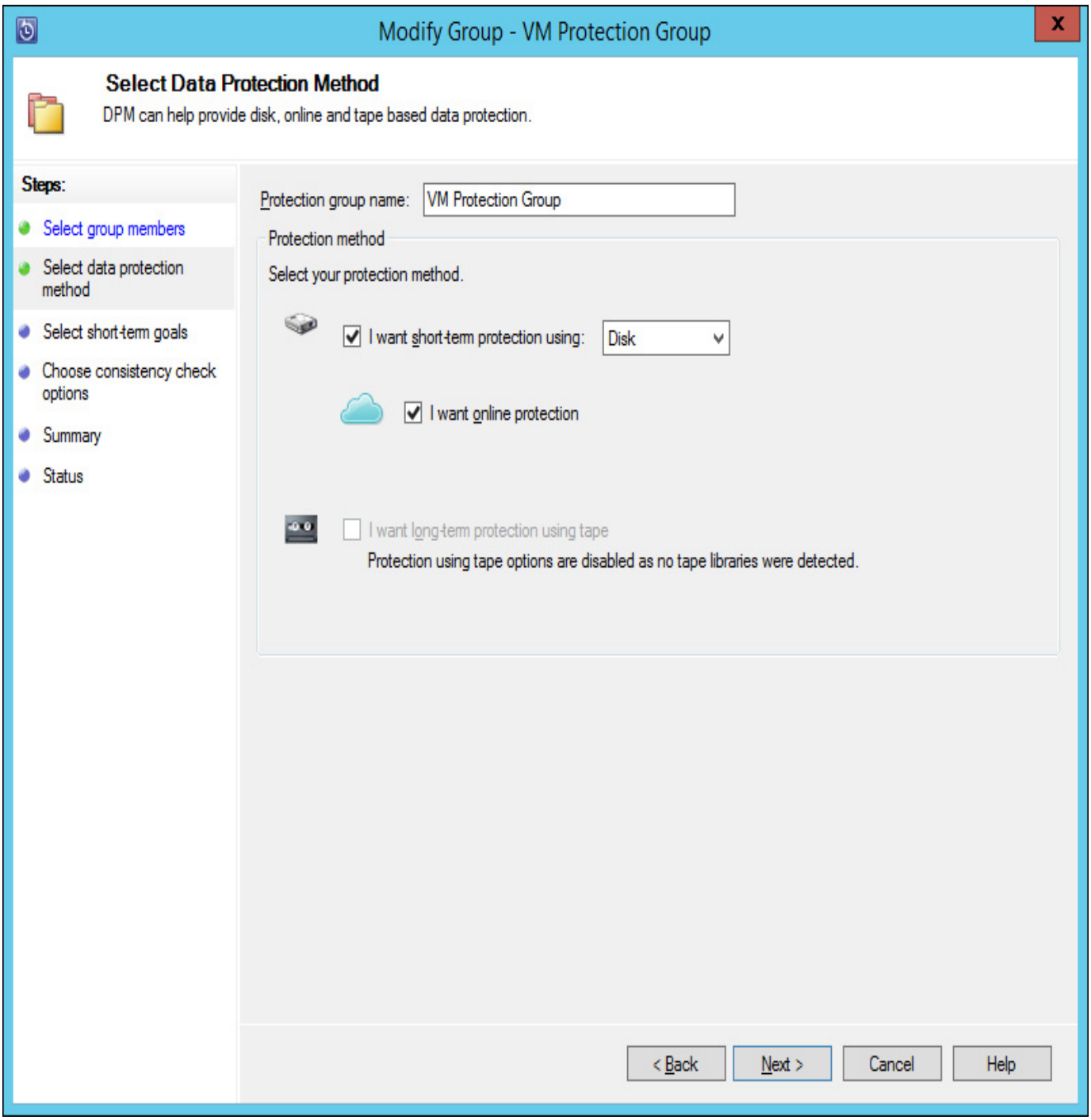

FIGURE 5-68 Select data protection method

Once you select the online protection option, you'll be able to configure which protection group data you want to protect. You can protect only a subset of the data protected by the protection group, rather than having to replicate all of the protected data to Microsoft Azure. Figure 5-69 shows the Online Protection Goals page of the wizard.

