Skip to content

Chapter 3. Monitor resources

On a day-to-day basis, an Operations Manager administrator needs to manage and respond to alerts, ensuring that they are notified about particularly important events that have occurred with the items that they are monitoring. They also need to be familiar with the variety of ways that Operations Manager displays collected data, knowing which dashboards and views are going to provide the most meaningful insight into the health and performance of the objects that they are responsible for monitoring.

Objectives in this chapter:

Objective 3.1: Monitor network devices

Once you have configured Operations Manager to collect data from network data, you need to configure how Operations Manager displays and interprets that data, from configuring notifications and alerts, through to analyzing overall network health. In the previous chapter you learned how to set up synthetic transactions, how to monitor network devices and how to perform device discovery. In this section you'll learn about managing alerts as well as how to view network devices and data.

This section covers the following topics:

- Managing alerts
- Configuring alert notifications
- Analyzing network devices and data

Managing alerts

Rules and monitors generate Operations Manager alerts. You view alerts in the Monitoring workspace shown in Figure 3-1. Rules and monitors can be configured to trigger an alert when certain sets of conditions are encountered. For example, an alert might be generated if a specific event is written to an event log of a monitored device or server, or when a monitored port on a network device surpasses a specific error threshold. Not all rules and monitors generate alerts. Alerts are raised by all types of monitored objects and aren't specific to network devices. However, rather than provide the same coverage across the different sections of this chapter, managing alerts is covered in this first section in a way that is universal to the way alerts are dealt with across all of the different objects you can monitor with Operations Manager.

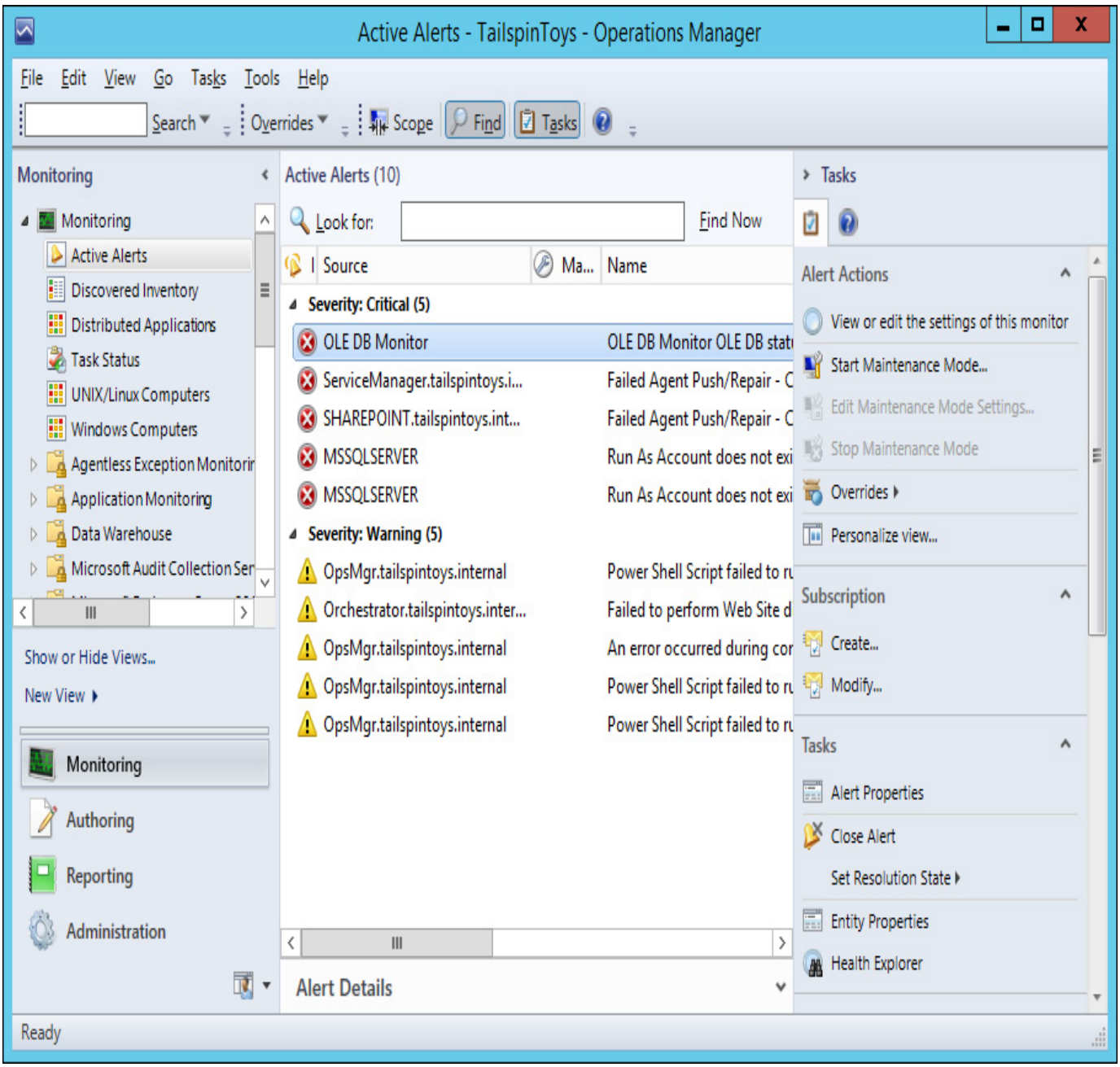

FIGURE 3-1 Active Alerts

You can configure a monitor to create an alert when the monitored item's health state changes from healthy (green) to warning (yellow), or from healthy to critical (red). An alert is only sent if the state changes from warning to critical, if the original alert sent when the monitor changed from healthy to warning has been closed. Alerts are not sent if the health state changes from warning or critical to healthy, but will again be sent if, once returned to healthy, the state changes again to warning or critical.

The majority of alerts generated by monitors automatically resolve when the monitor returns to a healthy state. If an alert does not automatically resolve when a monitor returns to a healthy state, you can ensure that it will in the future by configuring an override on the Auto-Resolve Alert parameter for the monitor. Figure 3-2 shows the configuration of an override for the Auto-Resolve Alert parameter on a monitor named Security.

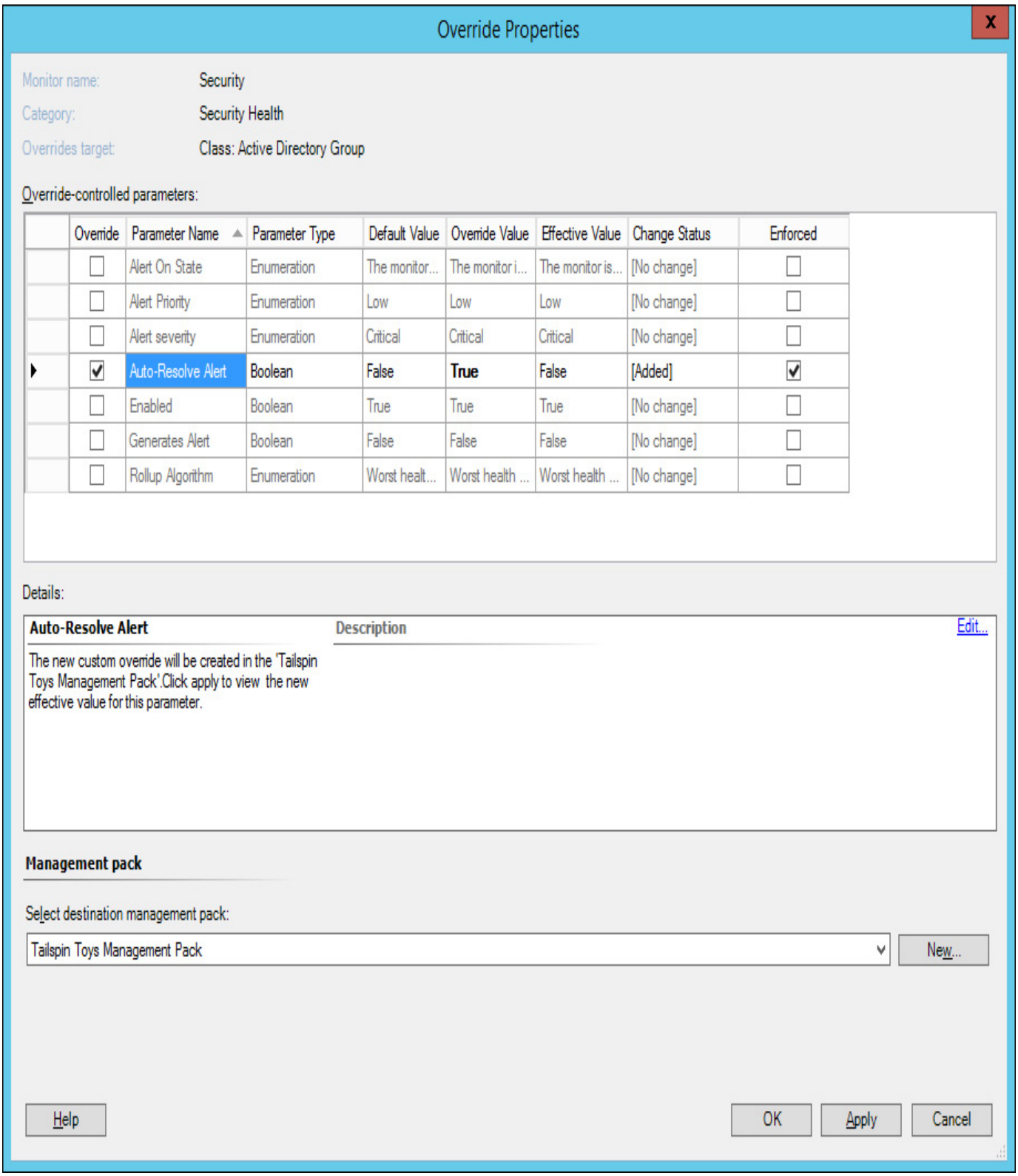

FIGURE 3-2 Override auto-resolve

Just as it is possible to configure a monitor that sends alerts with an override to stop it from sending alerts, it is also possible to configure a monitor that does not send alerts by default with an override so that it does send alerts.

Rules and monitors handle alerts differently. Rules cannot automatically resolve alerts. Unlike a monitor, that will send one alert while the condition that caused the alert is present, rules will continue to send alerts while the condition that caused the alert is present. To deal with the potential flood of alerts, you can configure alert suppression for the rule during rule creation. When you configure alert suppression, only the initial alert will be sent. Further alerts will be suppressed. Operations Manager will only suppress duplicate alerts that have suppression criteria, specified in the rule, that are identical. To be tagged as a duplicate, an alert must be created by the same rule and be in an unresolved state.

Exam Tip

You can only configure alert suppression during rule creation. You can't configure alert suppression as an override.

To view the number of suppressed alerts for a particular alert, you can add the Repeat Count column to the Active Alerts view. The repeat count will be incremented each time a new alert is suppressed. Figure 3-3 shows the Repeat Count column, with a figure of 307 for the first alert from MSSQLSERVER.

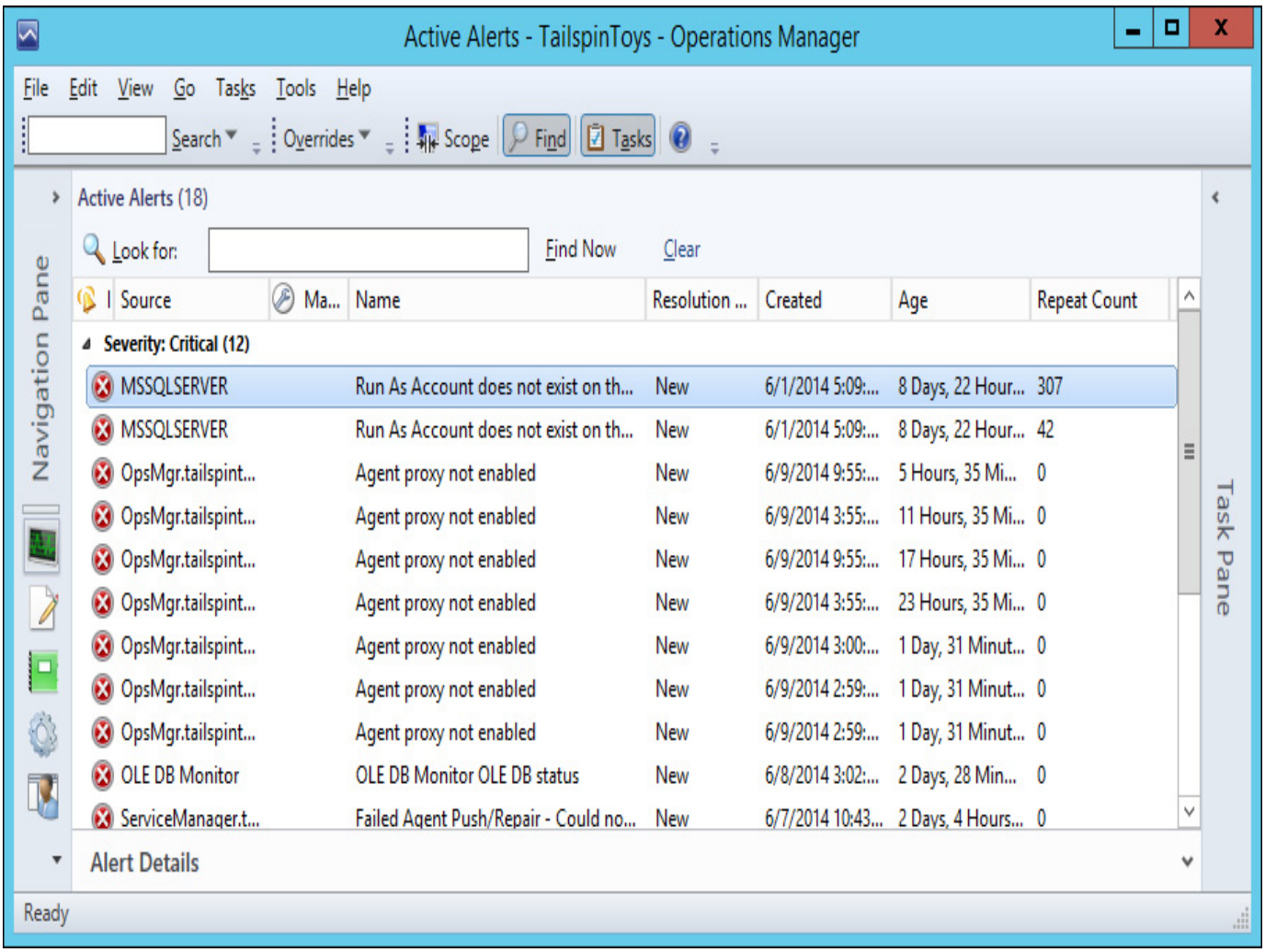

FIGURE 3-3 Repeat count

More Info: **Alert Creation**

You can learn more about alert creation at *http://technet.microsoft.com/en-us/library/hh212847.aspx*.

Alert details

Viewing the details of an alert is straightforward. Locate the alert in the Active Alerts node of the Monitoring workspace, and then click Alert Properties. This will bring up the Alert Properties dialog box, an example of which is shown in Figure 3-4. The General tab will provide information about the alert source, severity, priority, and repeat count in the event that the error has occurred more than once.

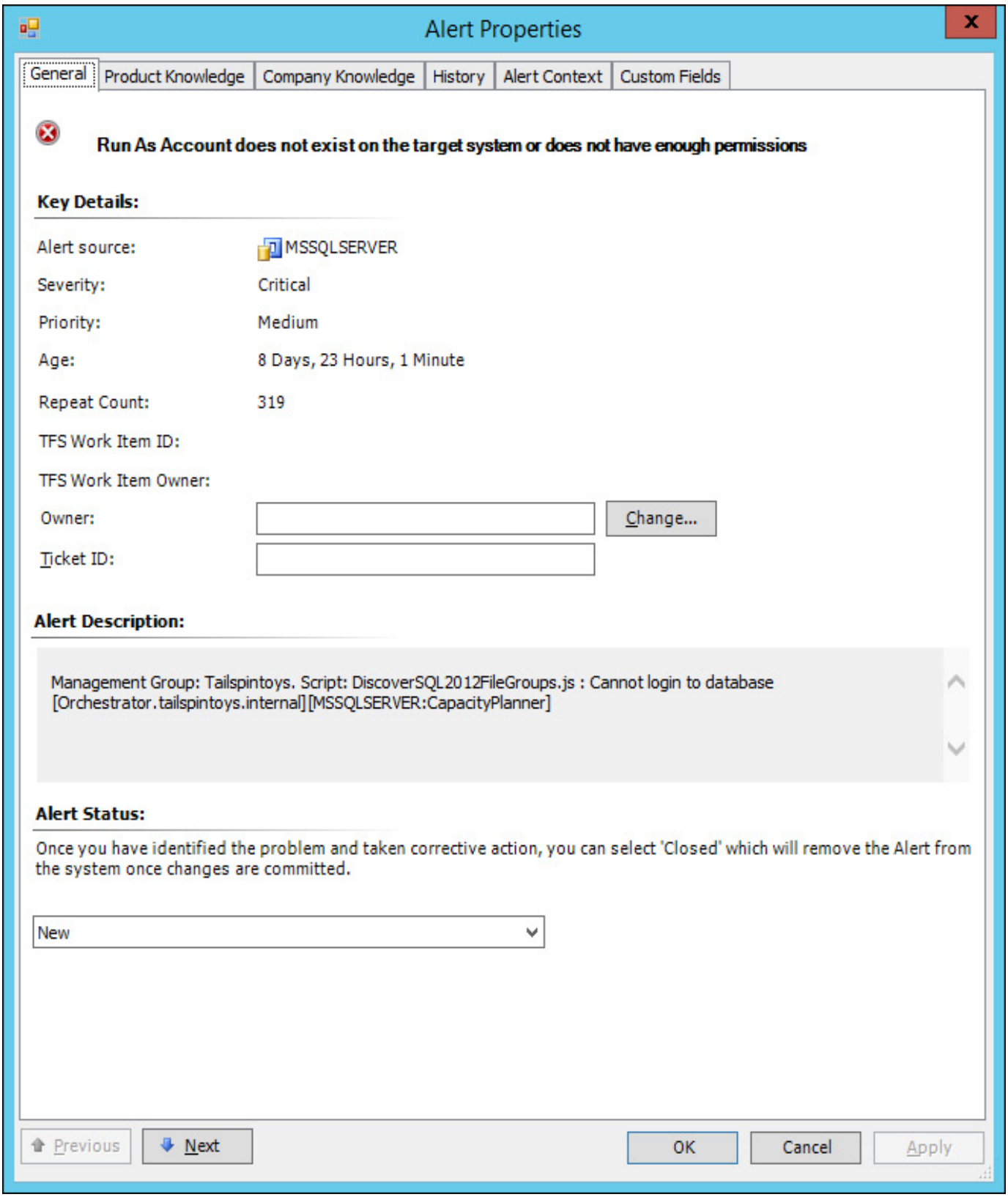

FIGURE 3-4 Alert properties

The Alert Properties dialog box also has the following information:

- The Product Knowledge tab will provide you with a summary of the alert, information about the causes of the alert, and possible resolution steps that you could implement.
- The Company Knowledge tab allows you to edit the rule that triggered the alert, and add extra information about the alert.
- The History tab allows you to enter history information in the form of comments about the alert.
- The Context tab provides further detail, including Log Name, Source, Event Number, Level, and Logging Computer, and is shown in Figure 3-5.

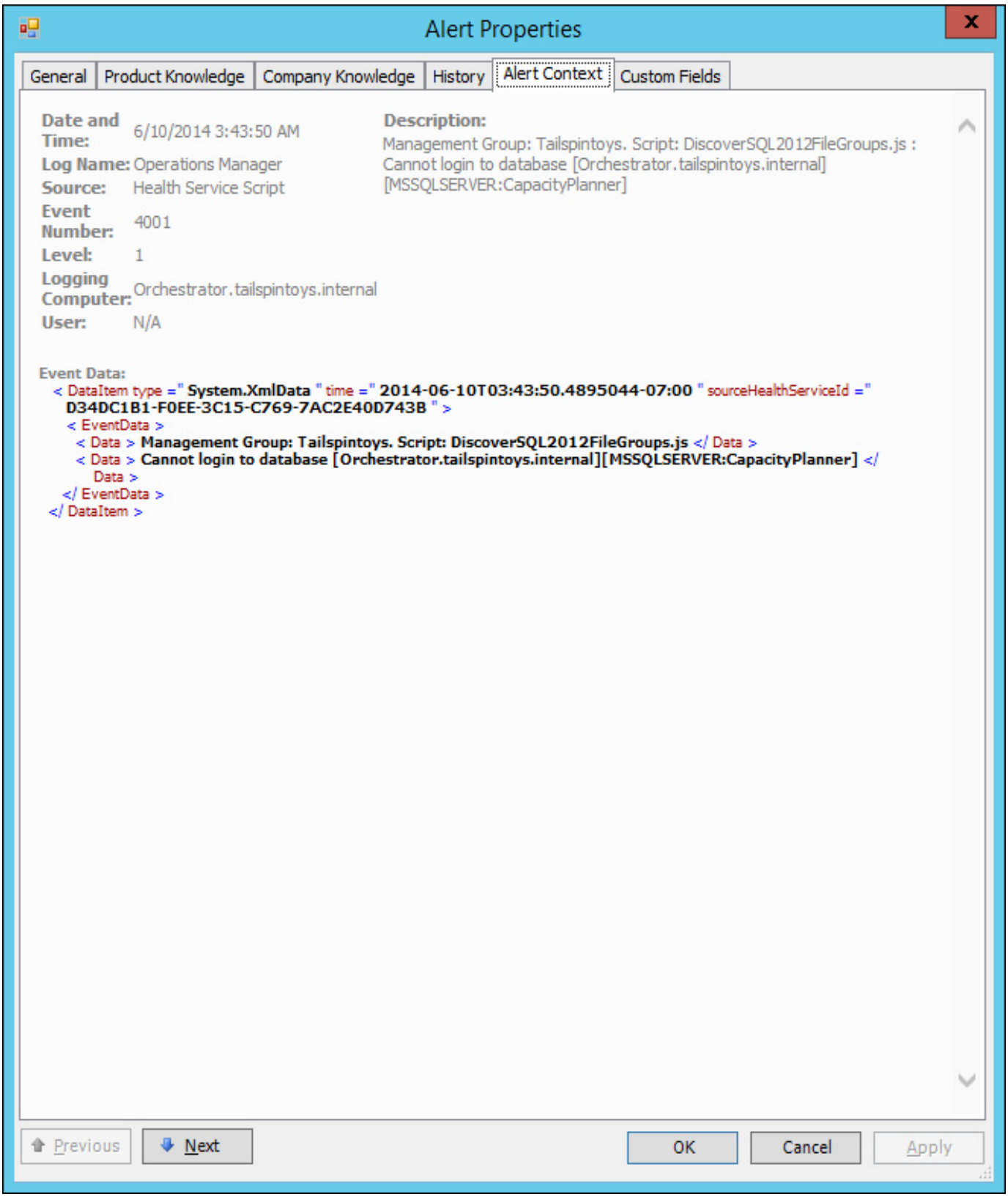

FIGURE 3-5 Alert context

- The Custom Fields tab allows you to enter custom field information.