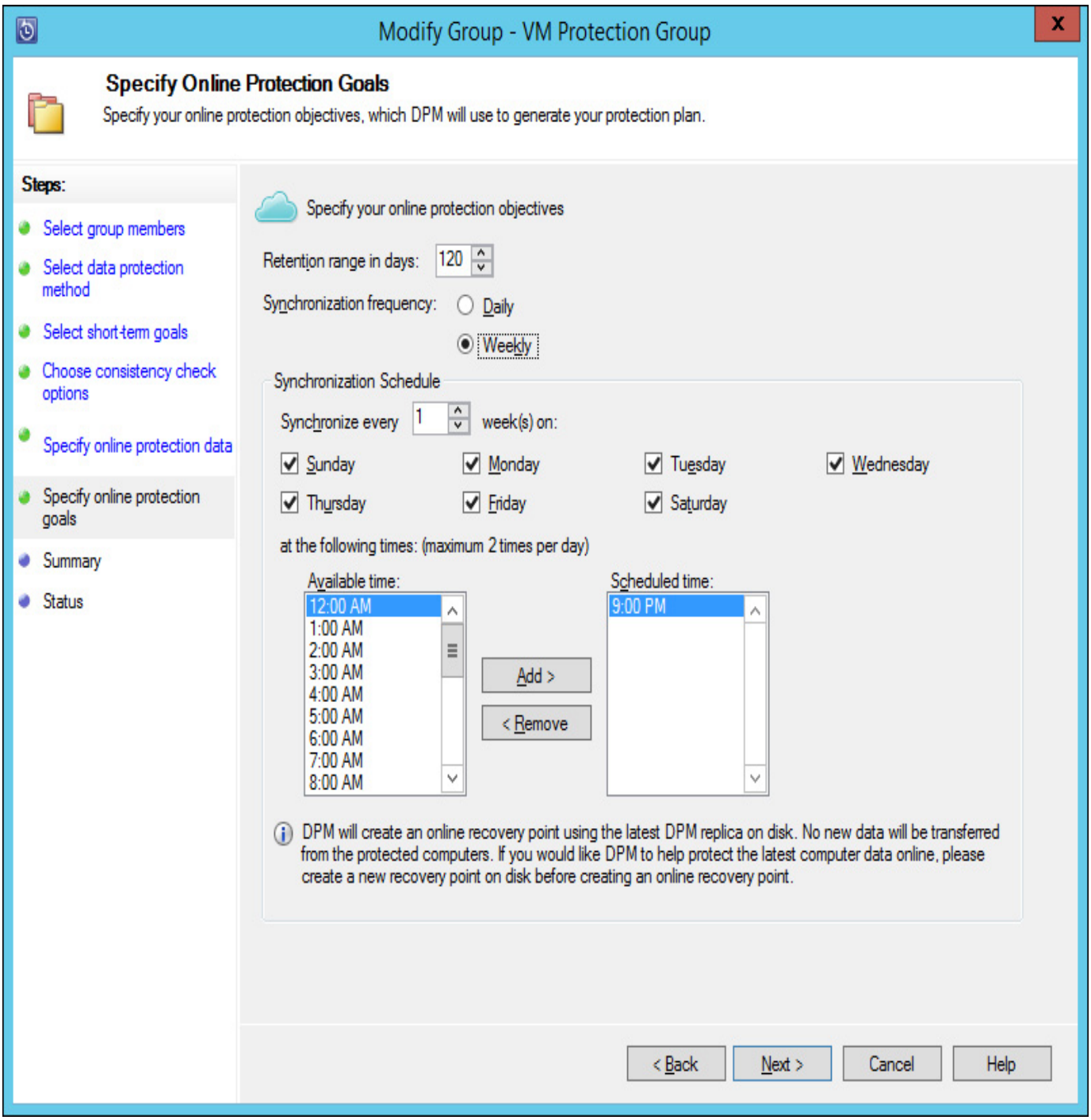

FIGURE 5-69 Online protection goals

You can force the creation of an online protection recovery point from the Protection workspace, as shown in Figure 5-70.