More Info: **Viewing Alert Details**

You can learn more about viewing alert details at *http://technet.microsoft.com/en-us/library/hh212923.aspx*.

Closing alerts

Closing an alert removes it from the list of Active Alerts. In most cases, you'll only close an alert if you can verify that the issue has been resolved. Resolving alerts works differently depending on whether an alert was generated by a monitor, or by a rule. The differences are as follows:

- If you close an alert that was generated by a rule and the issue that generated the alert occurs again, another alert will be sent. You can close an alert generated by a rule as part of the diagnostic process, as new alerts will be sent if you haven't resolved the underlying issue.
- If you close an alert that was generated by a monitor when the issue is not fixed, no additional alerts will be sent because alerts from monitors are generated by changes in state.

Since the alert won't be raised again unless there is a negative change of health state, you have to take care when closing alerts generated by monitors as you may simply hide an issue rather than fix it. For the most part, monitors automatically resolve the alerts that they generate. Having said that, not every monitor will automatically resolve the alerts it generates. Before closing an alert generated by a monitor, check Health Explorer, and verify that the state of the monitored segment has returned to healthy.

You can set multiple resolution states for alerts, and even create your own alert resolution states. Resolution states can have a value between 1 and 254, with the ID of 1 assigned for the New resolution state, and the ID of 255 assigned for the Closed resolution state. Figure 3-6 shows configuring the resolution state for an alert.

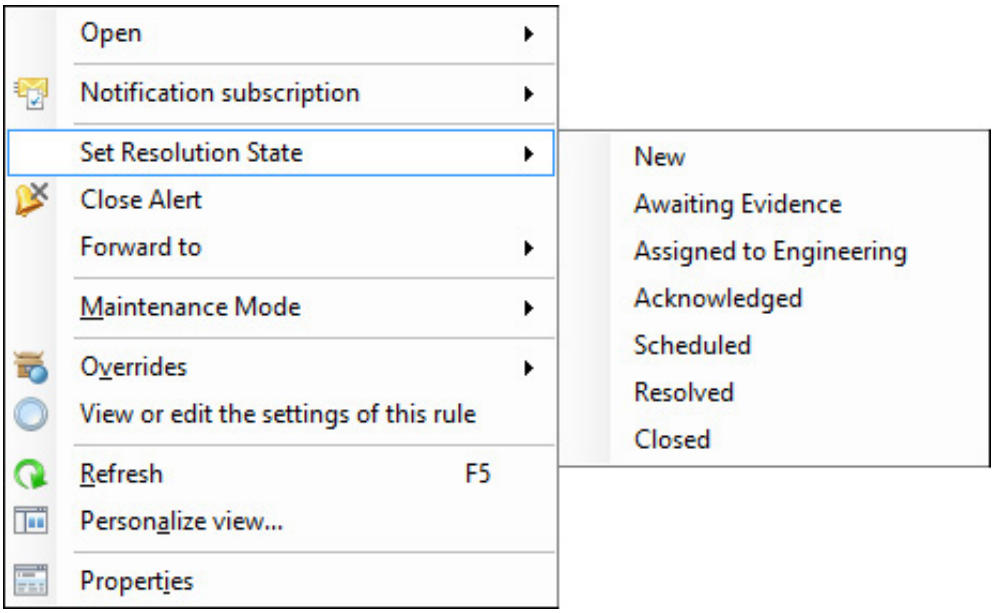

FIGURE 3-6 Resolution states

You configure additional alert resolution states by performing the following steps:

1. In the Administration workspace of the Operations Manager console, click Settings, click Alerts, and then click Properties in the Tasks pane.
2. On the Alert Resolution States dialog box, shown in Figure 3-7, click New.

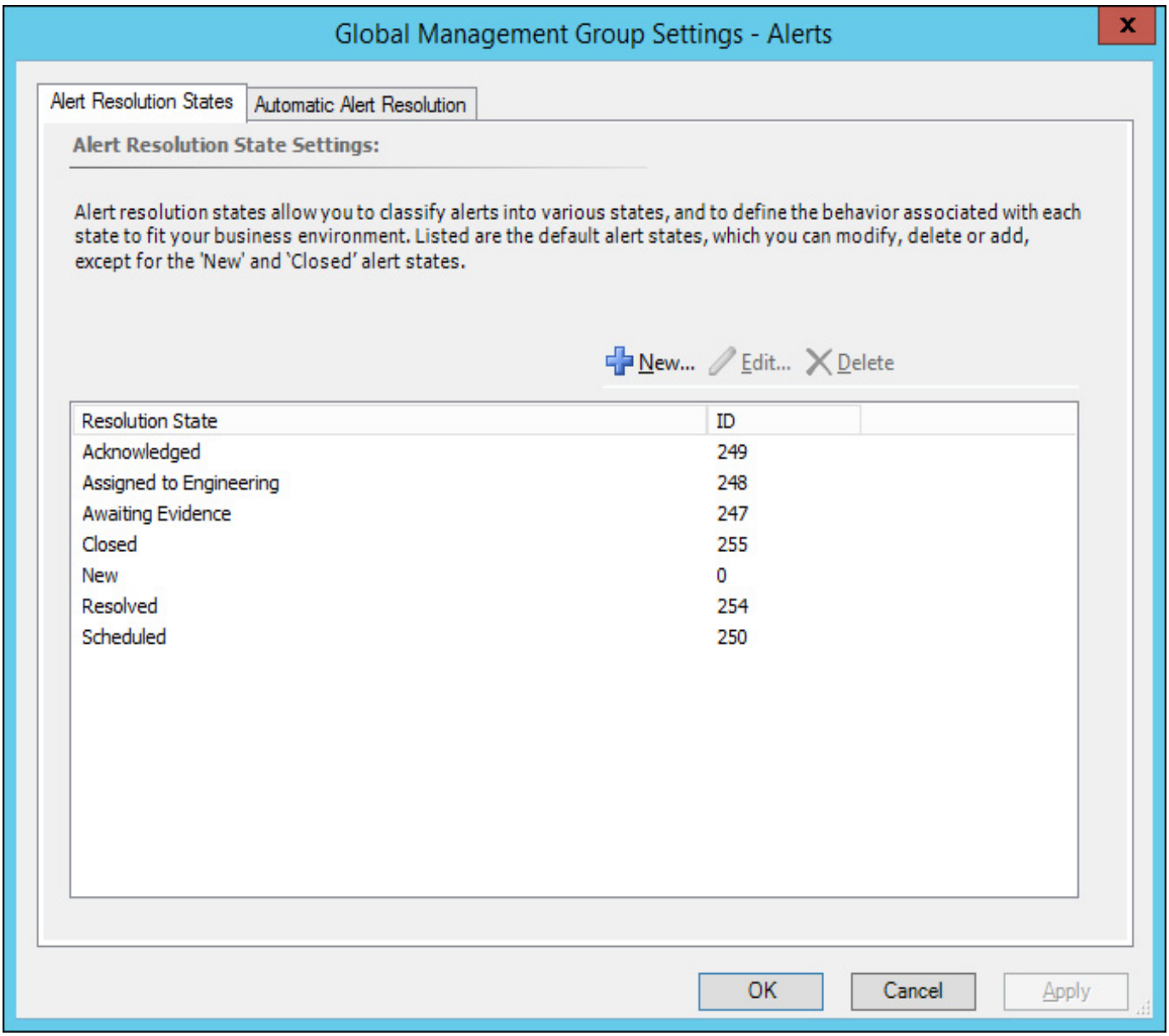

FIGURE 3-7 Alert resolution states

3. On the Add Alert Resolution State dialog box, provide a resolution state name, and an ID that has not been used. Figure 3-8 shows the resolution state set to Under Investigation, and a Unique ID set to 100.

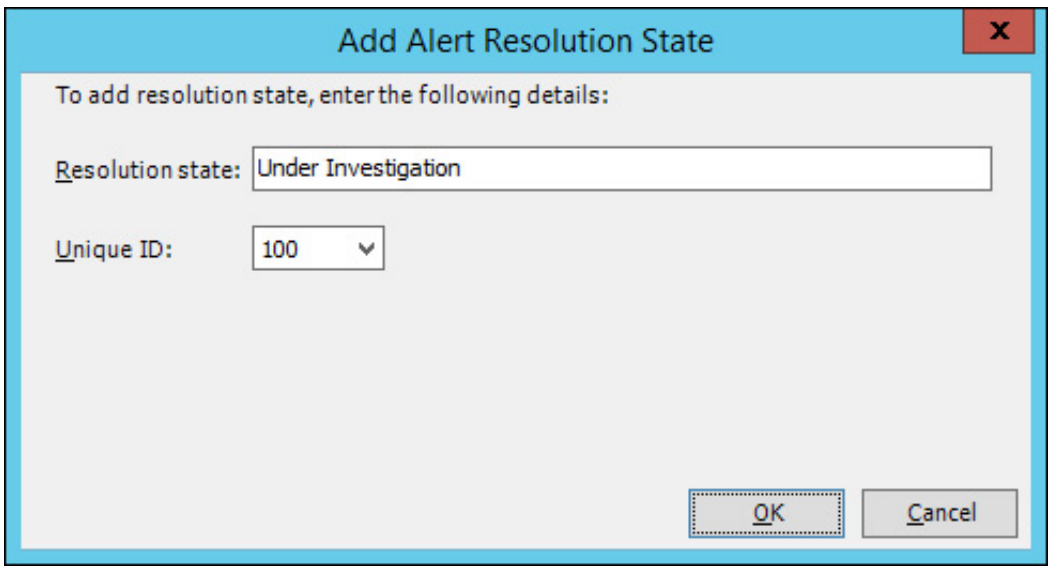

FIGURE 3-8 Add Alert Resolution state

4. The new resolution state will be listed, as shown in Figure 3-9.

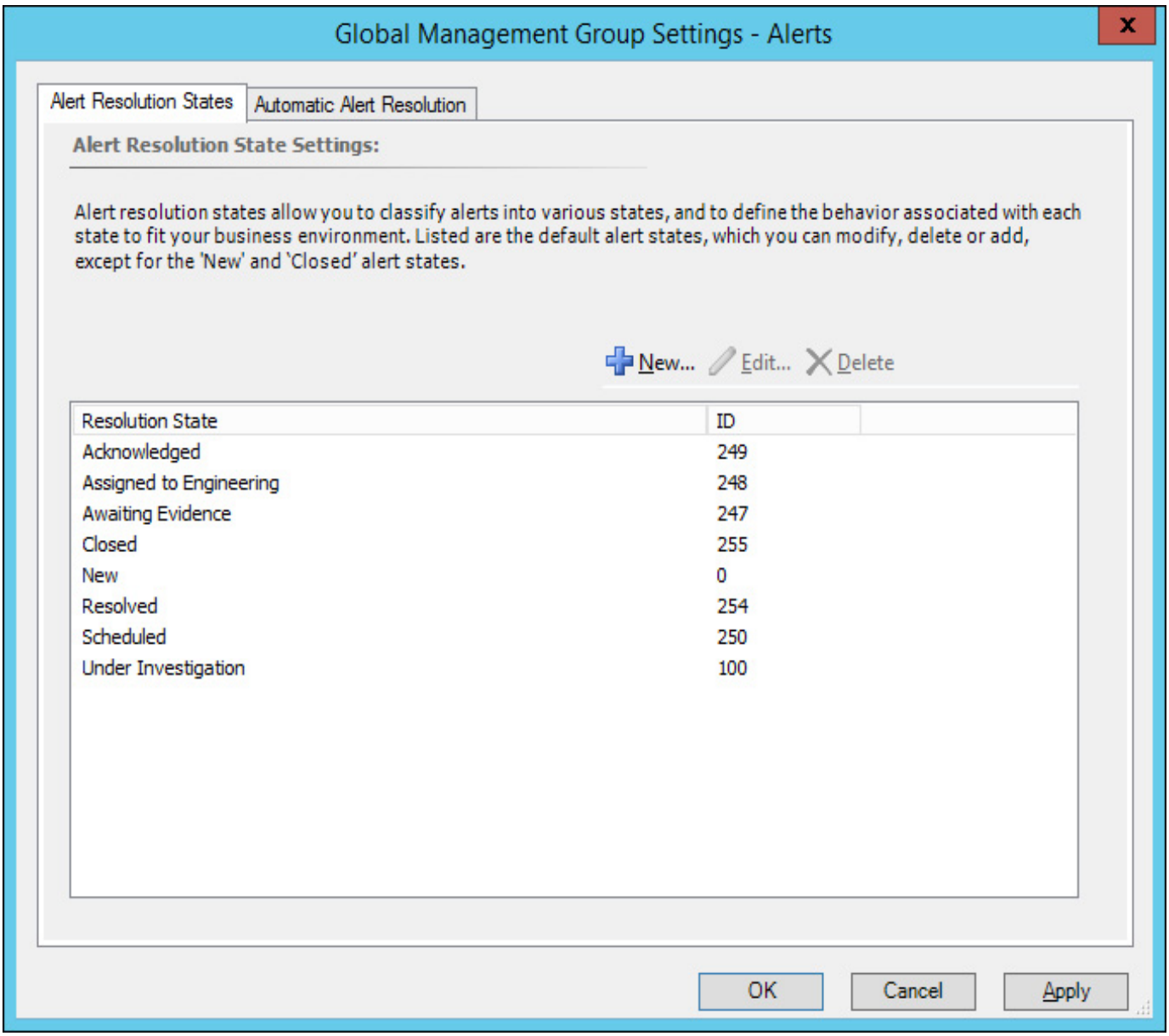

FIGURE 3-9 Review alert resolution states

More Info: **Closing Alerts**

You can learn more about closing alerts at *http://technet.microsoft.com/en-us/library/hh212903.aspx*.

Automatic alert resolution

Operations Manager automatically resolves alerts after a certain number of days. The default settings are to automatically resolve all active alerts that are in a new resolution state after 30 days. This automatic resolution only applies to alerts that haven't had their resolution changed to another resolution state. If, for example, the resolution state had been set to Acknowledged or Scheduled, then the alert will not be automatically resolved.

Automatic alert resolution will also occur in the event that the alert source remains in a healthy state after a specified number of days, with the default being 7 days. To configure Automatic Alert Resolution settings, perform the following steps:

1. In the Administration workspace of the Operations Manager console, click Settings, click Alerts, and on the Tasks pane, click Properties.
2. On the Global Management Group Settings - Alerts dialog box, click the Automatic Alert Resolution tab.
3. Configure the appropriate automatic alert resolution settings on the Global Management Group Settings - Alerts dialog box, as shown in Figure 3-10.

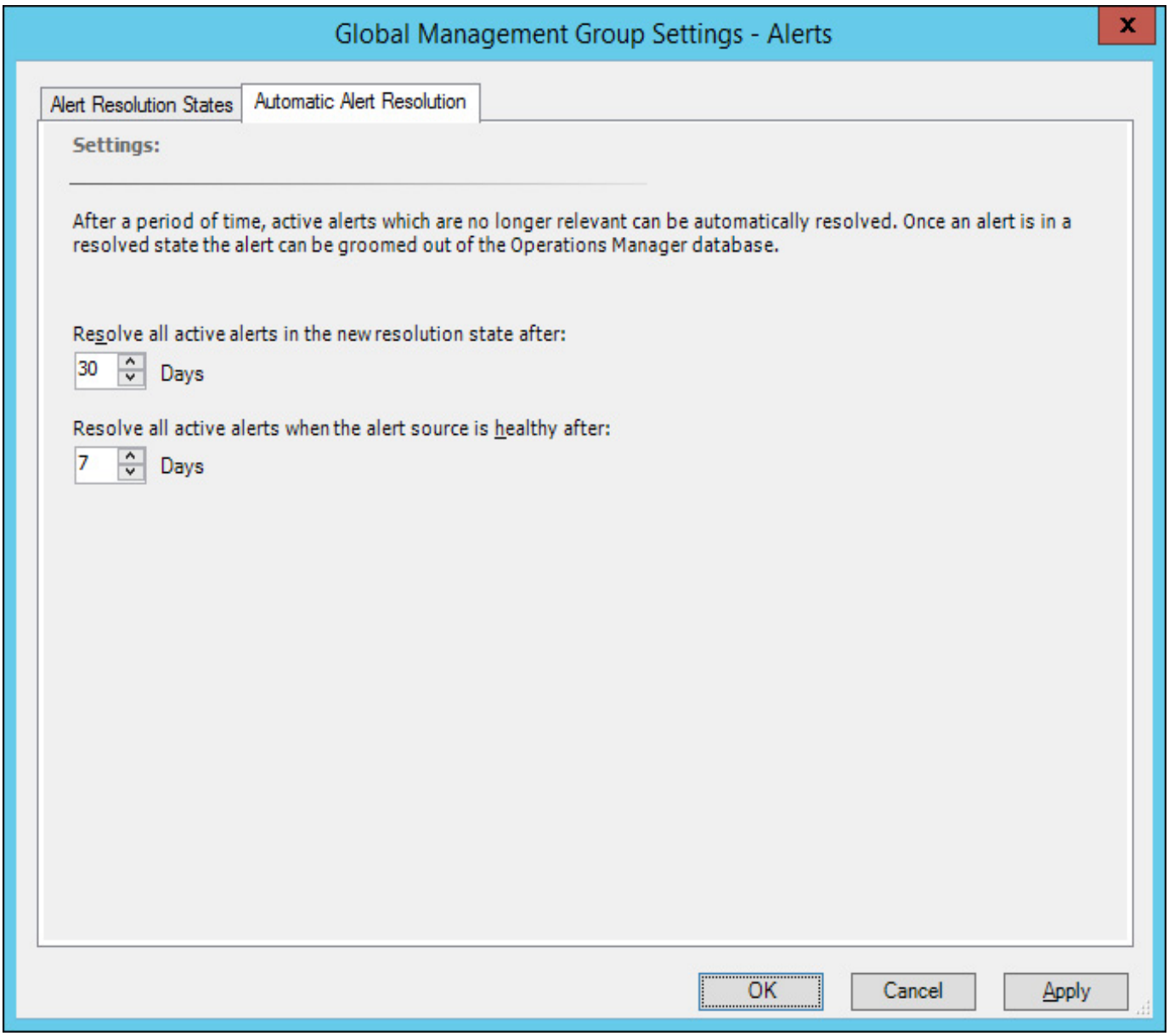

FIGURE 3-10 Automatic alert resolution

More Info: **Automatic Alert Resolution**

You can learn more about automatic alert resolution at *http://technet.microsoft.com/en-us/library/hh212897.aspx*.

Configuring alert notifications

You can configure Operations Manager to automatically send an email, instant message, send an SMS, or run a command when an alert is raised. Of course, you learned in Chapter 1 that if you integrate Orchestrator with Operations Manager, you can trigger runbook automation when an Operations Manager alert is raised, however this chapter is focused on Operations Manager.

To configure alert notifications, you must have prepared the following elements:

- Configure the Notification Account Run As Profile with a Run As account.
- Prepare a notification channel. The notification channel defines the notification format and method of transmission.
- Configure notification subscribers. Subscribers define the notification recipients and notification schedule.
- Prepare a notification subscription. This specifies the conditions for sending a notification, which notification is used, and which subscribers receive the notification.

More Info: **Alert Notifications**

You can learn more about alert notifications at *http://technet.microsoft.com/en-us/library/hh212725.aspx*.

Notification action accounts

Operations Manager uses the Notification Account Run As profile to send notifications. The Notification Account Run As profile requires a Run As account that has the necessary credentials for sending notifications. To create a notification action account, perform the following steps:

1. Right-click the Security node in the Administration workspace of the Operations Manager console, and click Create Run As Account.
2. On the General Properties page of the Create Run As Account Wizard, ensure that Windows is selected as the Run As account type. In the Display Name text box, type **Notification Action Account,** as shown in Figure 3-11.

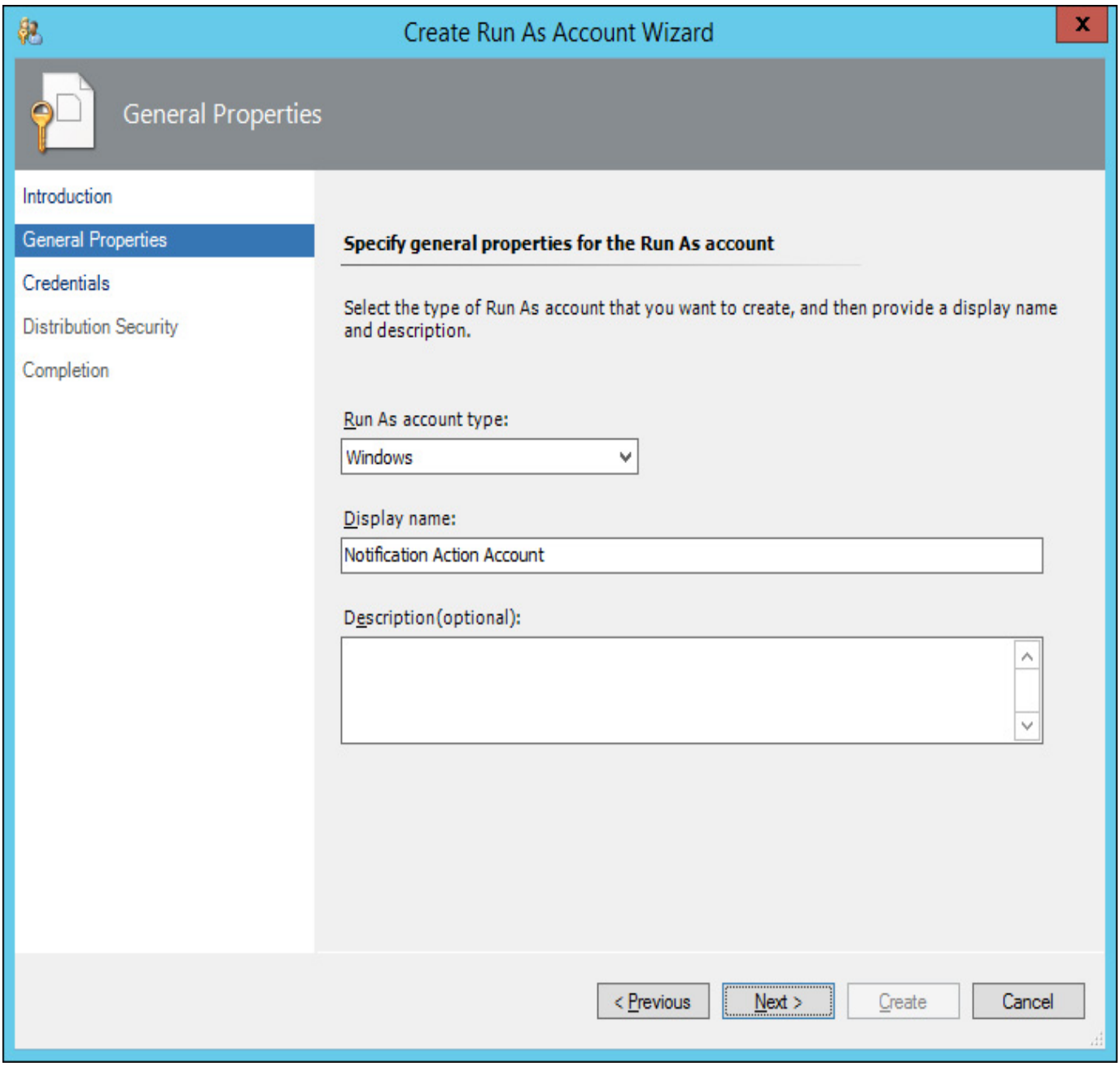

FIGURE 3-11 Notification action account

3. On the Credentials page, provide the username, password, and domain of the user account that will be used to send notifications.
4. On the Distribution Security options page, click More Secure, and then click Create, and then click Close.

5. Under Run As Configuration in the Administration workspace, click Accounts.
6. Double-click Notification Action Account.
7. On the Distribution tab, click Add. On the Computer Search page, click Search. In the list of available items, specify the computers to which you want the Action account distributed, and click Add, as shown in Figure 3-12, and then click OK. Click OK again to close the Run As Account Properties dialog box.

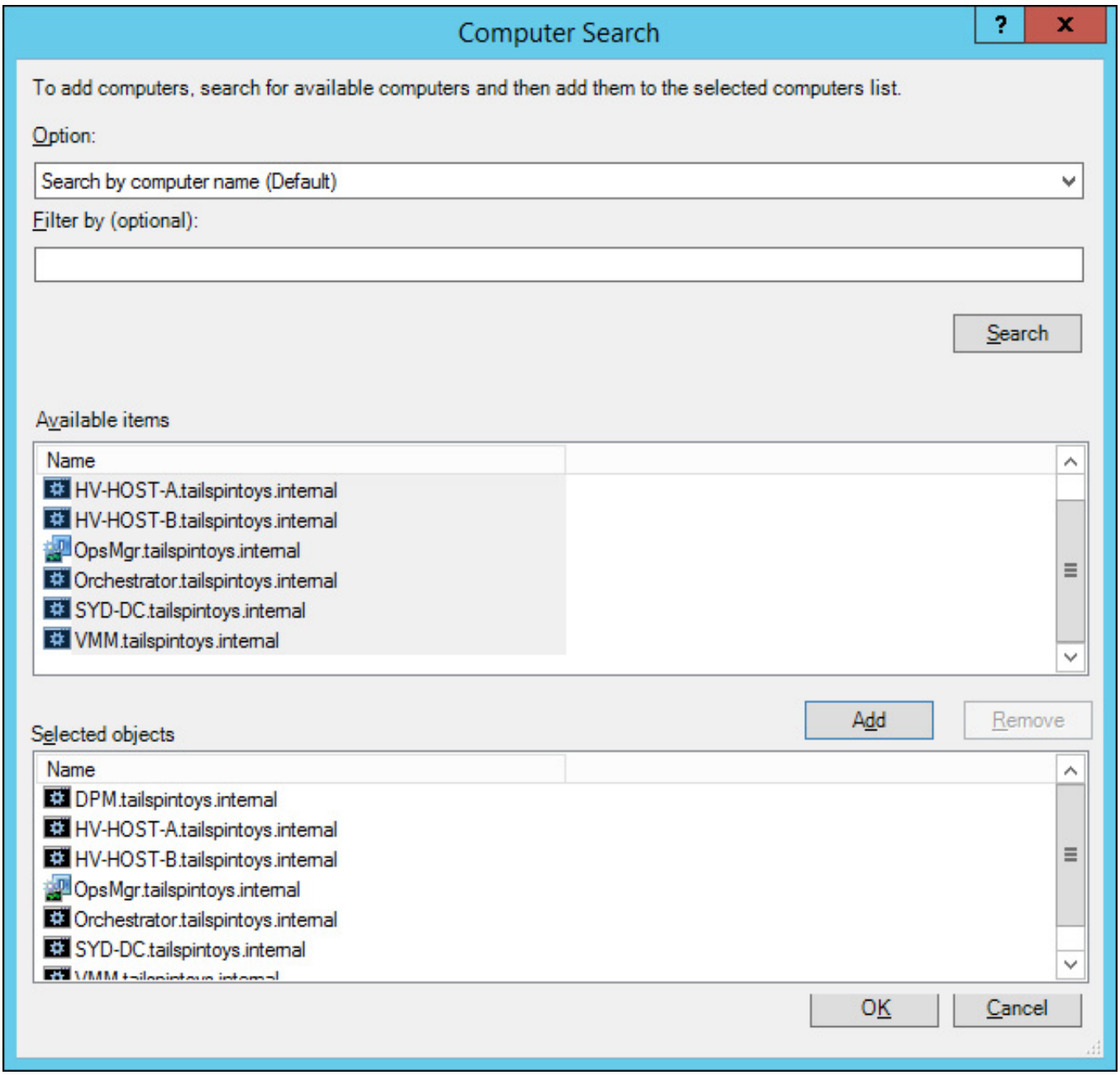

FIGURE 3-12 Computer Search

8. In the Administration workspace of the Operations Manager console, click Profiles under Run As Configuration. Double-click the Notification Account profile.
9. On the Run As Accounts page of the Run As Profile Wizard, click Add.
10. On the Add A Run As Account dialog box, use the drop-down menu to select the Notification Action Account created earlier, as shown in Figure 3-13, and then click OK.

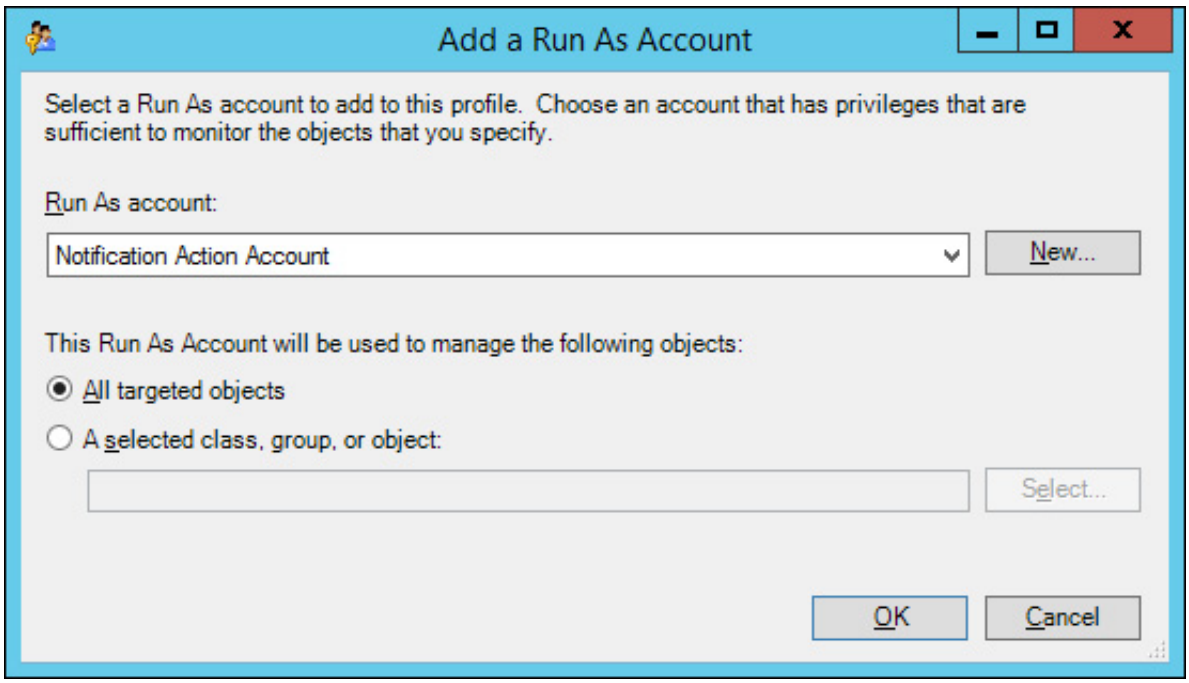

FIGURE 3-13 Add a Run As Account

11. Verify that the Run As account is listed, as shown in Figure 3-14, and then click Save.

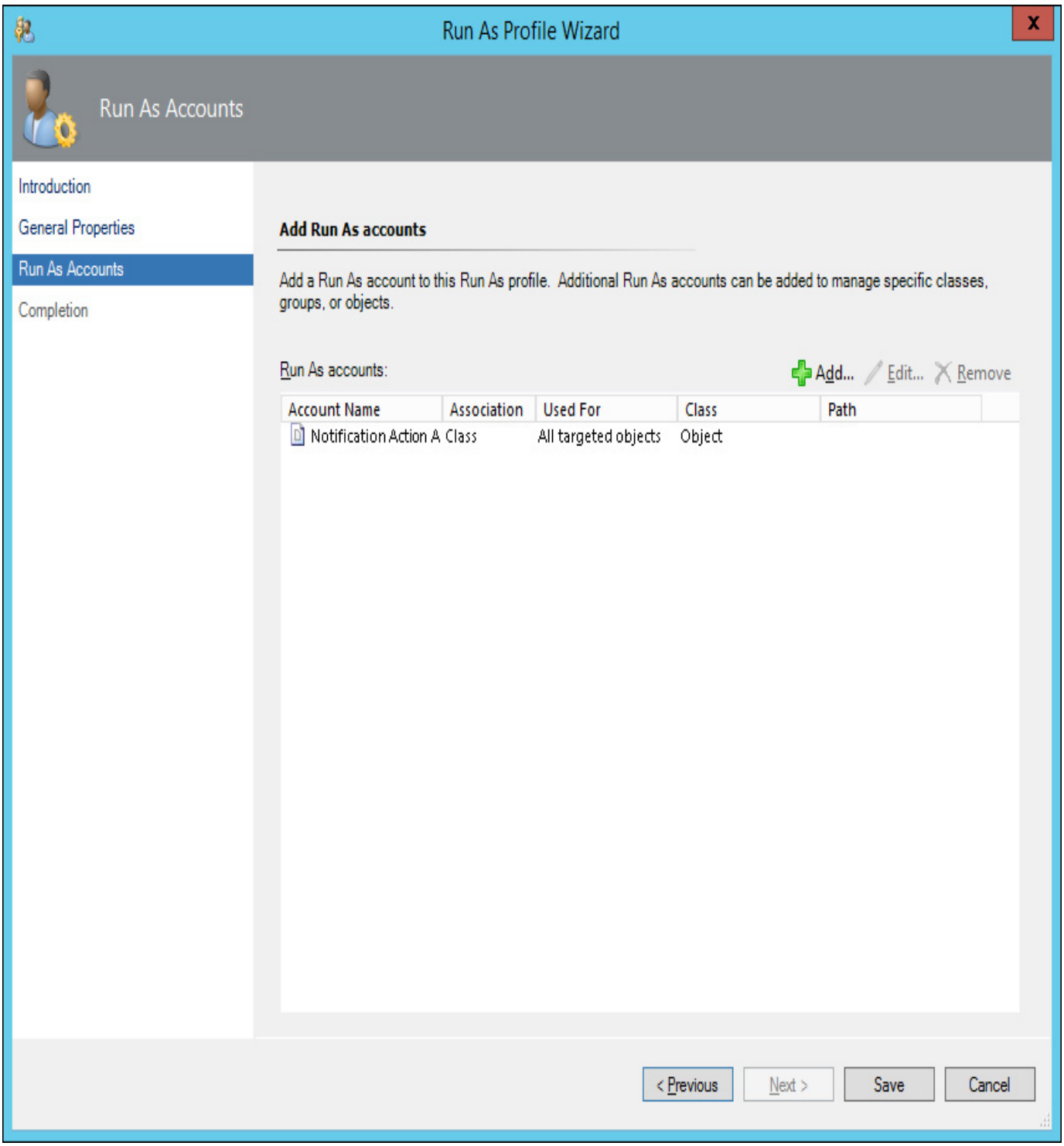

FIGURE 3-14 Run As Profile Wizard

More Info: **Notification Action Accounts**

You can learn more about configuring notification action accounts at *http://technet.microsoft.com/en-us/library/hh212835.aspx*.

Email notification channel

The most common method of notification is through email. This is especially true now that smartphones have email capability, and the cost of sending an email to a smartphone is an order of magnitude lower than the cost of sending an SMS. Prior to configuring an email notification channel, you'll need to have access to an SMTP server and have configured a mailbox to be used for return email addresses, should it be necessary to provide an email response to a notification.

To enable an email notification channel, perform the following steps:

1. In the Administration workspace of the Operations Manager console, right-click the Channels node under Notifications, click New Channel, and then click E-Mail (SMTP).

2. On the Settings page of the E-Mail Notification Channel Wizard, click Add.
3. On the Add SMTP Server dialog box, enter the FQDN of the SMTP server. Figure 3-15 shows this set to Smtp.tailspintoys.internal, and click OK.

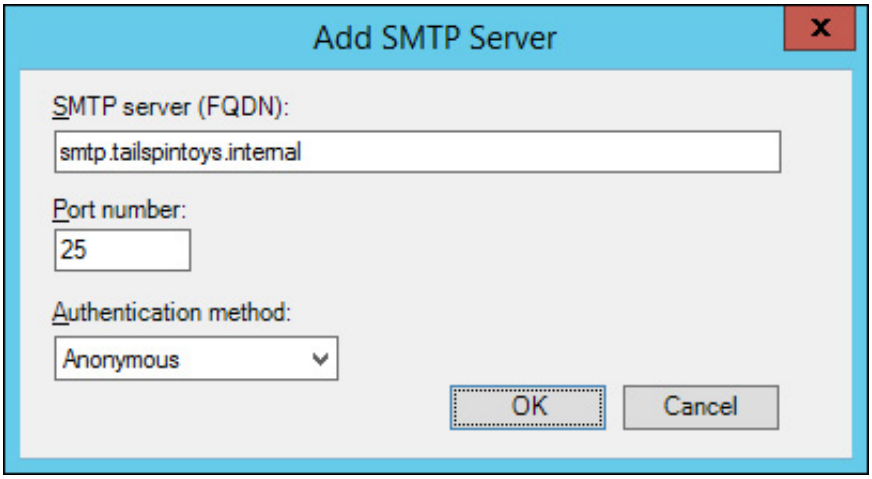

FIGURE 3-15 Add SMTP Server

4. On the Settings page, enter the return address. Figure 3-16 shows this set to alerts@tailspintoys.internal.

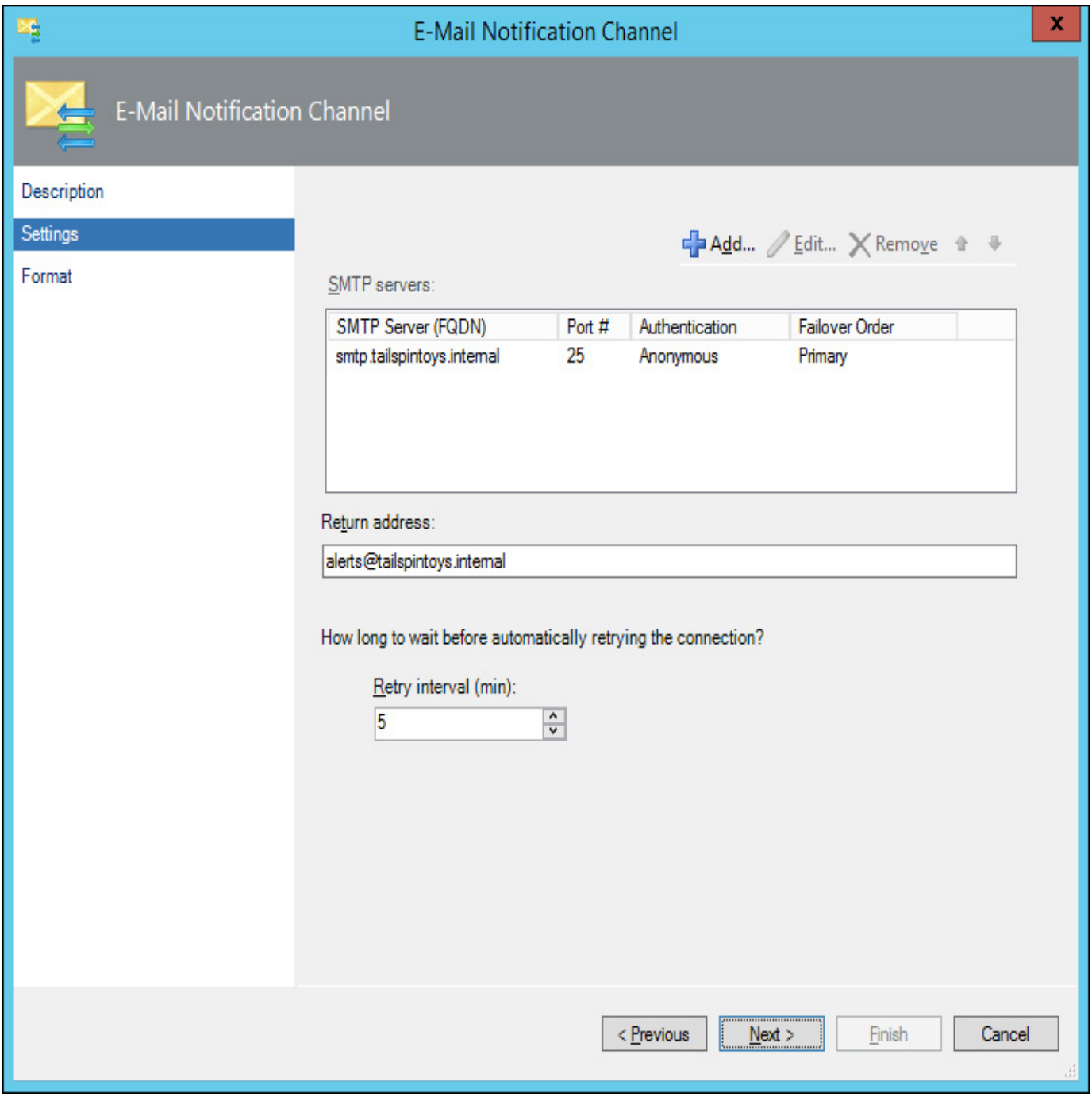

FIGURE 3-16 E-mail Notification Channel

5. On the Format page, review the default email format, as shown in Figure 3-17. You can modify this as necessary for your own environment. Click Finish to complete the wizard.

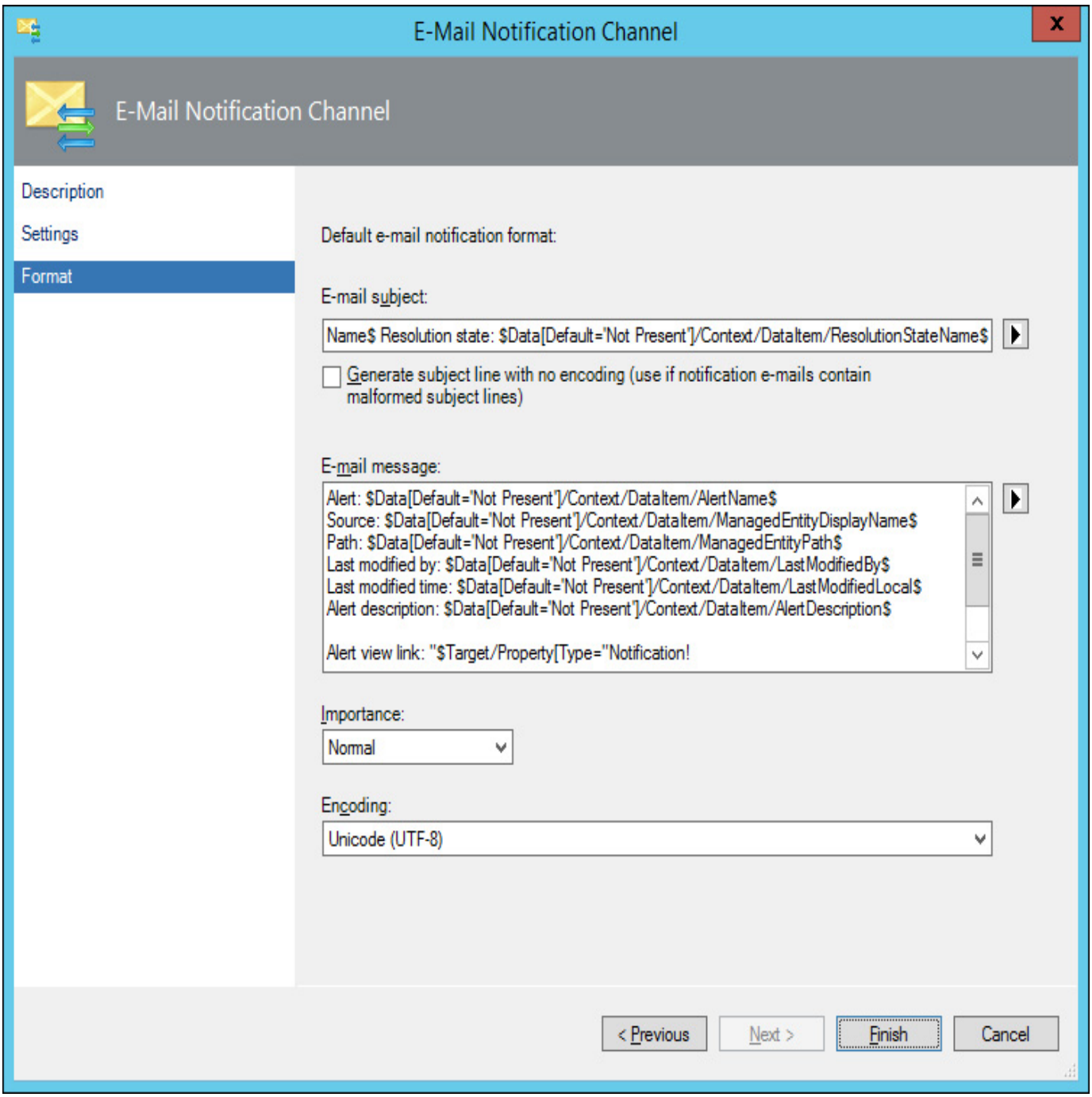

FIGURE 3-17 E-Mail Notification Channel

More Info: **Email Notification Channels**

You can learn more about configuring email notification channels at *http://technet.microsoft.com/en-us/library/hh212914.aspx*

Notification subscribers

Notification subscribers are the people who you want to receive notifications about an alert. You can only create notification subscribers after you've created a notification channel. To create a notification subscriber, perform the following steps:

1. In the Administration workspace of the Operations Manager console, click Subscribers under the Notifications node. In the Tasks menu, click New.
2. On the Description page of the Notification Subscriber Wizard, specify a name for the subscriber.
3. On the Schedule page, select whether you want to send notifications at any time, or whether subscribers should only receive notifications at specific times. For example, Figure 3-18 shows a configuration where notifications will only be sent between 9:00 A.M. and 5:30 P.M. on

weekdays. This is the master schedule. It is possible to configure schedules for individual subscribers when adding those individual subscribers.