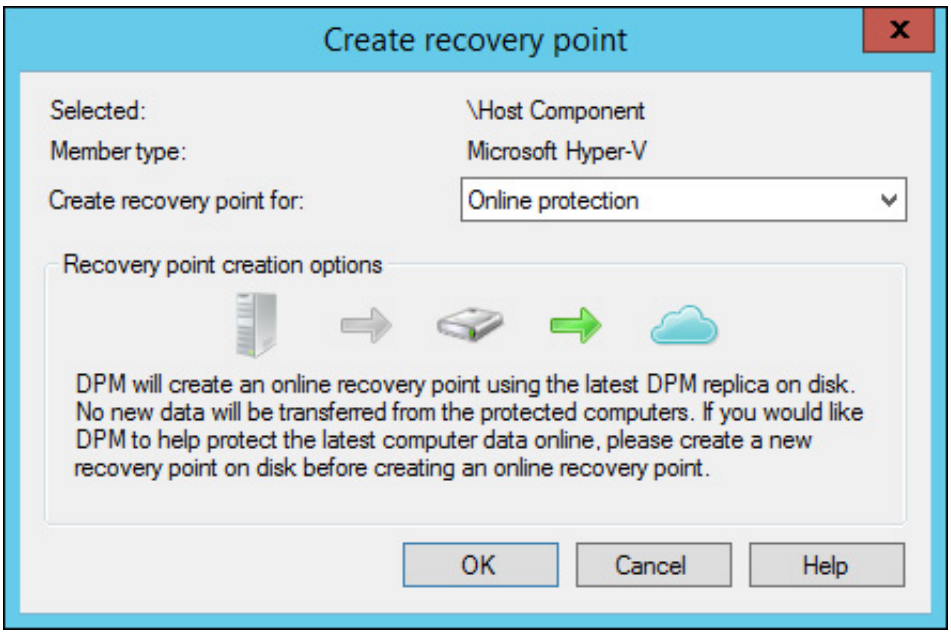

FIGURE 5-70 Create Recovery Point

To recover from Microsoft Azure backup, specify an online recovery point, as shown in Figure 5-71, and perform recovery normally.