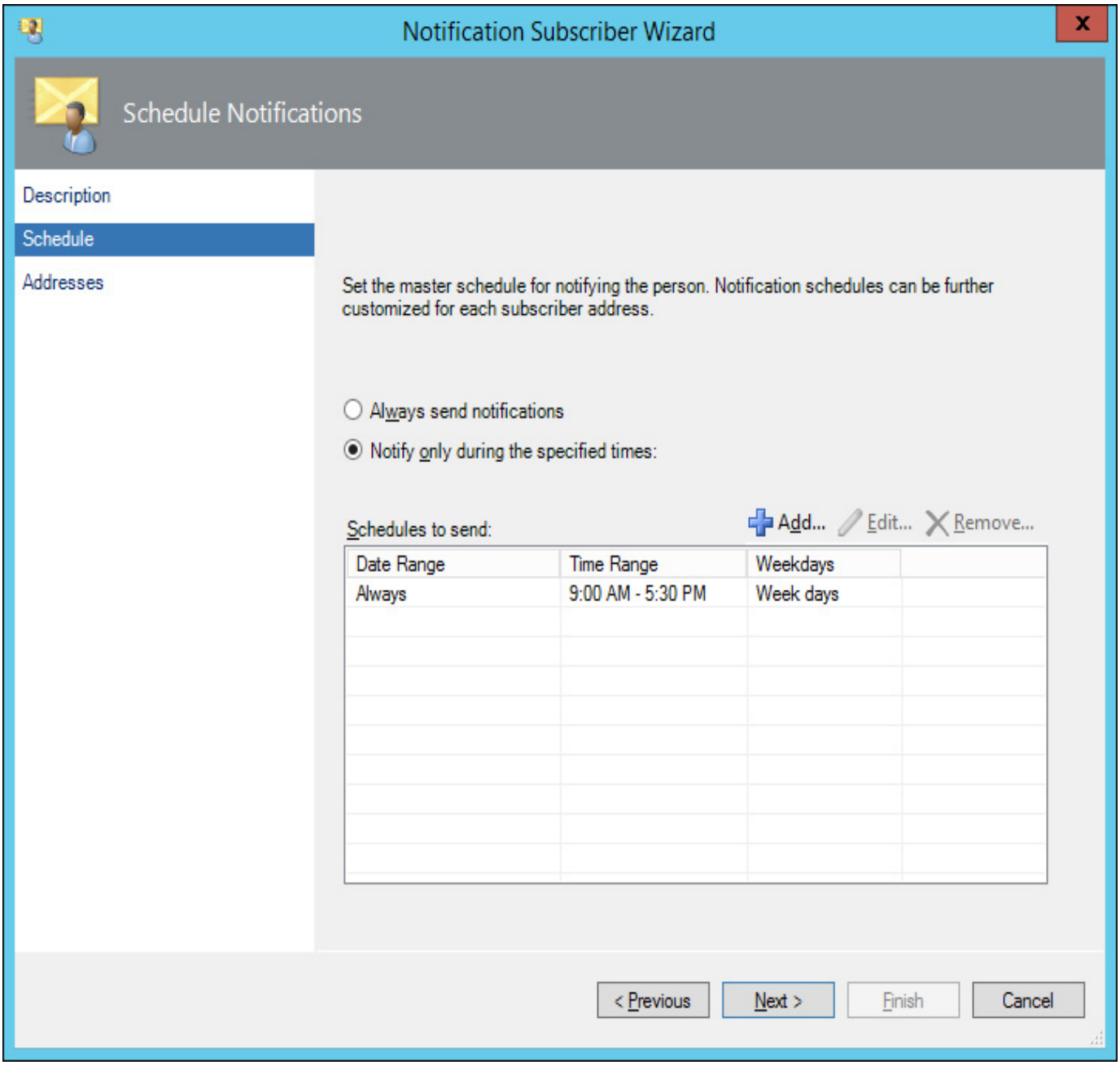

FIGURE 3-18 Notification subscriber schedule

4. On the Addresses page, click Add. This will launch the Subscriber Address Wizard, allowing you to specify the notification.
5. On the General page, specify the name of the address. This does not need to be the email address, but instead needs to be descriptive. For example, Figure 3-19 shows this set as Administrator Email Address.

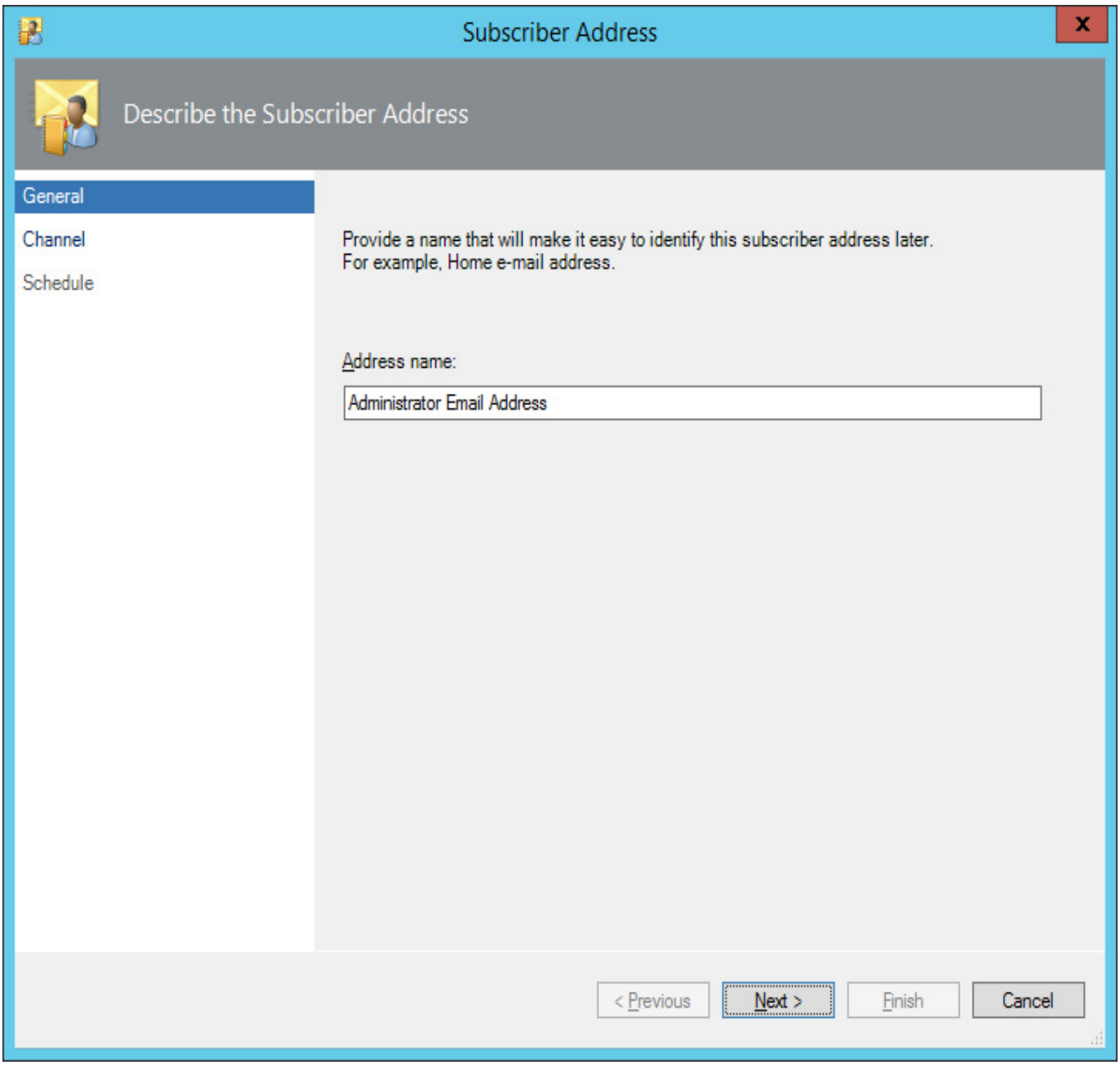

FIGURE 3-19 Subscriber Address

6. On the Channel page, use the drop-down menu to select the E-Mail (SMTP) Channel Type, and then specify the email address that will be used with this channel. Figure 3-20 shows the delivery address set to administrator@tailspintoys.internal.

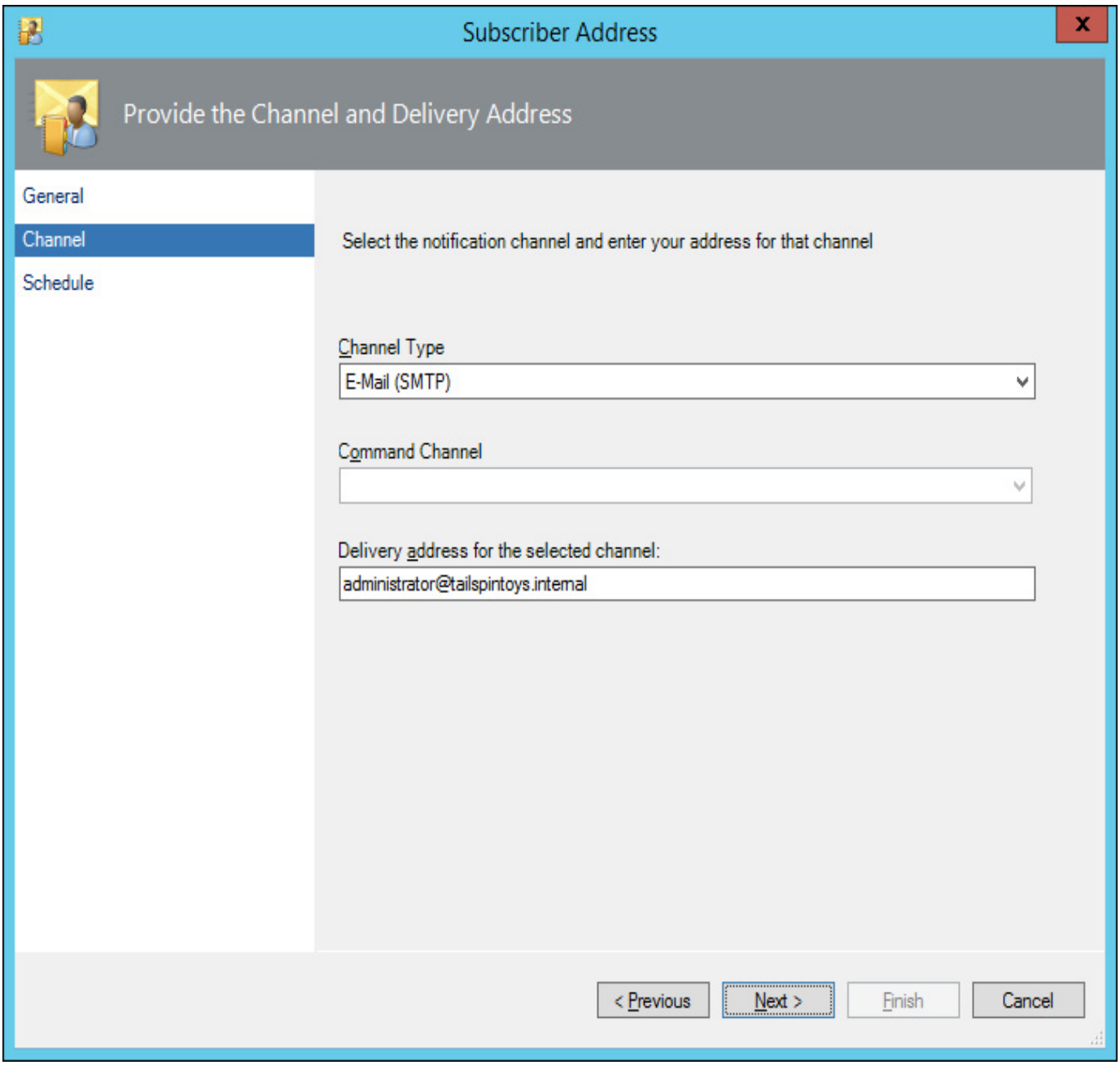

FIGURE 3-20 Subscriber address channel

7. On the Schedule page, you can specify when notifications can be sent to this particular subscriber. If you want to use the master schedule configured earlier, you don't have to configure a schedule here.

More Info: **Notification Subscribers**

You can learn more about configuring notification subscribers at *http://technet.microsoft.com/en-us/library/hh212812.aspx*.

---

8. On the Addresses page, shown in Figure 3-21, verify that all of the individual subscribers that you want to add are listed, and then click Finish.

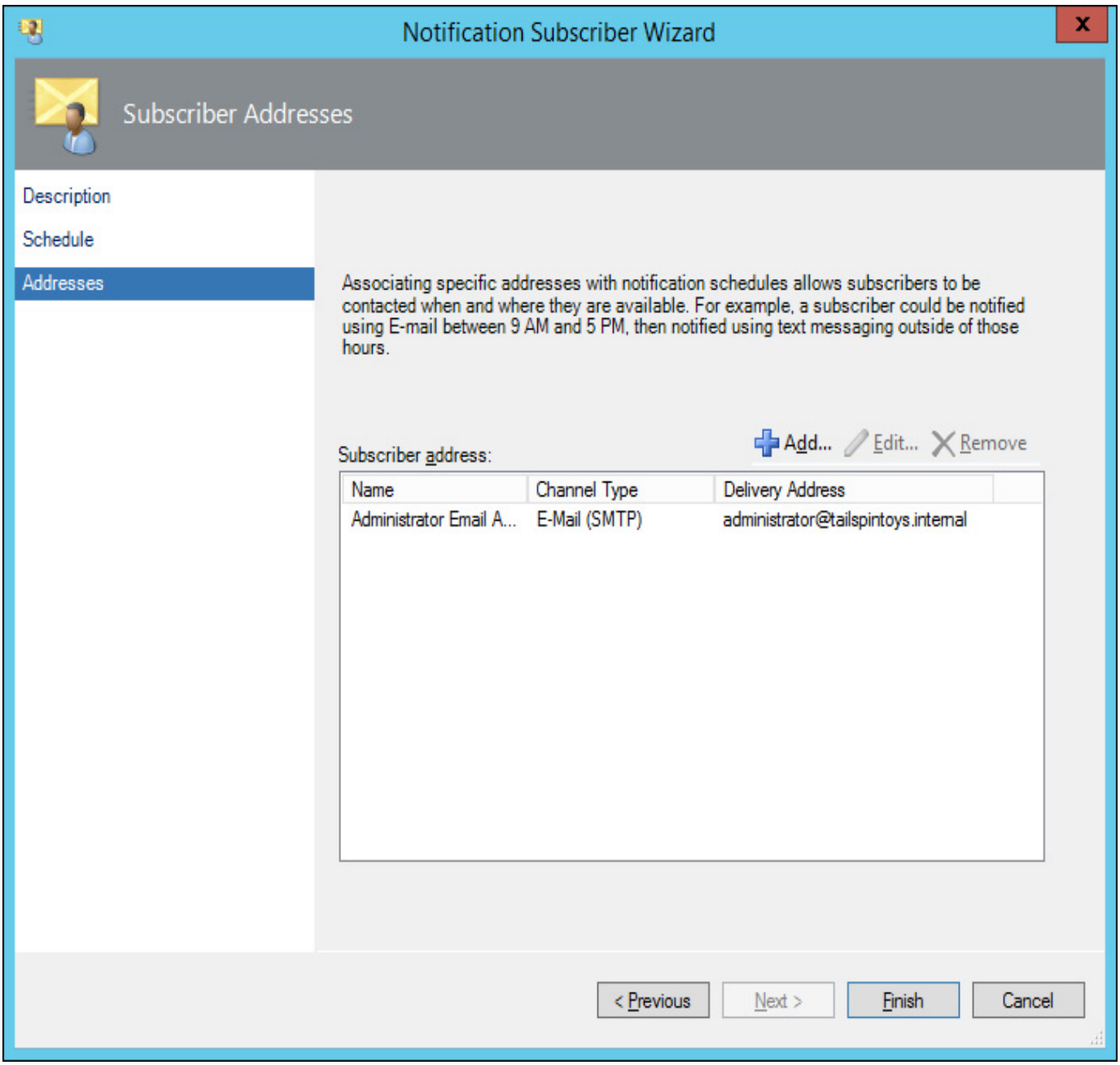

FIGURE 3-21 Notification subscriber addresses

Notification subscriptions

Notification subscriptions allow you to define the criteria for when a notification should be sent, whom it should be sent to, and the method that should be used to send that notification. You can create notification subscriptions based on the following criteria, shown in Figure 3-22:

- Raised By Any Instance In A Specific Group
- Raised By Any Instance Of A Specific Class
- Created By Specific Rules Or Monitors
- Raised By An Instance With A Specific Name
- Of A Specific Severity
- Of A Specific Priority
- With A Specific Resolution State
- With A Specific Name
- With Specific Text In The Description
- Created In A Specific Time Period
- Assigned To A Specific Owner
- Last Modified By A Specific User

- That Was Modified In A Specific Time Period
- Had Its Resolution State Changed In A Specific Time Period
- That Was Resolved In A Specific Time Period
- Resolved By Specific User
- With A Specific Ticked ID
- Was Added To The Database In A Specific Time Period
- From A Specific Site
- With Specific Text In Custom Field (1-10)
- With A Specific TFS Work Item ID
- With A Specific TFS Work Item owner

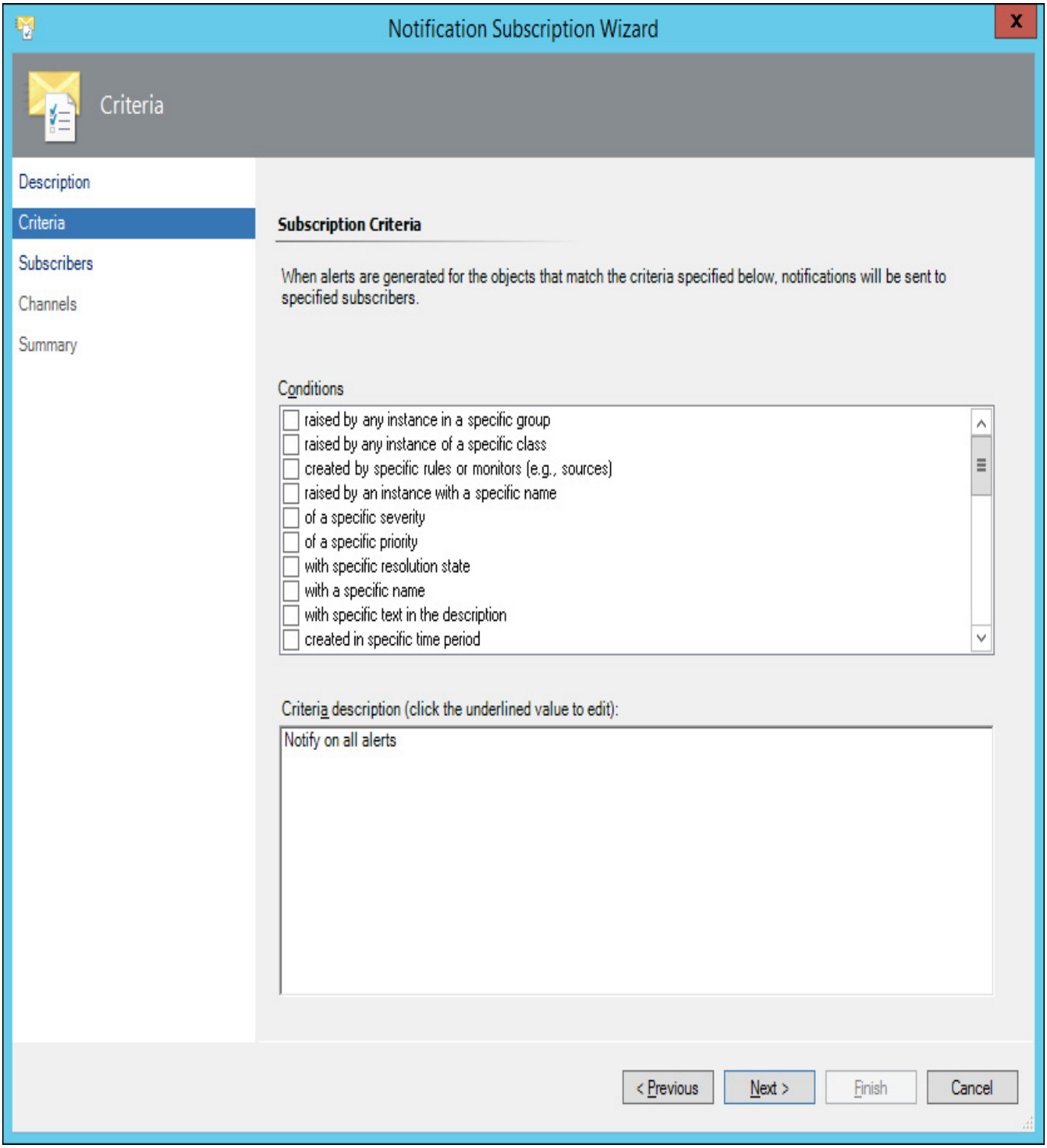

FIGURE 3-22 Notification subscription criteria

To create a notification subscription, perform the following steps:

1. In the Administration workspace of the Operations Manager console, click the Subscriptions node under the Notifications node. In the Tasks pane, click New.
2. On the Description page of the Notification Subscription Wizard, provide a meaningful subscription name.
3. On the Criteria page, specify the criteria that should trigger the notification. For example, Figure 3-23 shows a notification subscription that uses the criteria that an alert must have a critical severity and a high priority.

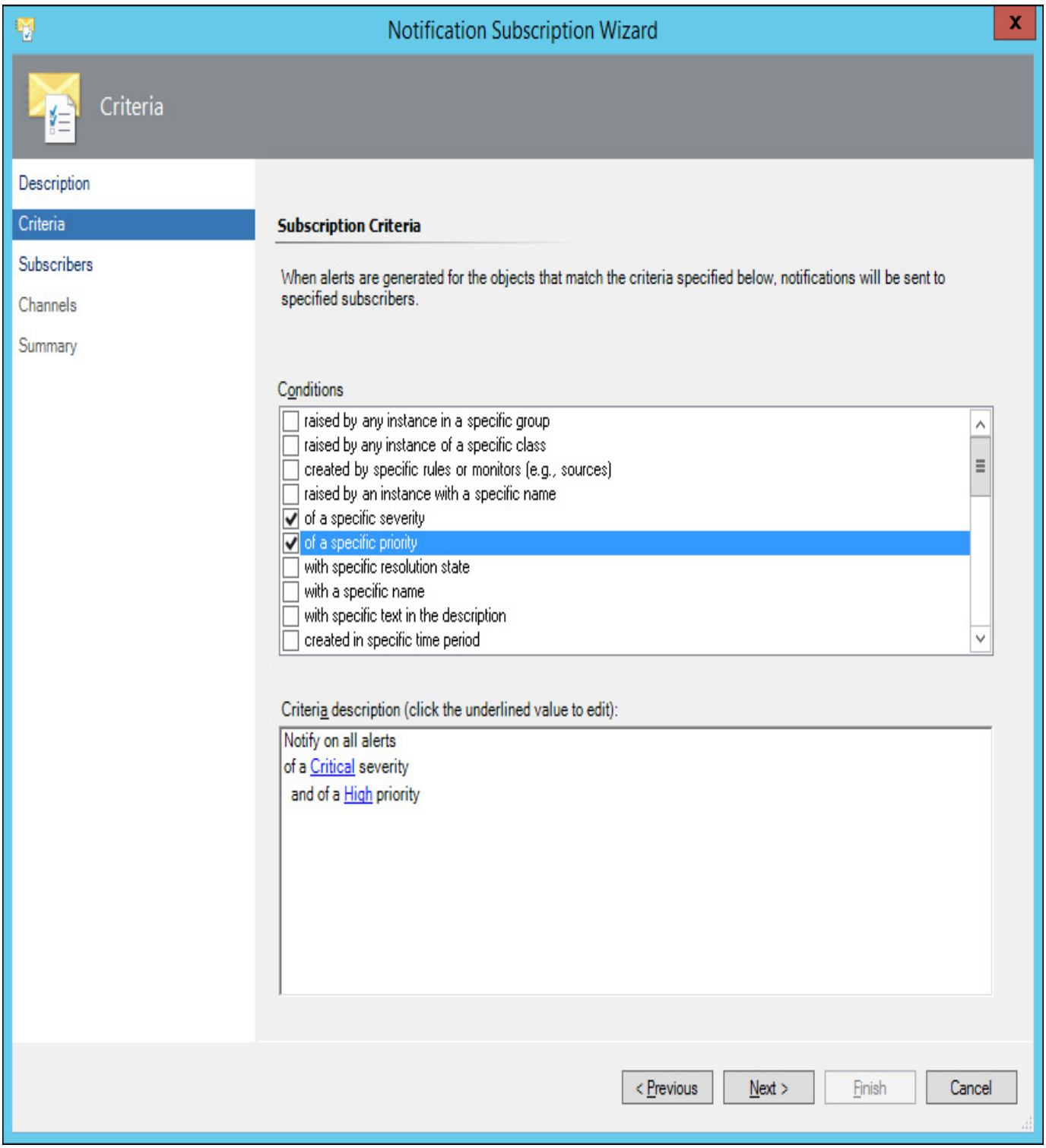

FIGURE 3-23 Notification subscription criteria

4. On the Subscribers page, click Add. On the Subscriber Search page, click Search. The list of subscribers that you have configured will be displayed. Select the ones that you wish to add to the notification subscription, and click OK. Figure 3-24 shows the subscriber named TAILSPINTOYS\Administrator being added as a selected subscriber.