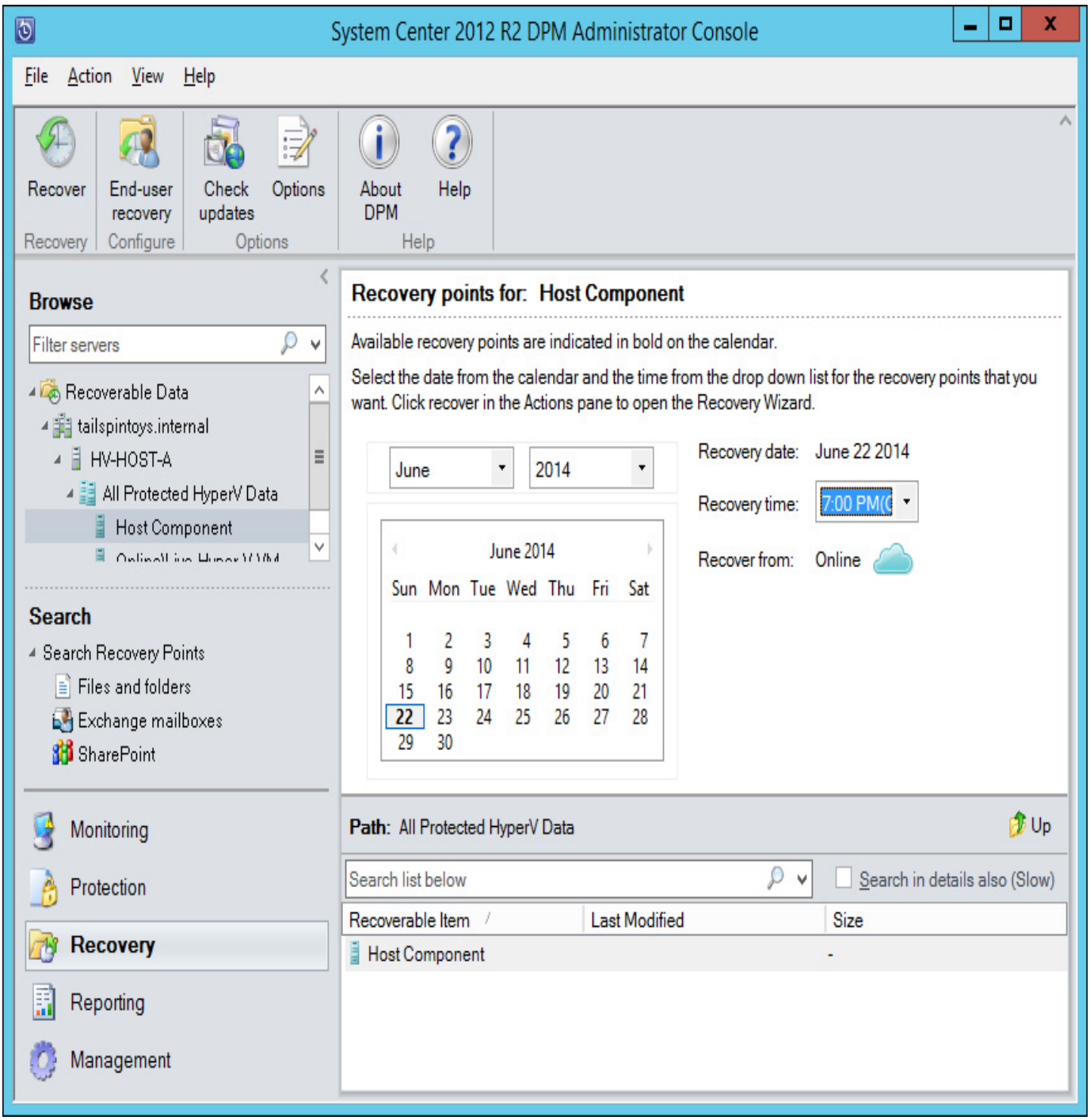

FIGURE 5-71 Online recovery

More Info: **Azure Backup**

You can learn more about configuring Microsoft Azure Online Backup at *http://technet.microsoft.com/en-us/library/jj728752.aspx*.

Using DPM Orchestrator integration pack

You can use the DPM integration pack for Orchestrator, shown in Figure 5-72, to create DPM specific runbook automation. These activities allow you to automate the following tasks when creating an Orchestrator runbook:

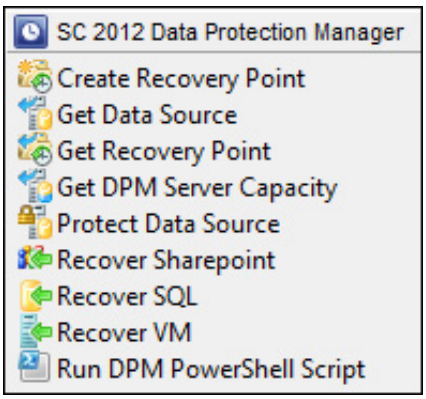

FIGURE 5-72 Orchestrator activities

- **Create Recovery Point** Use this activity to create a recovery point for a specific data source.
- **Get Data Source** Use this activity to determine information about available data sources.
- **Get Recovery Point** Use this activity to determine which recovery points exist for a specific protected data source.
- **Get DPM Server Capacity** Use this activity to determine a DPM server's capacity.
- **Protect Data Source** Use this activity to put a data source into protection. Use the Get Data Source activity to determine the identity of eligible data sources.
- **Recover Sharepoint** Use this activity to recover Sharepoint data.
- **Recover SQL** Use this activity to recover SQL data.
- **Recover VM** Use this activity to recover a protected virtual machine.
- **Run DPM PowerShell Script** Use this activity to run a DPM PowerShell script. You can use the information returned from this script in the Orchestrator runbook.

More Info: **DPM Integration Pack**

You can learn more about the DPM integration pack at *http://technet.microsoft.com/en-us/library/hh830694.aspx*.

Exam Tip

Remember what steps you need to take to configure a DPM server so that it can write protected data to Microsoft Azure.

***Thought experiment*: Data protection at Contoso**

You are in the process of planning data protection infrastructure for Contoso's private cloud deployment. You are researching how you will deploy and configure System Center 2012 R2 Data Protection Manager. As part of your planning, you want to know what steps you should take after deploying the DPM server before you can create protection groups. You're also interested in moving data to the cloud or another offsite location.

1. What steps do you need to take before adding virtualization hosts to DPM protection groups?
2. What steps could you take to ensure protected data is stored offsite?

Objective summary

- DPM requires agents to be deployed to servers that host data requiring protection.
- You need to add disks to a DPM storage pool before you can configure a protection group.
- DPM protection groups determine what is backed up, to where it is backed up, how often it is backed up, and how long it will remain backed up.
- You can integrate DPM with Microsoft Azure, allowing you to store protected data off site in the Microsoft Cloud.
- You can use the DPM integration pack for Orchestrator to create runbooks with DPM activities.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which DPM integration pack activity would you use with an Orchestrator runbook to generate a list of recovery points?
   - **A.** Create Recovery Point
   - **B.** Get Data Source
   - **C.** Get Recovery Point
   - **D.** Protect Data Source
2. You are planning on synchronizing data from a DPM protection group to a Microsoft Azure backup vault. You want to perform one synchronization per day. What is the maximum data retention period available given these conditions?
   - **A.** 60 days
   - **B.** 90 days
   - **C.** 120 days
   - **D.** 150 days
3. You have been using DPM to protect several Hyper-V virtualization hosts, as well as the VMs that they host. You want to recover a protected VM to a different Hyper-V virtualization host than the one it was originally hosted on. Which of the following conditions must the destination Hyper-V host meet?
   - **A.** The host must have the DPM agent installed.
   - **B.** The host must be running the same version of Hyper-V.
   - **C.** The host must have the Operations Manager agent installed.
   - **D.** The host must have the Configuration Manager agent installed.

Answers

This section contains the solutions to the thought experiments and answers to the lesson review questions in this chapter.

Objective 5.1: Thought experiment

1. You should deploy a System Center Advisor gateway server to collect traffic from servers on the internal network and forward it to the System Center Advisor servers in the cloud.
2. You need to connect via web browser to the System Center Advisor console hosted in the cloud.

Objective 5.1: Review

1. **Correct answers:** A, B, and C
   - **A. Correct**: You can add configuration items to compliance baselines.
   - **B. Correct**: You can add existing compliance baselines to new compliance baselines.

C. **Correct**: You can add software updates to configuration baselines.

D. **Incorrect**: Update baselines are used with VMM and not with Configuration Manager baselines.

2. **Correct answers:** A, B, and C

A. **Correct**: The System Center Process Pack for IT GRC requires an existing deployment of Configuration Manager, Operations Manager, and Service Manager.

B. **Correct**: The System Center Process Pack for IT GRC requires an existing deployment of Configuration Manager, Operations Manager, and Service Manager.

C. **Correct**: The System Center Process Pack for IT GRC requires an existing deployment of Configuration Manager, Operations Manager, and Service Manager.