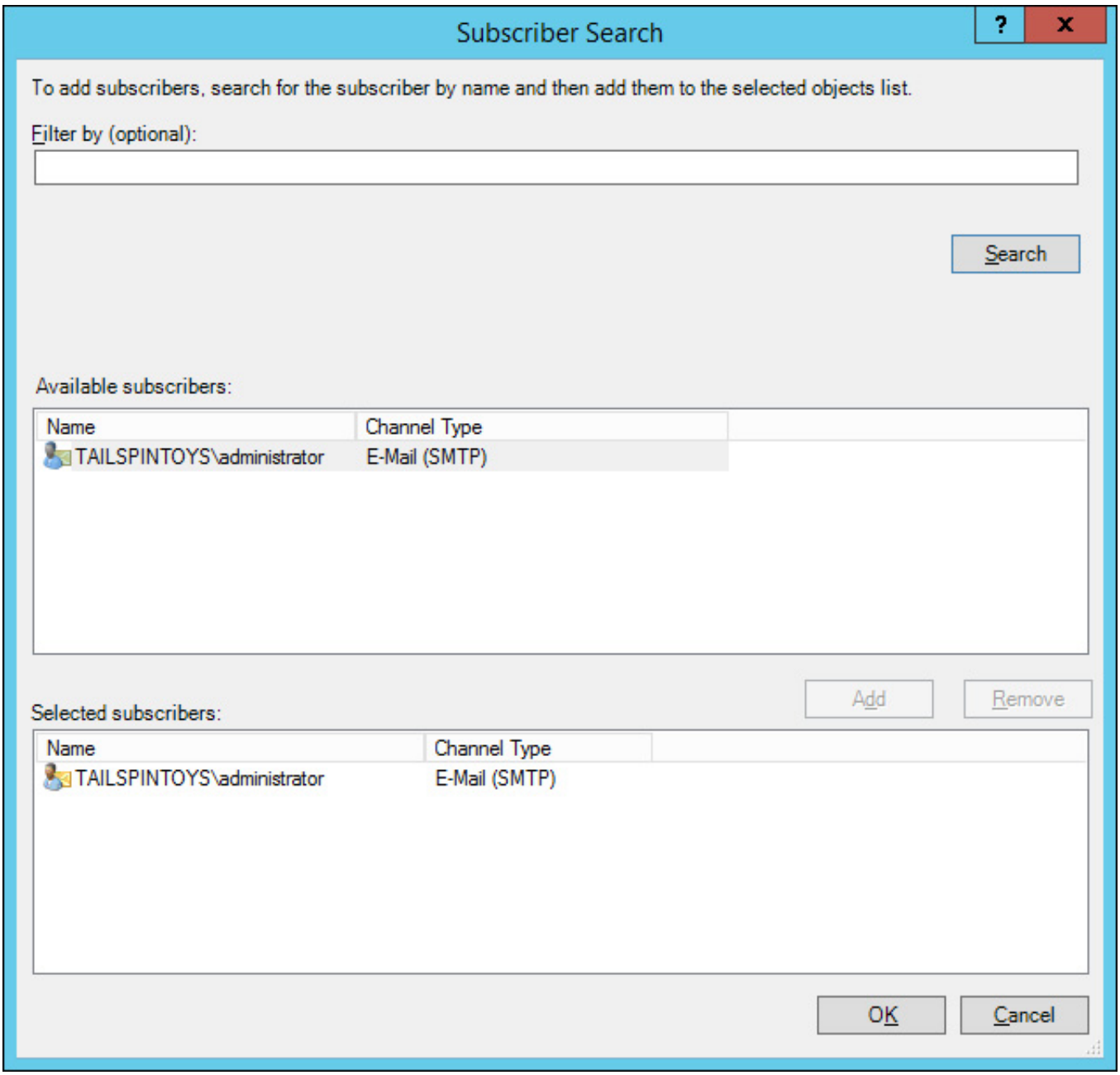

FIGURE 3-24 Subscriber Search

5. On the Channels page, click Add. On the Channel Search page, click Search. Select the channel that you want to use, click Add, and click OK. Figure 3-25 shows the Channels page with the SMTP Channel selected. Complete the wizard.

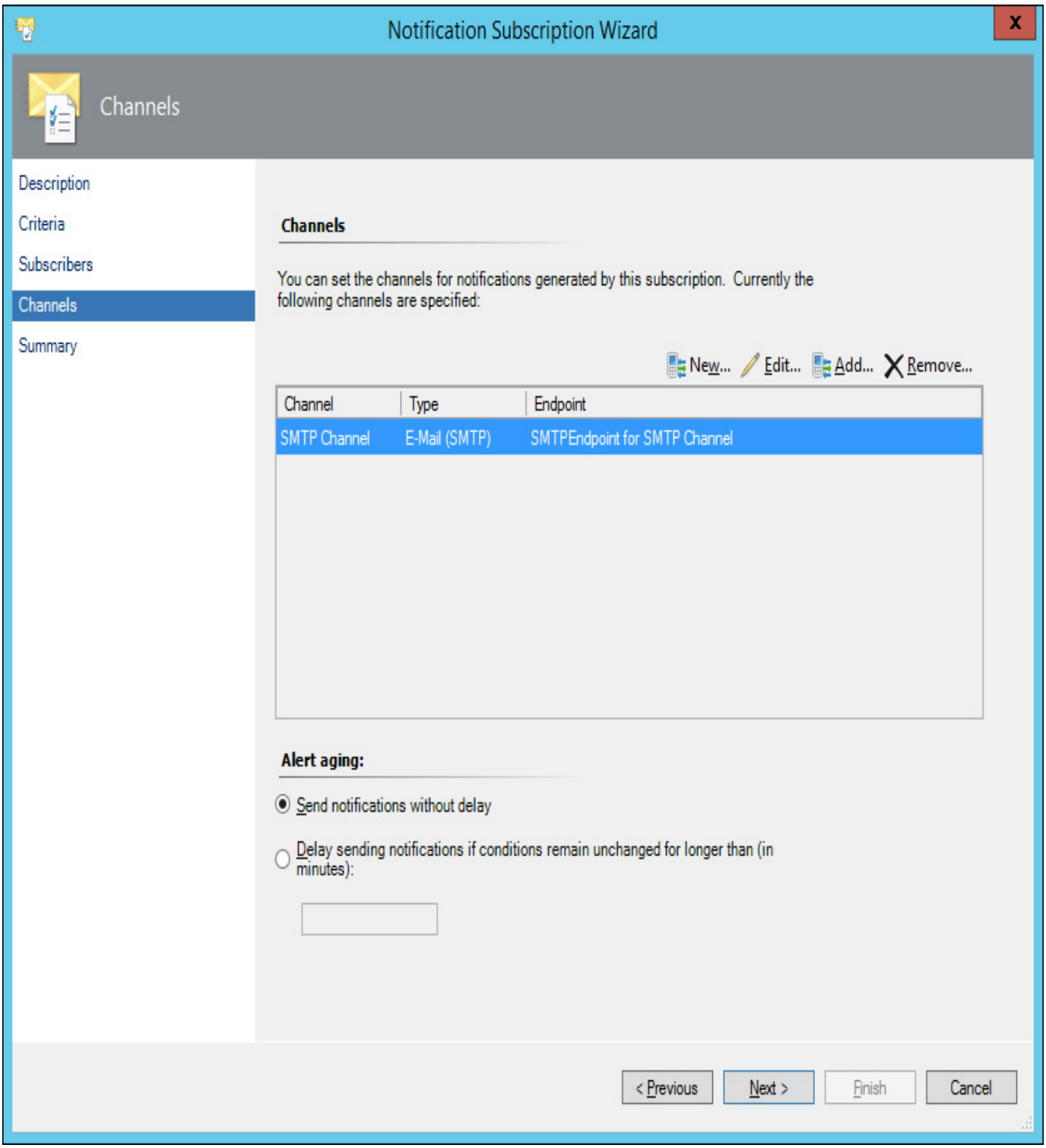

FIGURE 3-25 Notification subscription channels

More Info: **Notification Subscriptions**

You can learn more about creating notification subscriptions at *http://technet.microsoft.com/en-us/library/hh212789.aspx*.

Subscribe to an alert notification

While you can configure a notification subscription by setting up the conditions under which you should be notified, you can also use the Alerts view in the Monitoring workspace to locate a specific alert and use that as the basis of creating a new notification subscription.

To create a notification subscription from an existing alert, perform the following steps:

1. In the Monitoring workspace of the Operations Manager console, select the alert for which you want to create the notification subscription.
2. In the Tasks pane, under Subscription, click Create. This will launch the Notification

Subscription Wizard. The Description and Criteria pages of this wizard will already be populated with description and criteria information about the alert from which you are creating the notification subscription.

3. On the Subscribers page, click Add to select the subscriber who will be notified by the notification subscription.
4. On the Channels page, click Add to specify the method through which the subscriber will be notified. Figure 3-26 shows that the SMTP Channel is selected.

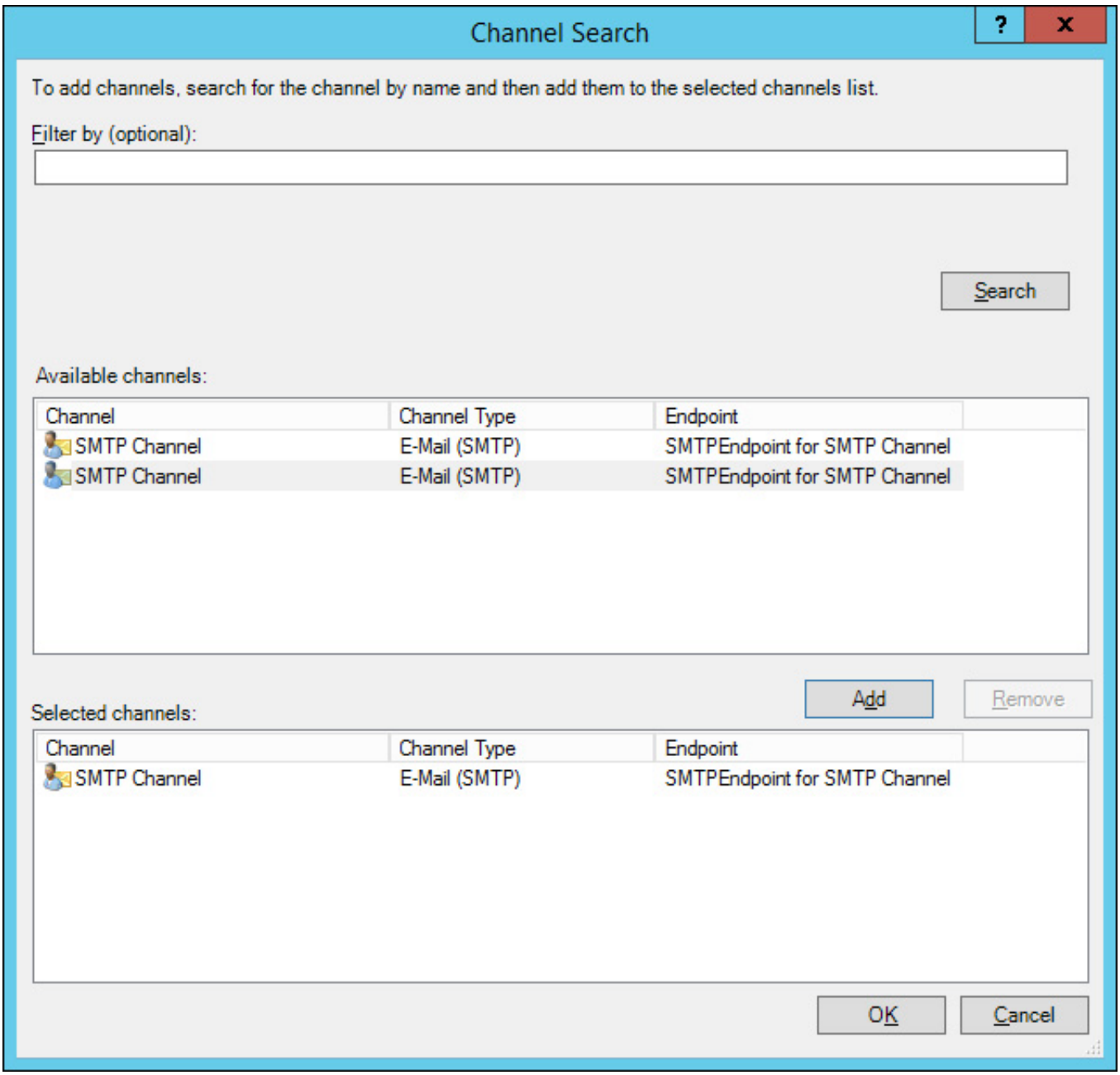

FIGURE 3-26 Channel Search

5. Complete the wizard to create the notification subscription based off of the alert.

More Info: **Subscribe to Notifications From an Alert**

You can learn more about subscribing to notifications from an alert at *http://technet.microsoft.com/en-us/library/hh212895.aspx*.

Analyzing network devices and data

The Network Monitoring node of the Monitoring workspace of the Operations Manager console allows you to view network-related monitoring information. These views include:

- Active Alerts

- Hosts
- HSRP Groups
- Legacy Network Devices
- Network Devices
- Network Summary Dashboard
- Routers
- Switches
- VLANS
- Performance

Network Summary Dashboard view

The Network Summary Dashboard view provides you with the following information about network devices, termed nodes that Operations Manager monitors:

- Nodes With Slowest Response (ICMP Ping)
- Nodes With Highest CPU Usage
- Interfaces With Highest Utilization
- Interfaces With Most Send Errors
- Interfaces With Most Receive Errors
- Notes With The Most Alerts
- Interfaces With The Most Alerts

Network Node Dashboard view

The Network Node Dashboard view is a network device specific dashboard view. You can access this view by selecting the network device you wish to view information for, and then in the Tasks pane, clicking Network Node Dashboard. This view allows you to view the following information about a specific device:

- Vicinity view of the node
- Availability statistics of the node over the last 24 hours / 48 hours / 7 days / 30 days
- Node properties
- Average response time
- Processor usage over the last 24 hours
- Current node interface health
- Alerts generated by the node
- Alert details

Network Interface Dashboard view

Operations Manager monitors network interfaces, such as the ports on monitored switches, as long as they are connected to other devices that Operations Manager also monitors. For example, a port on a monitored switch will be monitored if it also connects to a computer that is monitored by Operations Manager. The Network Interface Dashboard view allows you to view information about a specific interface on a monitored network device. This dashboard is accessible through the Network Node Dashboard view by clicking on Network Interface Dashboard in the Health Of Interfaces on this node area. The Network Interface Dashboard view provides the following information:

- Bytes sent and received over the past 24 hours
- Packets sent and received over the past 24 hours
- Interface properties
- Send and receive errors and discards over the past 24 hours

- Network interface usage percentage
- Alerts generated by this interface
- Alert details

Exam Tip

Remember what is visible through the Network Interface Dashboard view.

Network Vicinity Dashboard

The Network Vicinity Dashboard allows you to view a diagram of a device and all of the monitored devices and computers that connect directly to that device. You can configure the Network Vicinity Dashboard to go beyond direct connection, expanding out to five levels of connection. The Network Vicinity Dashboard provides a graphical representation of each monitored object and the health of the connections between those objects.

More Info: **Network Devices and Data**

You can learn more about network devices and data at *http://technet.microsoft.com/en-us/library/hh212706.aspx*.

***Thought experiment*: Network device monitoring at Contoso**

You are in the process of deploying Operations Manager as a network monitoring device solution at Contoso. As part of this deployment, you are training the existing network monitoring team on the features of Operations Manager's network monitoring dashboards. With this in mind, answer the following questions:

1. Which dashboard would you use to view the list of network device interfaces in the organization that had the most send errors?
2. Which dashboard would you use to view the availability statistics of a particular network device over the last seven days?
3. Which dashboard would you use to view the number of bytes sent on a specific router interface where Operations Manager monitors the router?

Objective summary

- Automatic alert resolution allows you to specify how long it will be before an alert is in a new resolution state.
- Closing an alert generated by a monitor will mean no new alerts will be generated unless a state change occurs from healthy to warning, healthy to critical, or warning to critical.
- Closing an alert generated by a rule will close the current alert, but new alerts generated by the rule will still be displayed.
- To subscribe to an alert notification, you need to configure a notification action account, notification channel, notification subscriber, and a notification subscription.
- The Network Summary Dashboard provides information about monitored network devices.
- The Network Node Dashboard provides information about a specific monitored network device.
- The Network Interface Dashboard provides information about a specific monitored device interface.
- The Network Vicinity Dashboard provides information about monitored objects connected to a

monitored device.

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. A monitor is configured for a network device. In which of the following situations will an alert be generated?
   - **A.** Monitor state changes from healthy to critical
   - **B.** Monitor state changes from critical to healthy
   - **C.** Monitor state changes from warning to healthy
   - **D.** Monitor state changes from healthy to warning
2. You have imported a management pack for a network device that includes a monitor that raises an alert related to network connectivity. While you find this alert useful, you have noticed that the alert does not automatically resolve itself when the monitor returns to a healthy state. Which of the following parameters would you configure an override for on the monitor to ensure that the alert was automatically resolved when the monitor returned to a healthy state?
   - **A.** Alert On State
   - **B.** Alert Priority
   - **C.** Alert Severity
   - **D.** Auto-Resolve Alert
3. Which of the following statements about closing alerts generated by rules and monitors is true?
   - **A.** If you close an alert generated by a monitor without resolving the issue that generated the alert, the monitor will generate another alert.
   - **B.** If you close an alert generated by a rule without resolving the issue that generated the alert, the rule will generate another alert.
   - **C.** If you close an alert generated by a monitor without resolving the issue that generated the alert, the monitor will not generate another alert.
   - **D.** If you close an alert generated by a rule without resolving the issue that generated the alert, the rule will not generate another alert.
4. Which of the following Operations Manager network dashboards would you use to determine the monitored servers connected to a specific monitored switch?
   - **A.** Network Summary Dashboard
   - **B.** Network Node Dashboard view
   - **C.** Network Interface Dashboard view
   - **D.** Network Vicinity Dashboard
5. Which of the following Operations Manager network dashboards would you use to determine the statistics of a switch uplink port that connected two network switches monitored by Operations Manager?
   - **A.** Network Vicinity Dashboard
   - **B.** Network Interface Dashboard view
   - **C.** Network Node Dashboard view
   - **D.** Network Summary Dashboard

Objective 3.2: Monitor servers

Once you have configured Operations Manager to collect data from the servers in your environment, you will need to configure how Operations Manager displays and interprets that data, including configuring notifications and alerts about important items that should be brought to the attention of the people responsible for monitoring these computers. Managing servers also involves following up on agents that are reporting problems, being able to put monitored objects into maintenance mode, understanding how heartbeat alerts work, as well as configuring health explorer, and audit collection services.

This section covers the following topics:

- Understanding not monitored and gray agents
- Using maintenance mode
- Understanding heartbeat alerts
- Using Health Explorer
- Configuring Audit Collection Services (ACS)

Understanding not monitored and gray agents

In some scenarios, you'll find computers that you've just deployed the Operations Manager agent to, listed as having a healthy agent status, also shown to be in a not monitored state. Figure 3-27 shows several computers with this status. A computer is in a state where the Operations Manager agent is shown to be in a healthy state and the computer is not monitored when the management pack for the computer's operating system is not installed. For example, the computers shown below are in this state because it was only after I took this screenshot that I installed the Windows Server 2012 R2 related management packs.

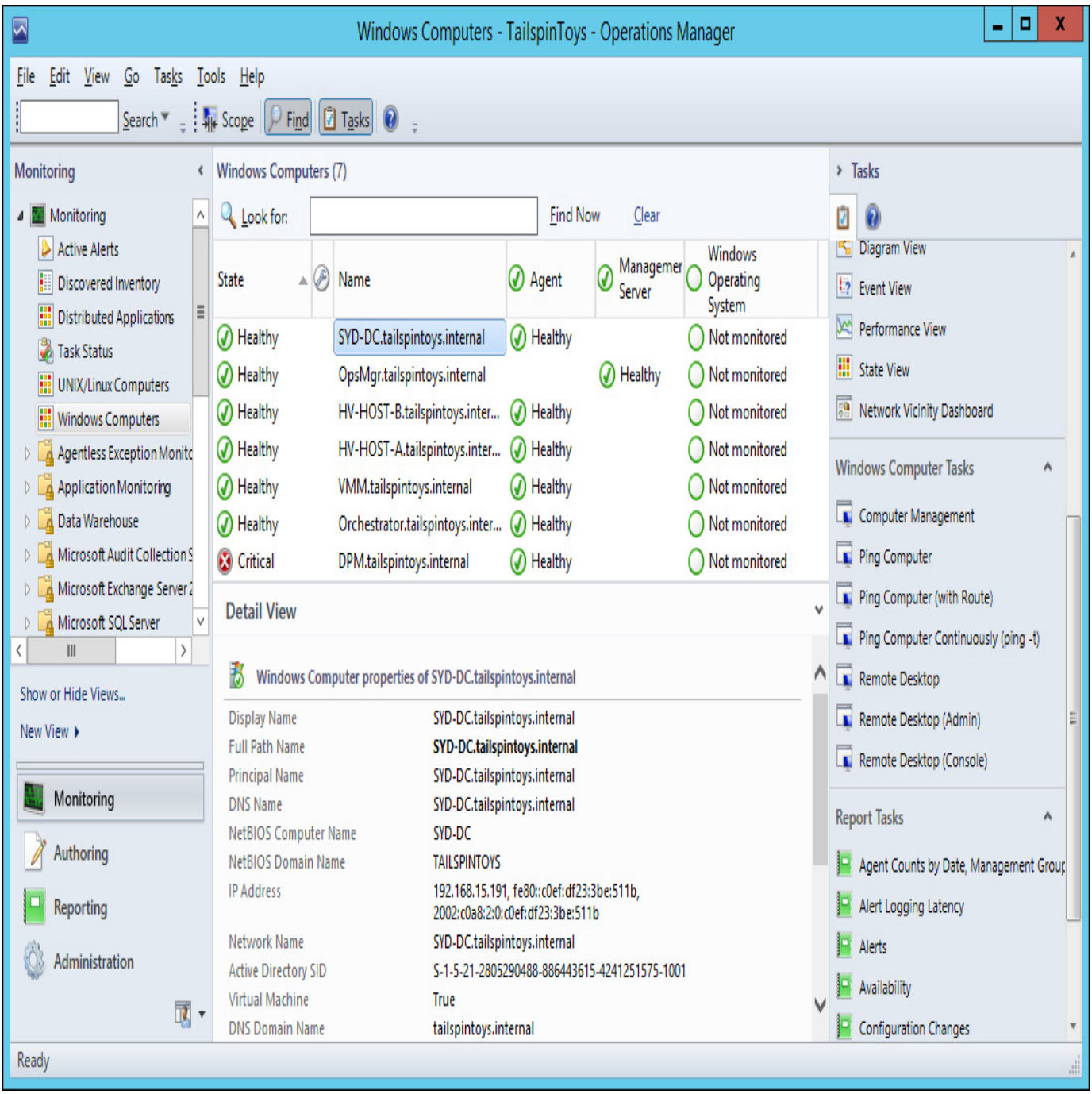

FIGURE 3-27 Not monitored

Another reason why the status of a server might show as not monitored is because you have uninstalled and then reinstalled it. The default configuration of Operations Manager has the grooming of deleted agents occur after 48 hours. If the previous agent information is still in the database, the newly installed agent won't be recognized.