D. **Incorrect**: The System Center Process Pack for IT GRC requires an existing deployment of Configuration Manager, Operations Manager, and Service Manager.

3. **Correct answers:** A, C, and D

A. **Correct**: The System Center Process Pack for IT GRC requires that Service Manager be configured with the Active Directory, Operations Manager, and Configuration Manager connectors.

B. **Incorrect**: The System Center Process Pack for IT GRC requires that Service Manager be configured with the Active Directory, Operations Manager, and Configuration Manager connectors.

C. **Correct**: The System Center Process Pack for IT GRC requires that Service Manager be configured with the Active Directory, Operations Manager, and Configuration Manager connectors.

D. **Correct**: The System Center Process Pack for IT GRC requires that Service Manager be configured with the Active Directory, Operations Manager, and Configuration Manager connectors.

Objective 5.2: Thought experiment

1. You configure the Specify intranet Microsoft update service location policy to configure a computer with the address of the WSUS server.
2. You assign computers to WSUS computer groups using the Enable client-side targeting policy.

Objective 5.2: Review

1. **Correct answers:** A and C

A. **Correct**: You need to create a software update group.

B. **Incorrect**: You create update baselines when using software updates with VMM, not with Configuration Manager.

C. **Correct**: You need to download the updates and create a deployment package prior to deploying the updates.

D. **Incorrect**: You don't need to create an automatic approval rule prior to deploying the updates.

2. **Correct answers:** A and C

A. **Correct**: You add software updates to update baselines in VMM.

B. **Incorrect**: You use Software Update Groups with Configuration Manager, not with VMM.

C. **Correct**: You can assess compliance by assigning update baselines to virtualization hosts.

D. **Incorrect**: You don't assign software update groups in VMM, you deploy them in Configuration Manager.

3. **Correct answers:** B and C

A. **Incorrect**: The VMST is not supported for System Center 2012 R2 Virtual Machine Manger. Instead, you use a service management automation runbook to update offline VM images in

the VMM library.

B. **Correct**: You use a service management automation runbook to update offline VM images in the VMM library.

C. **Correct**: The service management automation runbook interacts with WSUS to obtain updates that can be applied to offline VM images in the VMM library.

D. **Incorrect**: You don't use Configuration Manager to perform offline updates of virtual machine images in the VMM library.

Objective 5.3: Thought experiment

1. You need to deploy protection agents to the virtualization hosts. You also need to create a storage pool.
2. You could connect the DPM instance to Microsoft Azure, which allows you to store a copy of protected data in an offsite location. Although not discussed in the text, you can also create a DPM replica in another site.

Objective 5.3: Review

1. **Correct answer:** C
   A. **Incorrect:** The Create Recovery Point activity allows you to create a new recovery point.
   B. **Incorrect**: The Get Data Source activity provides information about available data source.
   C. **Correct**: The Get Recovery Point activity allows you to generate a list of recovery points.
   D. **Incorrect**: The Protect Data Source activity allows you to protect a specific data source.
2. **Correct answer:** C
   A. **Incorrect**: With one synchronization per day, Microsoft Azure, when integrated with DPM, supports a maximum data retention period of 120 days.
   B. **Incorrect**: With one synchronization per day, Microsoft Azure, when integrated with DPM, supports a maximum data retention period of 120 days.
   C. **Correct**: With one synchronization per day, Microsoft Azure, when integrated with DPM, supports a maximum data retention period of 120 days.
   D. **Incorrect**: With one synchronization per day, Microsoft Azure, when integrated with DPM, supports a maximum data retention period of 120 days.
3. **Correct answers:** A and B
   A. **Correct**: You can only restore a VM in its entirety to a Hyper-V host that has the DPM agent installed.
   B. **Correct**: You can't restore a VM to a host if it is running an earlier version of Hyper-V.
   C. **Incorrect**: Only the DPM agent is required.
   D. **Incorrect**: Only the DPM agent is required.

Prev
Chapter 4. Configure and maintain service management
Next
Index