If the Operations Manager agent is shown as healthy, but is dimmed, it means that the health service on the monitored computer is not receiving heartbeat data from the Operations Manager agent. The healthy status is shown in gray because everything was functioning properly at some point in the recent past. Common causes for a gray state include:

- Heartbeat failure
- Nonfunctioning health service
- Improper configuration
- System workflows failure
- Poor Operations Manager or data warehouse database performance
- Network problems
- Authentication issues

When diagnosing the cause of gray agents, you can run the Show Gray Agent Connectivity Data task. This will provide the following information:

- The last time a management server received a heartbeat from the agent.
- The status of the System Center Management Health service.
- Whether the agent responds to ping requests.
- The last time the agent's configuration was updated.
- The management server to which the agent reports.

More Info: **Not Monitored and Gray Agents**

You can learn more about not monitored and gray agents at *http://technet.microsoft.com/en-us/library/hh212870.aspx*.

Using maintenance mode

You use maintenance mode to apply a special status to a monitored object to stop errors and alerts occurring when you are performing maintenance tasks on that object. For example, you want to restart a server to apply software updates or shut it down temporarily to change the hardware configuration. Prior to performing these maintenance tasks, you would use the Operations Manager console to place the server into maintenance mode so that the server restarting or going offline does not trigger a host of alerts and notifications. Enabling maintenance mode suspends the following features:

- Rules and monitors
- Notifications
- Automatic responses
- State changes
- New alerts

To put a computer into maintenance mode, perform the following steps:

1. In the Operations Manager console, click the Windows Computers node under the Monitoring node. This node is shown with the computer SYD-DC.tailspintoys.internal selected in Figure 3-28.

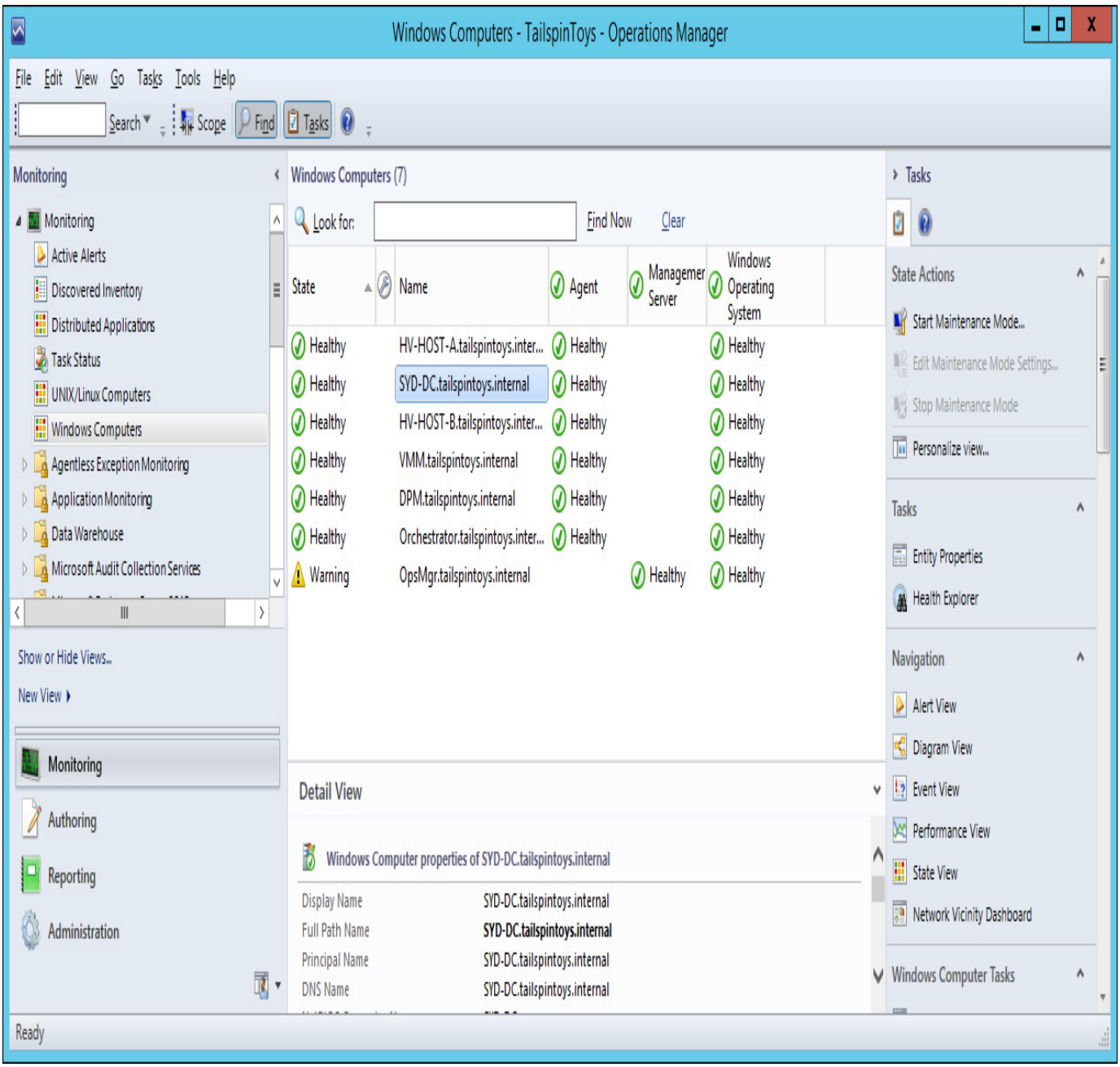

FIGURE 3-28 Windows Computers node

2. With the computer that you want to put into maintenance mode selected, click Start Maintenance mode on the Tasks menu.
3. In the Maintenance Mode Settings dialog box, shown in Figure 3-29, configure the following settings:
   - **Apply To** You can select between the selected object, and the selected object and all contained object.
   - **Category** You can use this to specify the reason for the object being put into maintenance mode. You can select whether the maintenance mode is planned, and can specify one of the following reasons:
   - Other (Planned/Unplanned)
   - Hardware: Maintenance (Planned/Unplanned)
   - Hardware: Installation (Planned/Unplanned)
   - Operating System: Reconfiguration (Planned/Unplanned)
   - Application: Maintenance (Planned/Unplanned)
   - Application: Installation (Planned/Unplanned)
   - Security Issue

- **Duration** You can specify the number of minutes, or a specific end time for the maintenance mode status.

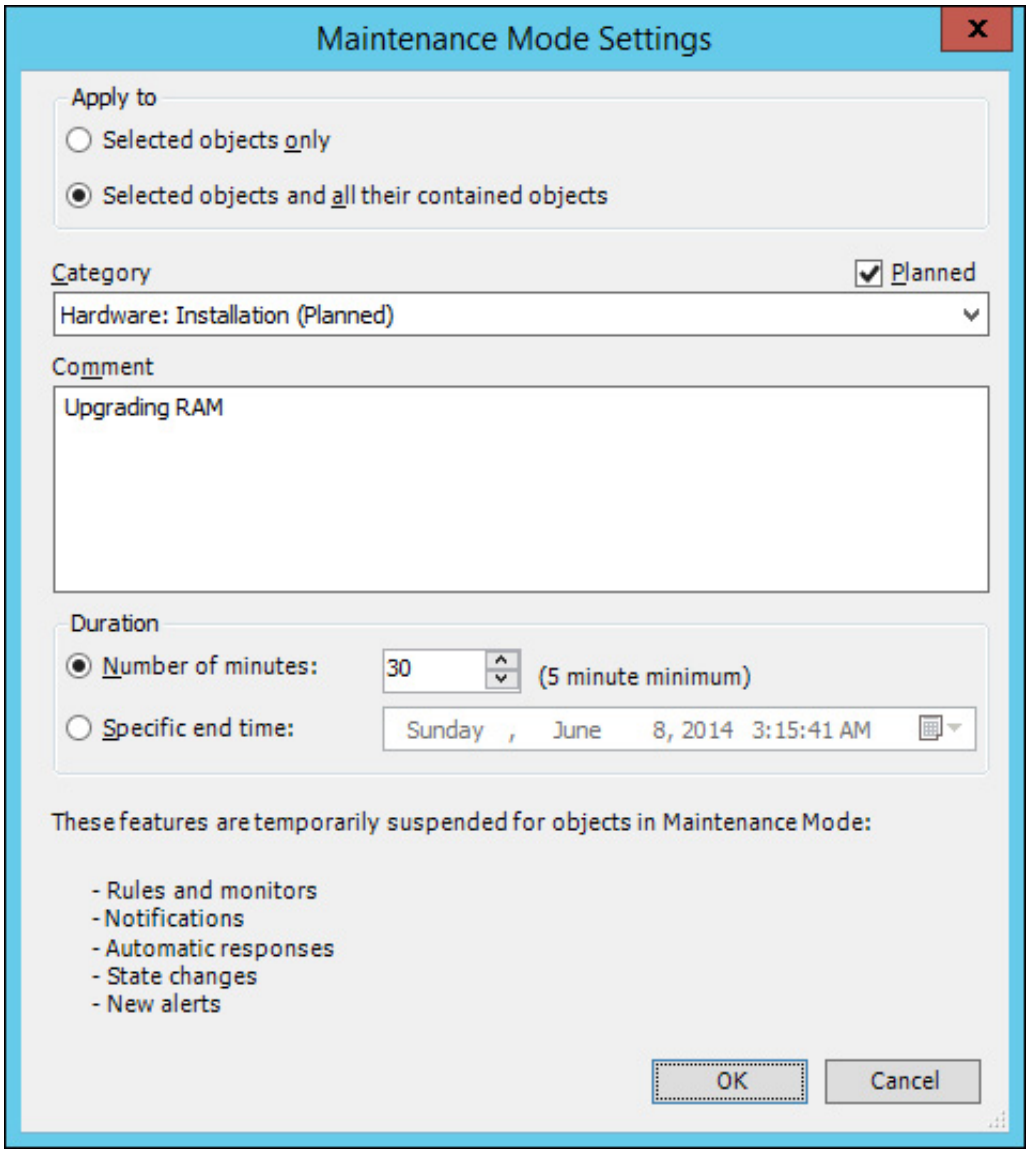

FIGURE 3-29 Maintenance Mode Settings

4. Once in maintenance mode, a maintenance mode icon, like the one shown in Figure 3-30, will appear next to the computer until the maintenance period expires.

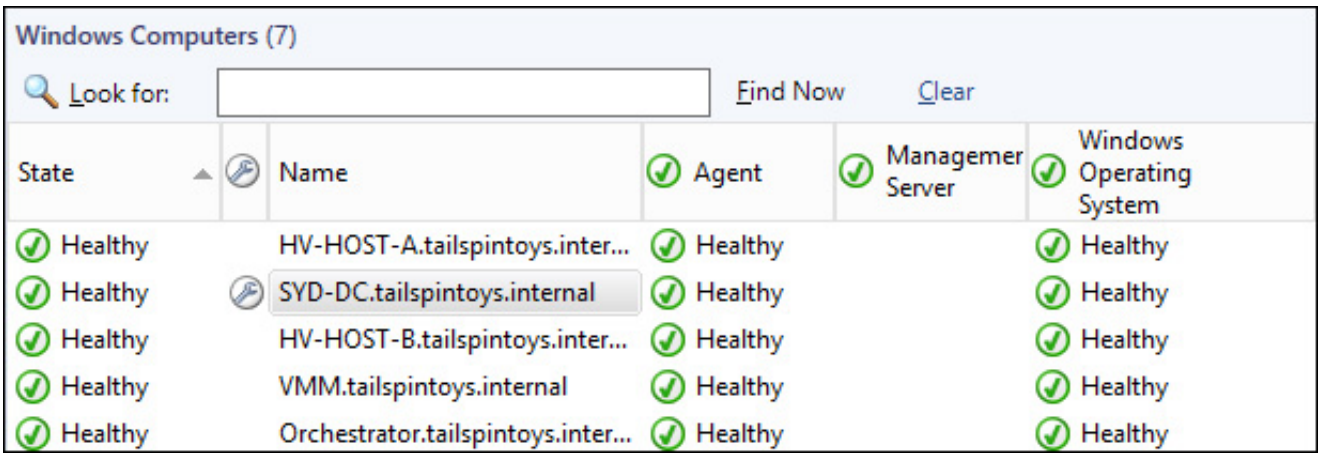

FIGURE 3-30 Maintenance mode icon

You can edit maintenance mode, for example to increase the amount of time that the maintenance period lasts, by right-clicking the object, and clicking Maintenance Mode, and then clicking Edit Maintenance Mode settings. This will return you to the Maintenance Mode Settings dialog box that you can use to change the maintenance mode settings.

Exam Tip

Remember how to extend maintenance mode.

You can stop maintenance mode on a computer by clicking the computer in the Windows Computers node of the Monitoring workspace, and clicking Stop Maintenance Mode. You will then be prompted to confirm that you want to stop maintenance mode, as shown in Figure 3-31.

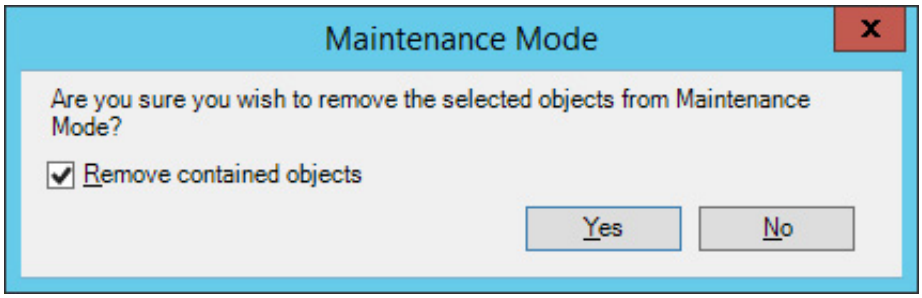

FIGURE 3-31 Maintenance Mode

More Info: **Maintenance Mode**

You can learn more about maintenance mode at *http://technet.microsoft.com/en-us/library/hh212870.aspx*.

Understanding heartbeat alerts

A heartbeat is a UDP packet sent on port 5723 every 60 seconds that Operations Manager uses to monitor communication channels between the Operations Manager agent and its primary management server. If the Operations Manager management server fails to receive four consecutive heartbeats from an agent, two things happen:

- Operations Manager will generate a Health Service Heartbeat Failure alert, as shown in Figure 3-32.

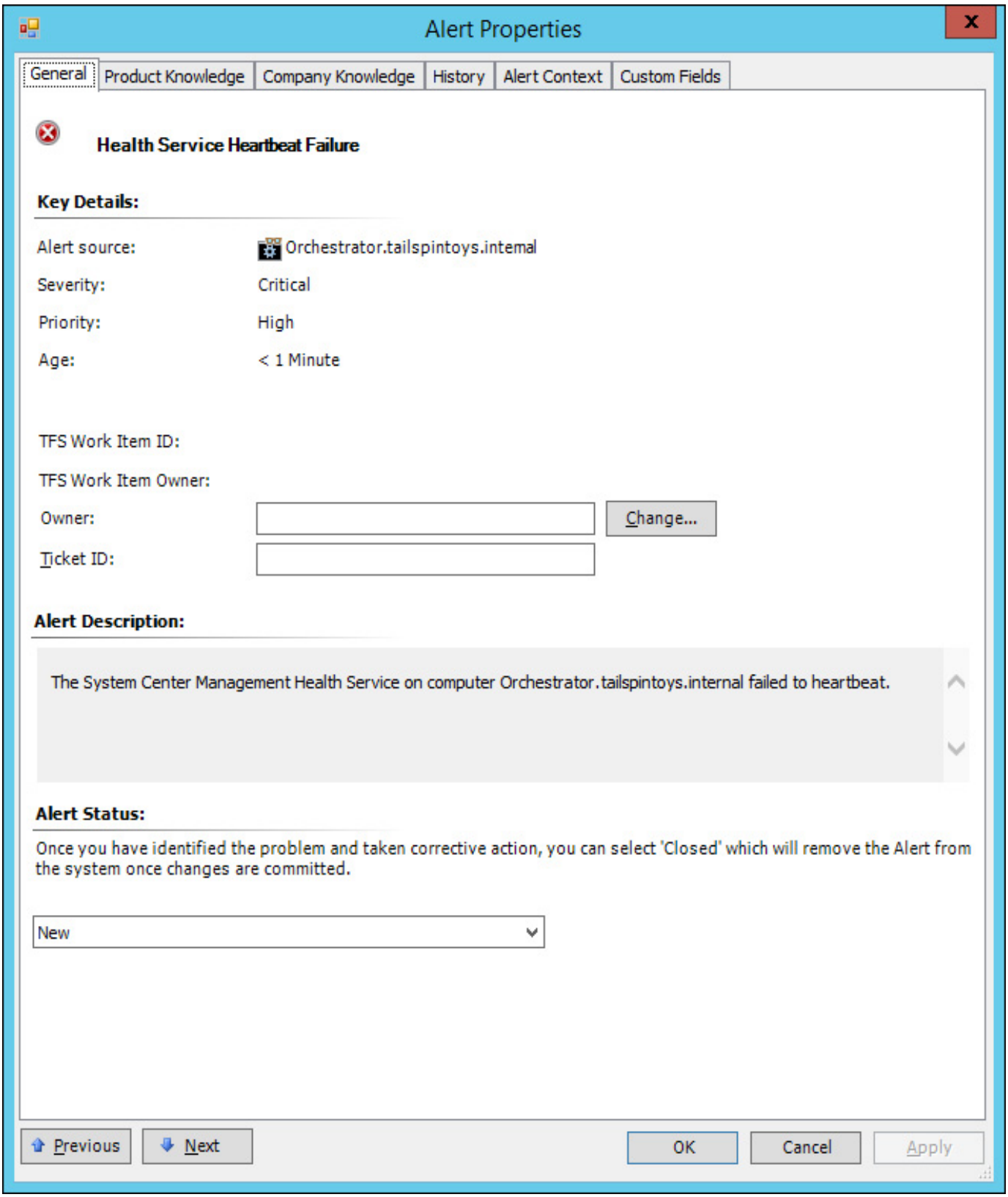

FIGURE 3-32 Alert properties

- The management server will attempt to ping the computer that hosts the agent.

If the computer that hosts the agent does not respond to the ping request, Operations Manager will generate a Failed To Connect To Computer alert. If you see the Health Service Heartbeat Failure alert, but not the Failed To Connect To Computer alert, you can deduce that there is a problem with the Operations Manager agent, as the computer itself remains contactable. Both of these alerts will be closed automatically once heartbeat traffic resumes.

You can change the heartbeat settings for all management servers by performing the following steps:

1. In the Settings node of the Administration workspace of the Operations Manager console, click Heartbeat under Agent, and then click Properties.
2. On the Global Agent Settings dialog box, shown in Figure 3-33, adjust the heartbeat interval to

the desired figure.

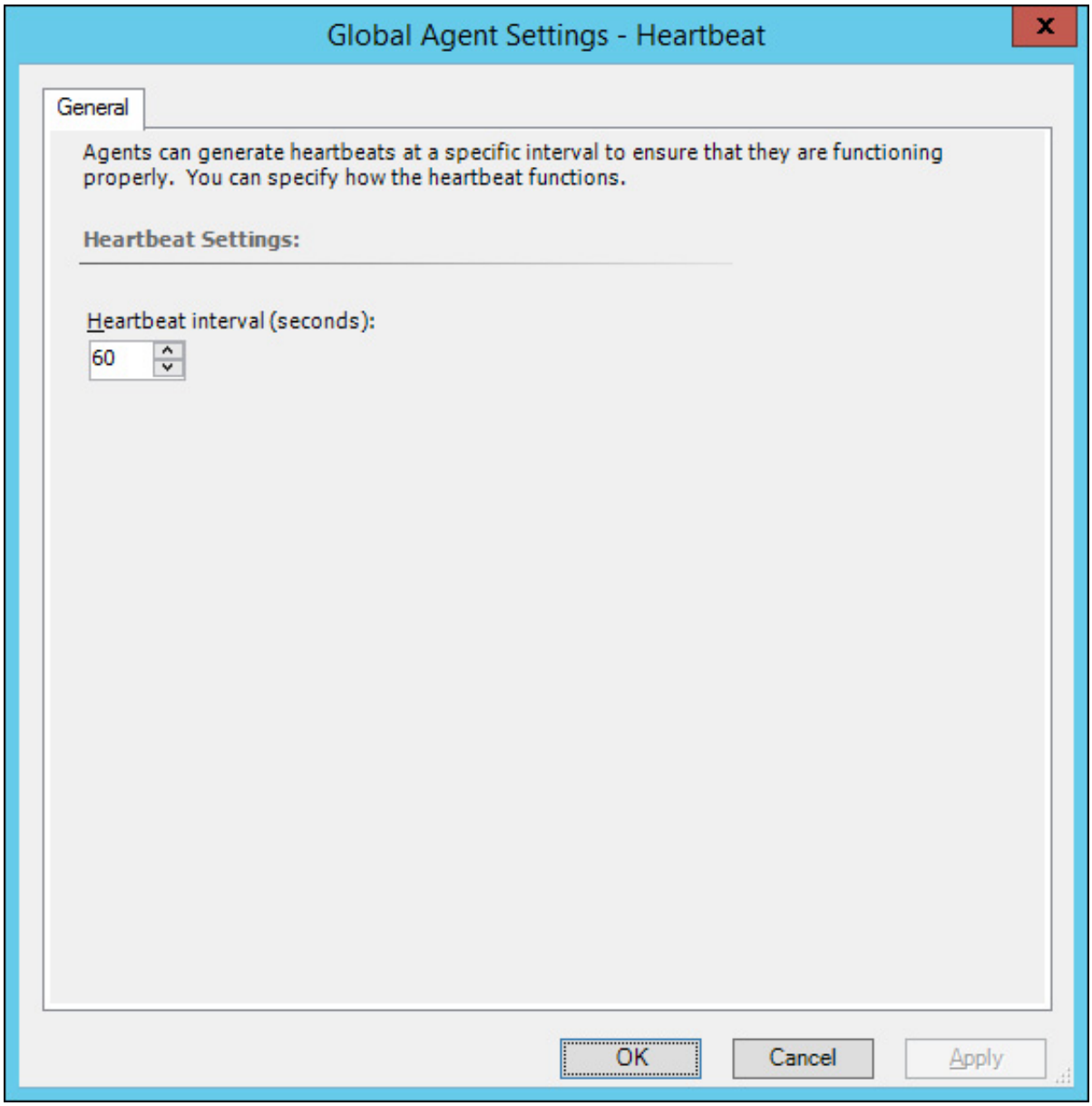

FIGURE 3-33 Global heartbeat settings

3. Under Server, click Heartbeat, and then click Properties in the Tasks pane.
4. On the Global Management Server Settings - Heartbeat dialog box, set the Number Of Missed Heartbeats Allowed, as shown in Figure 3-34.

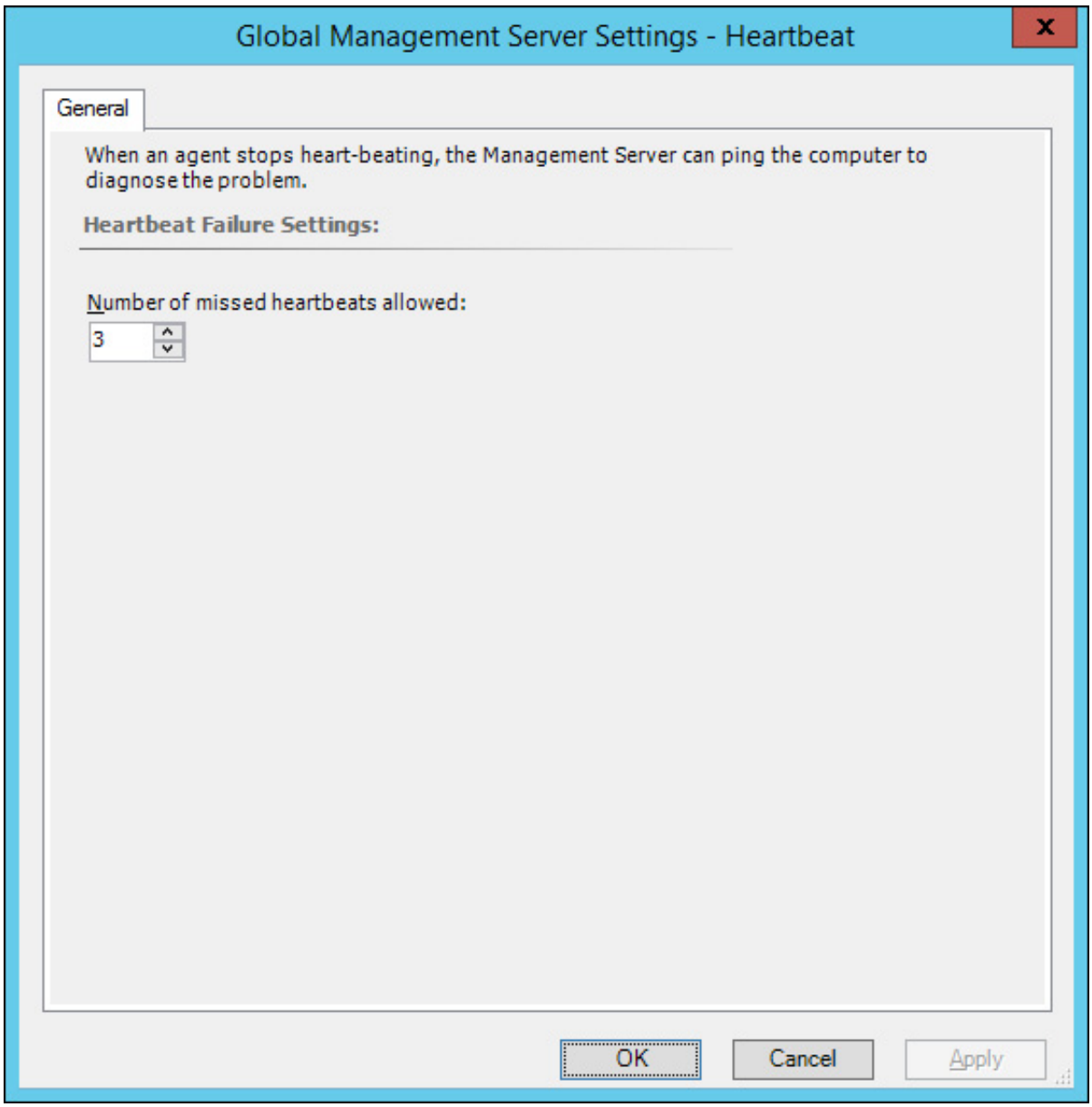

FIGURE 3-34 Heartbeat settings

You can change the heartbeat settings for an individual computer by performing the following steps:

1. In the Agent Managed node of the Administration workspace of the Operations Manager console, click the computer for which you want to change the heartbeat settings, and then click Properties in the Tasks pane.
2. On the Heartbeat tab of the Agent Properties dialog box, select the Override Global Agent Settings check box, and specify the new Heartbeat settings. Figure 3-35 shows the heartbeat interval for computer Orchestrator.tailspintoys.internal set to 90 seconds.

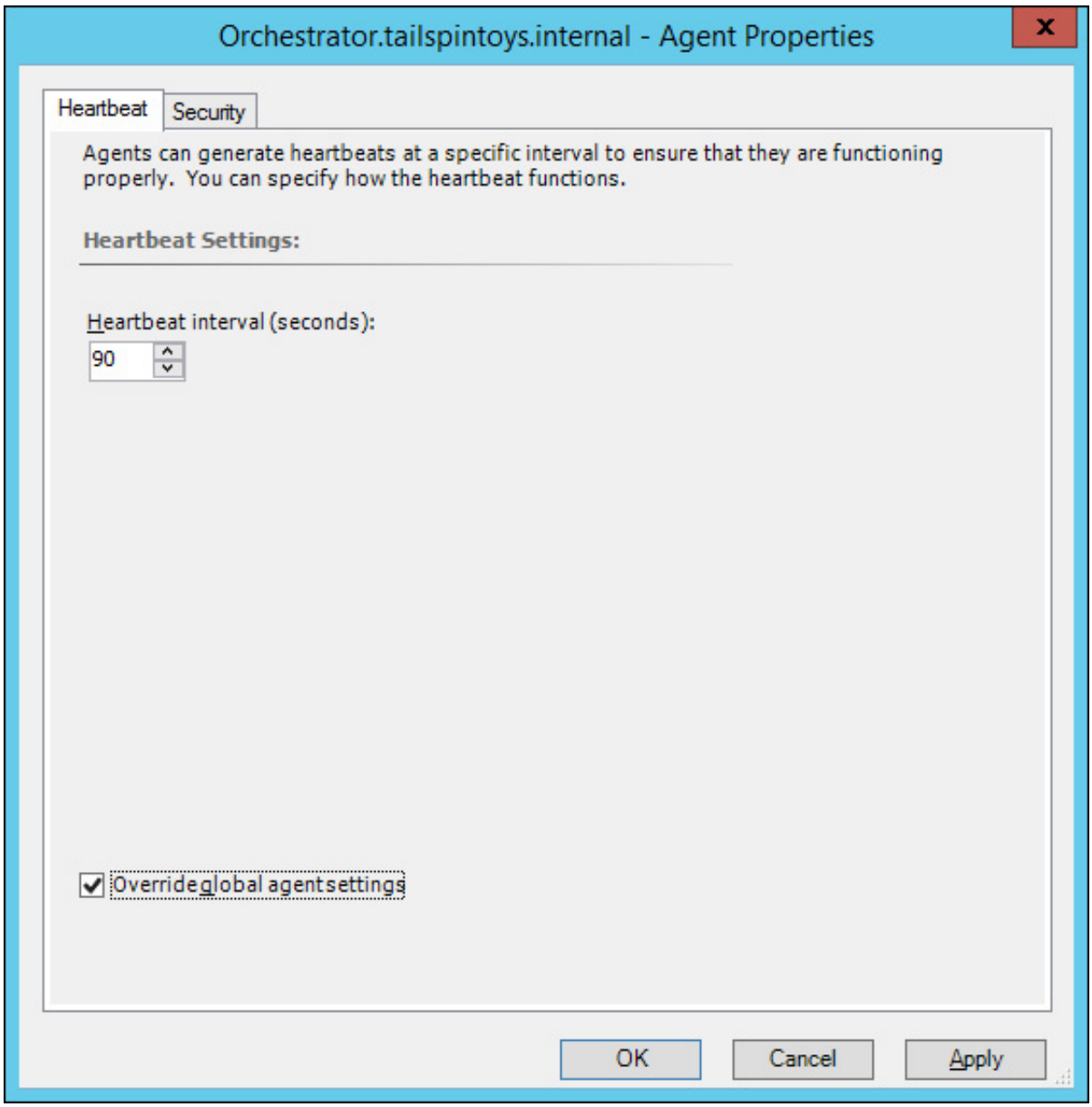

FIGURE 3-35 Individual server heartbeat settings

You can trigger a Health Service Heartbeat Failure alert for testing purposes by stopping the Microsoft monitoring agent (formerly System Center Management service) on a computer with an agent installed, as shown in Figure 3-36.

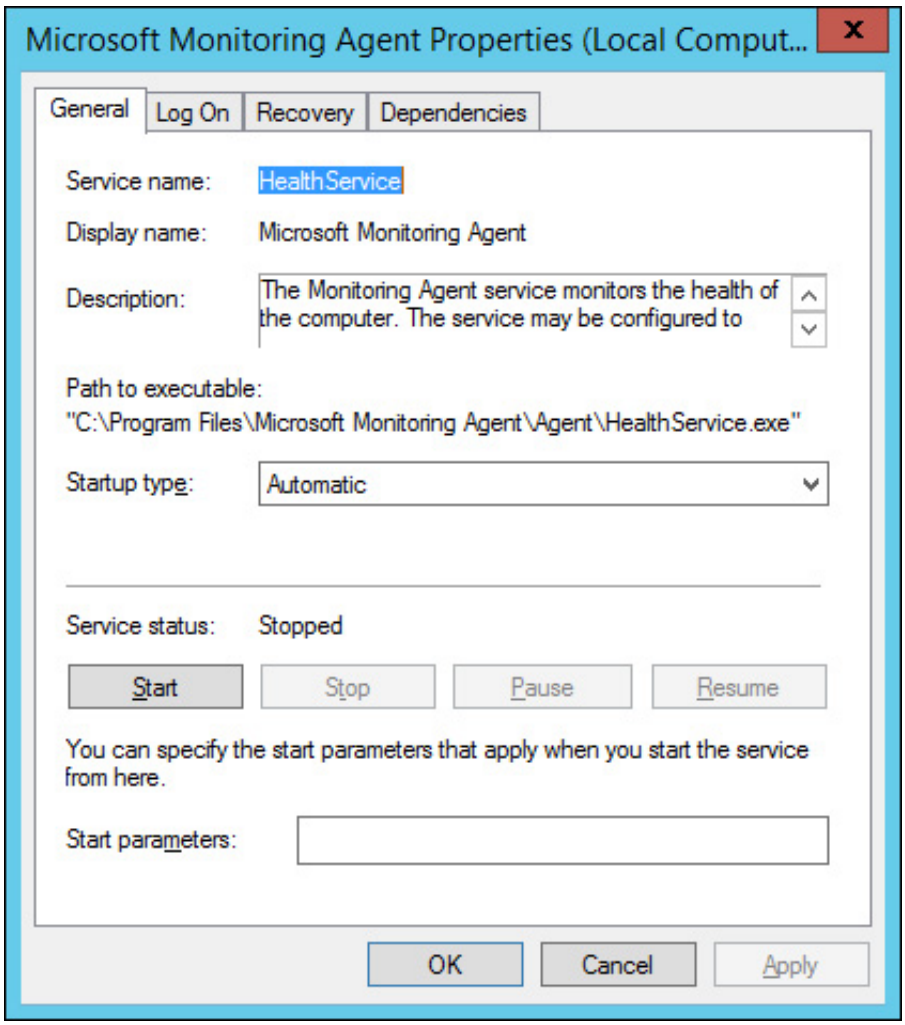

FIGURE 3-36 Stopped health service

More Info: **Heartbeat Alerts**

You can learn more about heartbeat alerts at *http://technet.microsoft.com/en-us/library/hh212798.aspx*.

Using Health Explorer

The Health Explorer tool allows you to view the health of an entity, for example the health of a monitored computer. Health Explorer also allows you to view the history of state changes for that object. For example, Figure 3-37 shows the Health Explorer for the computer Orchestrator.tailspintoys.com. You can see in the figure where the health state of the computer has changed between healthy to warning, and then from warning back to healthy.

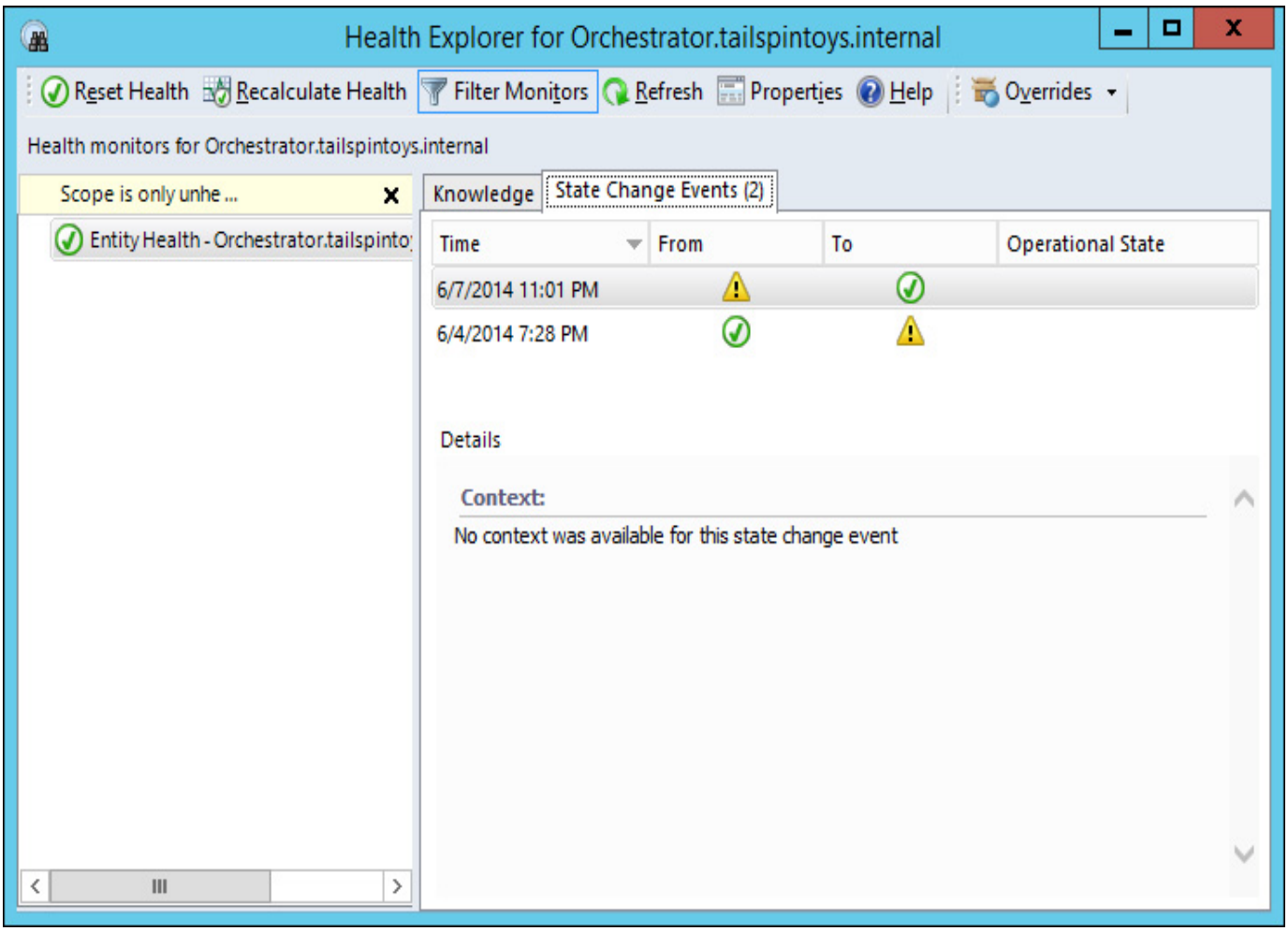

FIGURE 3-37 State change events

Through Health Explorer, you can view the alerts that are present on a particular entity. Figure 3-38 shows the alerts that are relevant to the monitored computer Orchestrator.tailspintoys.internal. You can use Health Explorer to locate all of the monitors that are in a state that requires attention. This allows you to quickly assess and diagnose the issues with a particular computer, which might be responsible for a multitude of separate alerts.

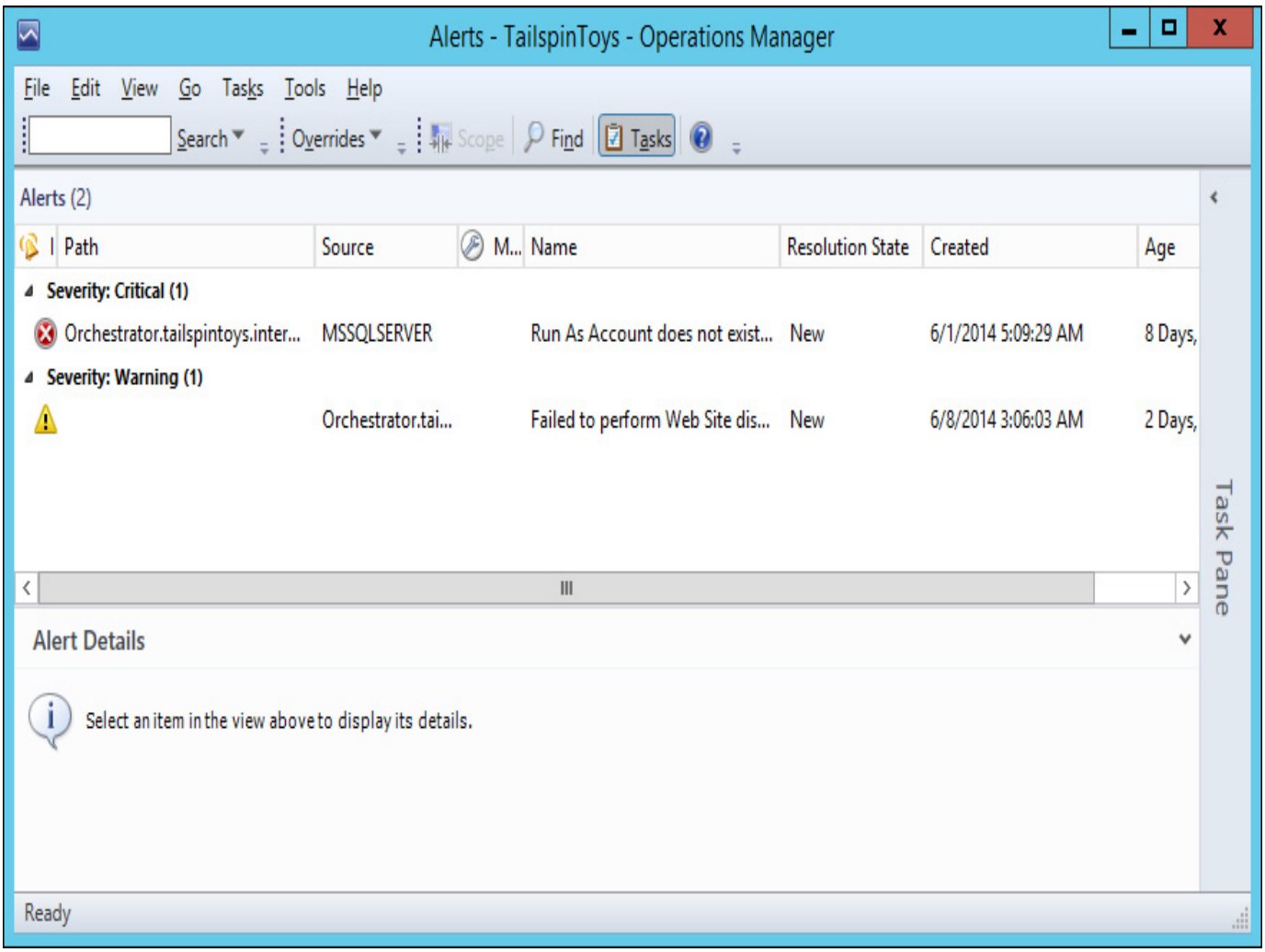

FIGURE 3-38 Alerts

More Info: **Health Explorer**

You can learn more about using Health Explorer at *http://technet.microsoft.com/en-us/library/hh212766.aspx*.

Configuring Audit Collection Services

One of the challenges of using the built-in auditing capabilities of Windows computers is that each computer stores event logs locally. While it is possible to configure event log forwarding as a way of centralizing the storage of event logs, event log data is still kept in the standard event log format, making it challenging to analyze.

Audit Collection Services (ACS) is a segment of Operations Manager that allows you to collect event log records generated by an audit policy, and to place them in a SQL Server database. With ACS, you can then use SQL Server tools, including data analysis and reporting tools, to analyze security events generated by some or all of the computers in your organization.

ACS uses the following segments:

- ACS forwarders
- ACS collectors
- ACS database

ACS forwarders

ACS forwarders forward security event log information to ACS collectors. The ACS forwarder is part of the Operations Manger agent. While the service is installed, the ACS forwarder will not be active until you run the Enable Audit Collection task. Once this task has been run, all events that would normally be written to the computer's Security log are also forwarded to the ACS collector.

To configure a computer as an ACS forwarder, perform the following steps:

1. In the Monitoring workspace of the Operations console, expand Operations Manager, expand Agent Details, and then select Agent Health State.
2. Two panes are displayed. In the right pane, select all of the computers that you want to configure as ACS forwarder, as shown in Figure 3-39, and then click Enable Audit Collection under Health Service Tasks.

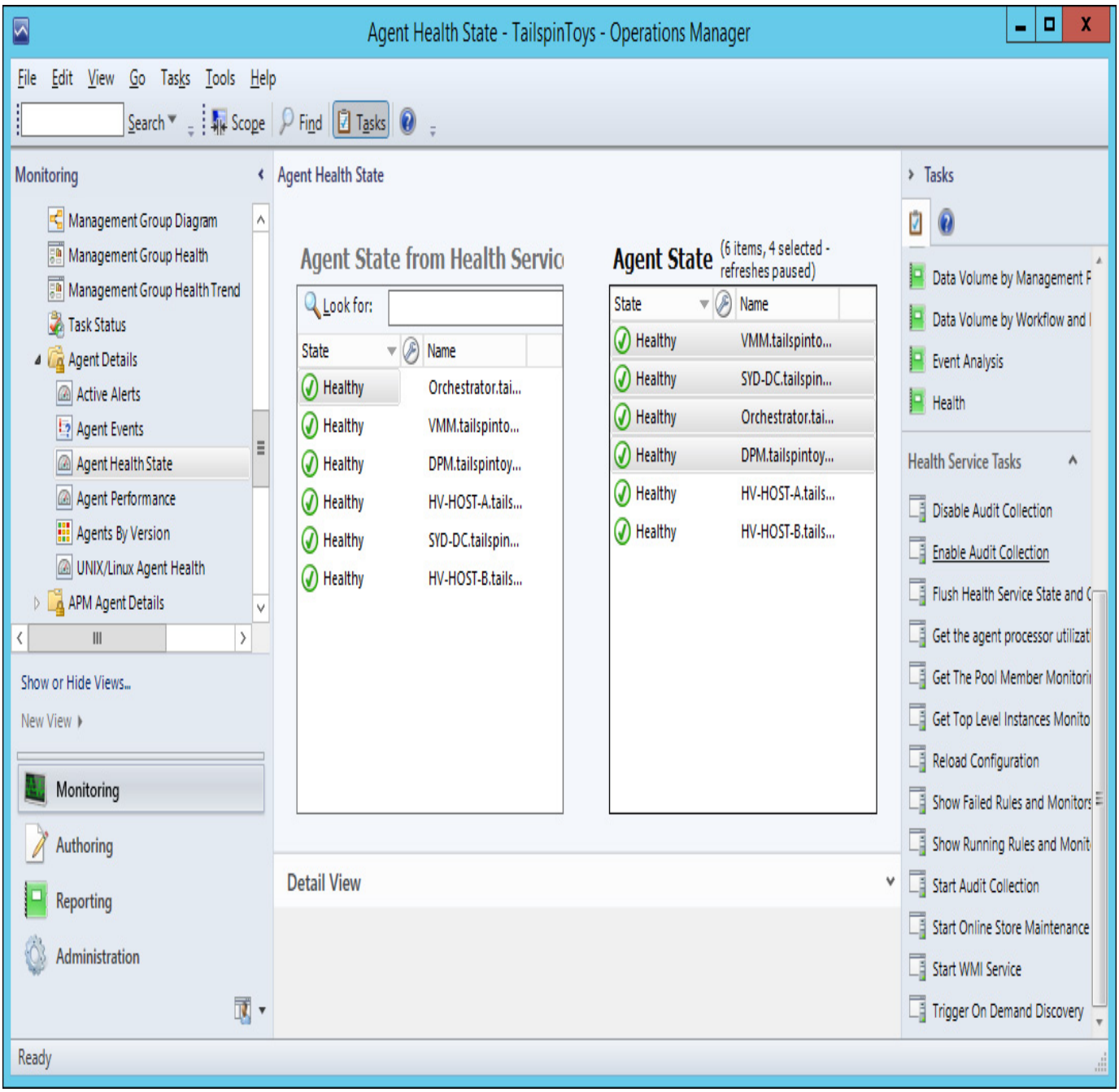

FIGURE 3-39 Enable audit collection

3. On the Run Task - Enable Audit Collection, click Override under Task Parameters.
4. On the Override Task Parameters dialog box, enter the FQDN of the ACS collector, as shown in Figure 3-40, and click Override.

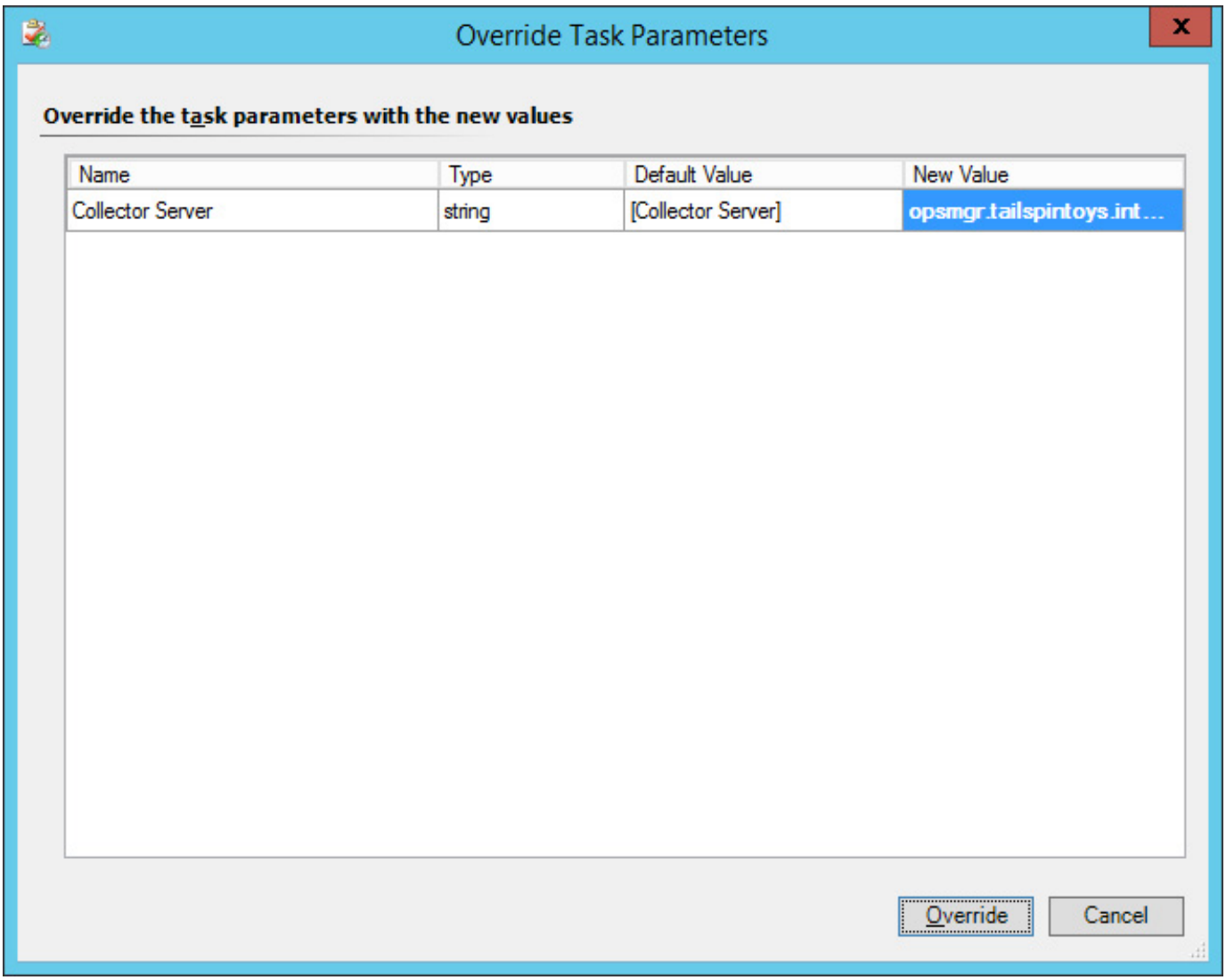

FIGURE 3-40 Set collector server

5. Verify that the Collector Server is listed properly under Task Parameters, as shown in Figure 3-41, and click Run.

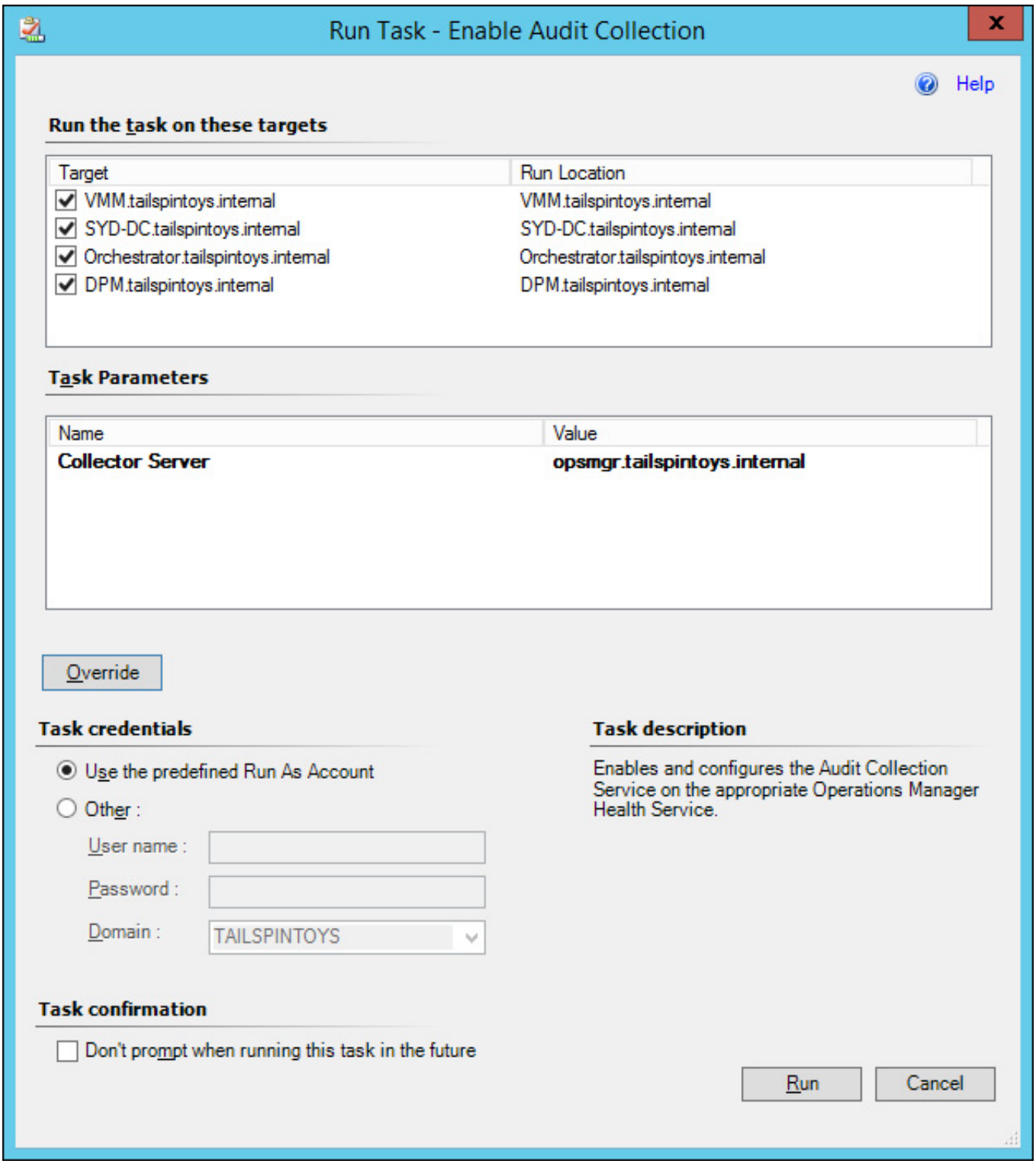

FIGURE 3-41 Enable audit collection

ACS collectors

A computer that functions as an ACS collector processes security event information forwarded by ACS forwarders, and then forwards this data to the ACS database. Microsoft recommends that you don't install the ACS collector on an Operations Manager management server. This is because the ACS collector role can place an undue performance burden on the management server.

It is possible to deploy multiple ACS collectors. Each ACS collector requires an individual ACS database. ACS collectors require the following:

- An Operations Manager management server must be present.
- The server that hosts the ACS collector role must be a member of an Active Directory domain that is in the same forest as the Operations Manager management server.
- The server that hosts the ACS collector role has a minimum of 1 GB of RAM, with 2GB or more recommended, and 10 GB of free space to store the ACS database.

ACS database

The ACS database hosts all of the security event log items forwarded to the ACS collectors by the ACS forwarders. System Center 2012 Operations Manager SP1 and System Center 2012 R2 Operations Manager support using SQL Server 2008 R2 SP1 and later, and SQL Server 2012 and later to host the ACS database. Microsoft recommends using the Enterprise rather than Standard edition of SQL Server because of the performance requirements involved in processing traffic from the ACS forwarder.

To install the ACS collector and ACS database role, perform the following steps:

1. On the Operations Manager installation screen, shown in Figure 3-42, click Audit Collection Services in the list of Optional Installations. This will start the Audit Collection Services Collector Setup Wizard.

FIGURE 3-42 Installation dialog box

2. After accepting the license terms, select Create A New Database, and enter the data source name and the database instance details.
3. On the Database Authentication page, select whether Windows or SQL authentication is being used, and the folders that will store the database and log files.
4. On the Event Retention Schedule page, shown in Figure 3-43, specify how long events will be retained in the database.

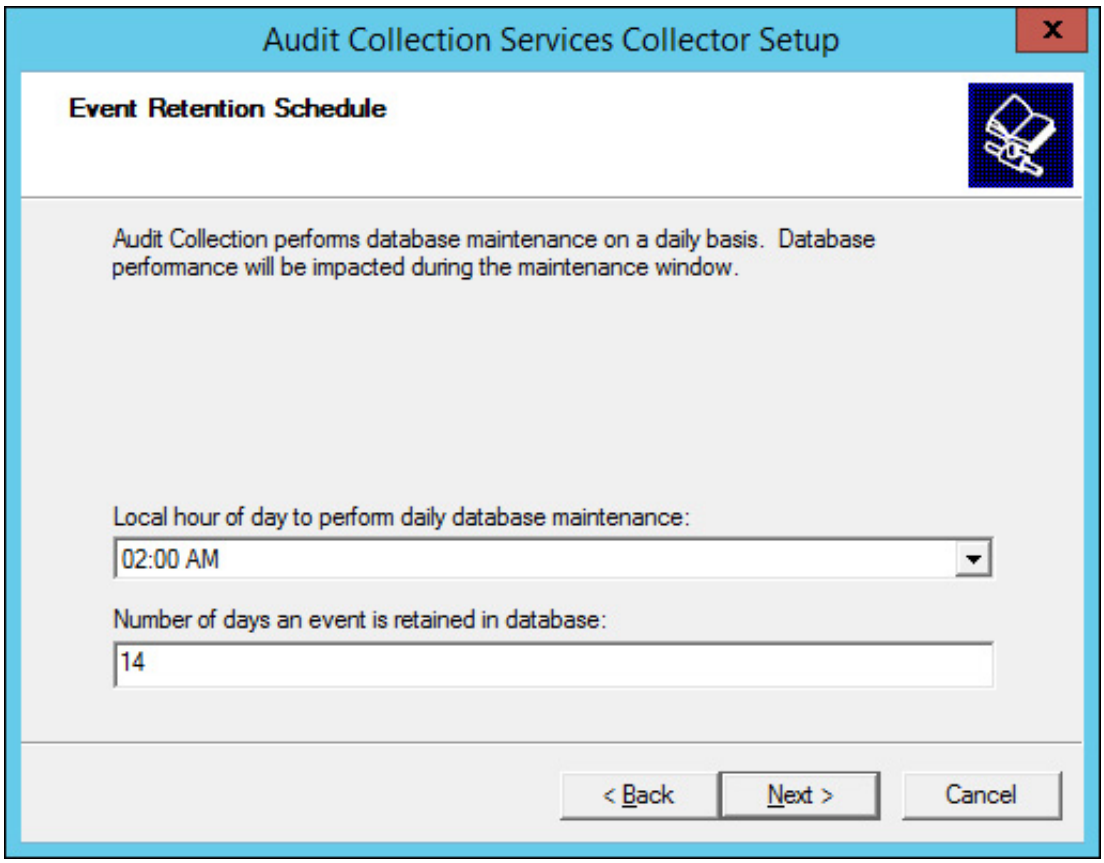

FIGURE 3-43 ACS collector setup

5. On the ACS Stored Timestamp Format page, choose between Local Time or Universal Coordinated Time, and then complete the Setup Wizard.

ACS and Dynamic Access Control

System Center 2012 SP1 Operations Manager and later supports integration with Dynamic Access Control. Dynamic Access Control allows audit policies based on user, resource, environmental claims, and properties. Operations Manager doesn't require additional configuration to support integration with Dynamic Access Control. Interaction with this feature is through additional reports that become available when you install ACS Reporting

---

More Info: **Audit Collection Services**

You can learn more about using Audit Collection Services at *http://technet.microsoft.com/en-us/library/hh212908.aspx*.

***Thought experiment*: Server monitoring at Margie's Travel**

You are working on some issues related to the monitoring of server operating systems at Margie's travel. Specifically:

- You have deployed the Operations Manager agent to 10 new servers running the Windows Server 2012 R2 operating system. Each of these servers is shown in the Monitoring console as having a healthy agent, but is also listed as not monitored.
- In the last day, two servers have switched from having their health statuses displayed in green in the Monitoring workspace of the Server Manager console, to having their health statuses displayed in gray.

With this information in mind, answer the following questions:

1. What steps can you take to ensure that all of the computers with the Windows Server 2012 R2 operating system are no longer listed as not monitored?
2. Which service should you check first, on the two servers with a gray health status?

Objective summary

- An agent may show a server to be in a not monitored state because the management pack of the host operating it is not installed on the Operations Manager management server.
- Maintenance mode suspends rules and monitors, notifications, automatic responses, state changes, and new alerts.
- An Health Service Heartbeat Failure alert will be triggered if the Operations Manager server fails to receive four consecutive heartbeats from an agent.
- When a Health Service Heartbeat Failure alert is triggered, the Operations Manager server attempts to ping the computer. If the computer does not respond to the ping request, a Failed To Connect To Computer alert will be raised.
- An ACS forwarder is installed on a computer that will forward security event logs to an ACS collector.
- An ACS collector processes data forwarded from an ACS forwarder, and sends it to the ACS database.

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. A Health Service Heartbeat Failure alert for computer SYD-FS1 is present in alerts view. You look for a Failed To Connect To Computer alert in alerts view, but one is not present. Which of the following diagnoses is probable given this state of affairs?
   - **A.** SYD-FS1 is in a healthy state.
   - **B.** There is a problem with the Operations Manager agent on SYD-FS1.
   - **C.** The Operations Manager management server is unable to ping SYD-FS1.
   - **D.** SYD-FS1 has been assigned a new IP address.
2. You have five domain controllers that audit user logon activity. You want to deploy Operations Manager Audit Collection Services on a new server named ACS1. ACS1 will host the ACS database. Which of the following answers best describes how you should deploy ACS roles in this scenario?
   - **A.** Enable the ACS forwarder role on each domain controller

B. Install the ACS collector role on each domain controller

C. Enable the ACS forwarder role on ACS1.

D. Enable the ACS collector role on ACS1.

3. Which of the following is disabled or suspended when you put a monitored server into maintenance mode using the Operations Manager console?

A. Microsoft monitoring agent service on the monitored server.

B. Rules and monitors related to the monitored server.

C. New alerts from the monitored server.

D. Message queuing service on the monitored server.

Objective 3.3: Monitor the virtualization layer

Once you have configured Operations Manager to collect data from virtualization hosts and virtual machines, you need to configure how Operations Manager displays and interprets that data. This means configuring notifications and alerts through to analyzing overall virtualization layer health. When integrated with Virtual Machine Manager, Operations Manager provides a number of dashboards and views that allow you to monitor the functionality and performance of your organization's fabric.

This section covers the following topics:

- Integrating Operations Manager with Virtual Machine Manager
- Using the Fabric Health Dashboard
- Understanding the Fabric Monitoring Diagram view

Integrating Operations Manager with Virtual Machine Manager

To be able to monitor your organization's virtualization layer when you are using a System Center 2012 and System Center 2012 R2 managed private cloud, you need to integrate Operations Manager with Virtual Machine Manager.

Integrating Operations Manager with Virtual Machine Manager provides you with the following dashboards and views as shown in Figure 3-44:

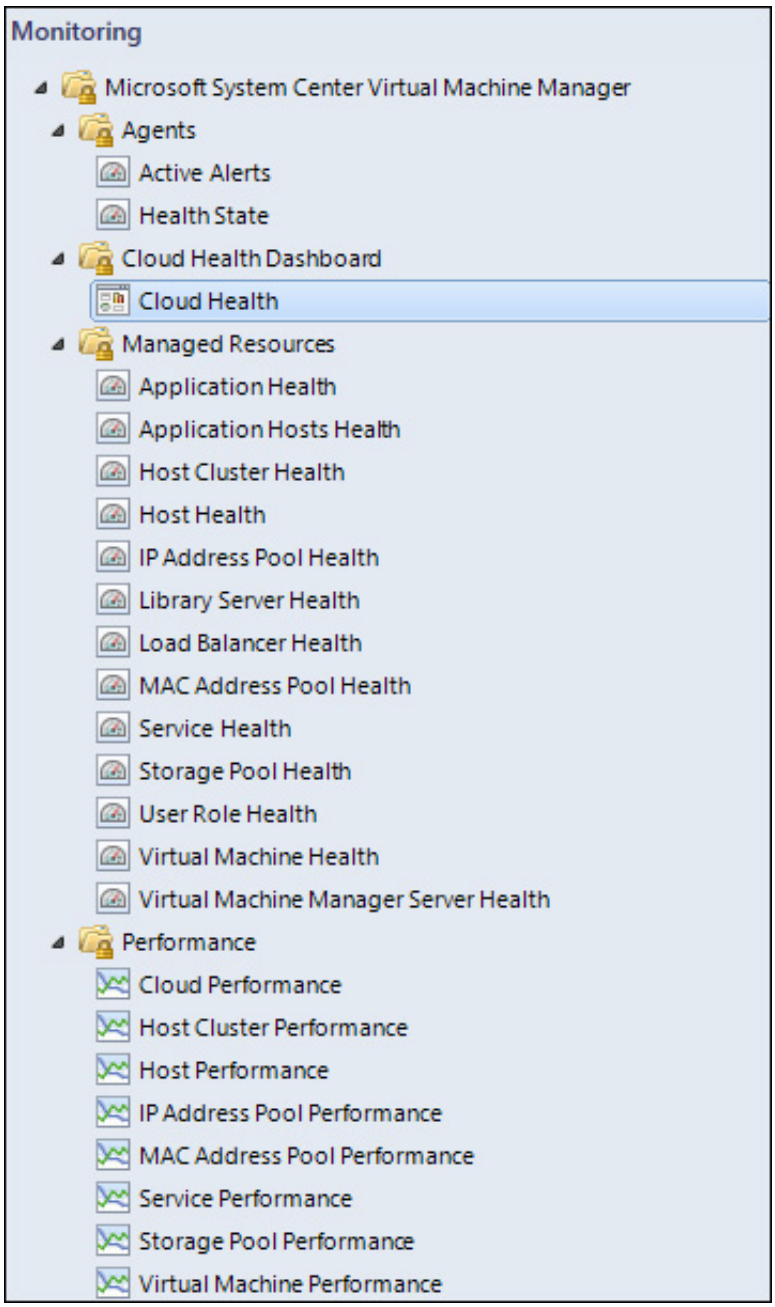

FIGURE 3-44 Virtualization dashboards and views

- Cloud Health
- Application Health
- Application Hosts Health
- Host Cluster Health
- Host Health
- IP Address Pool Health
- Library Server Health
- Load Balancer Health
- MAC Address Pool Health
- Service Health
- Storage Pool Health
- User Role Health
- Virtual Machine Health
- Virtual Machine Manager Server Health

The Virtual Machine Health dashboard is shown in Figure 3-45.

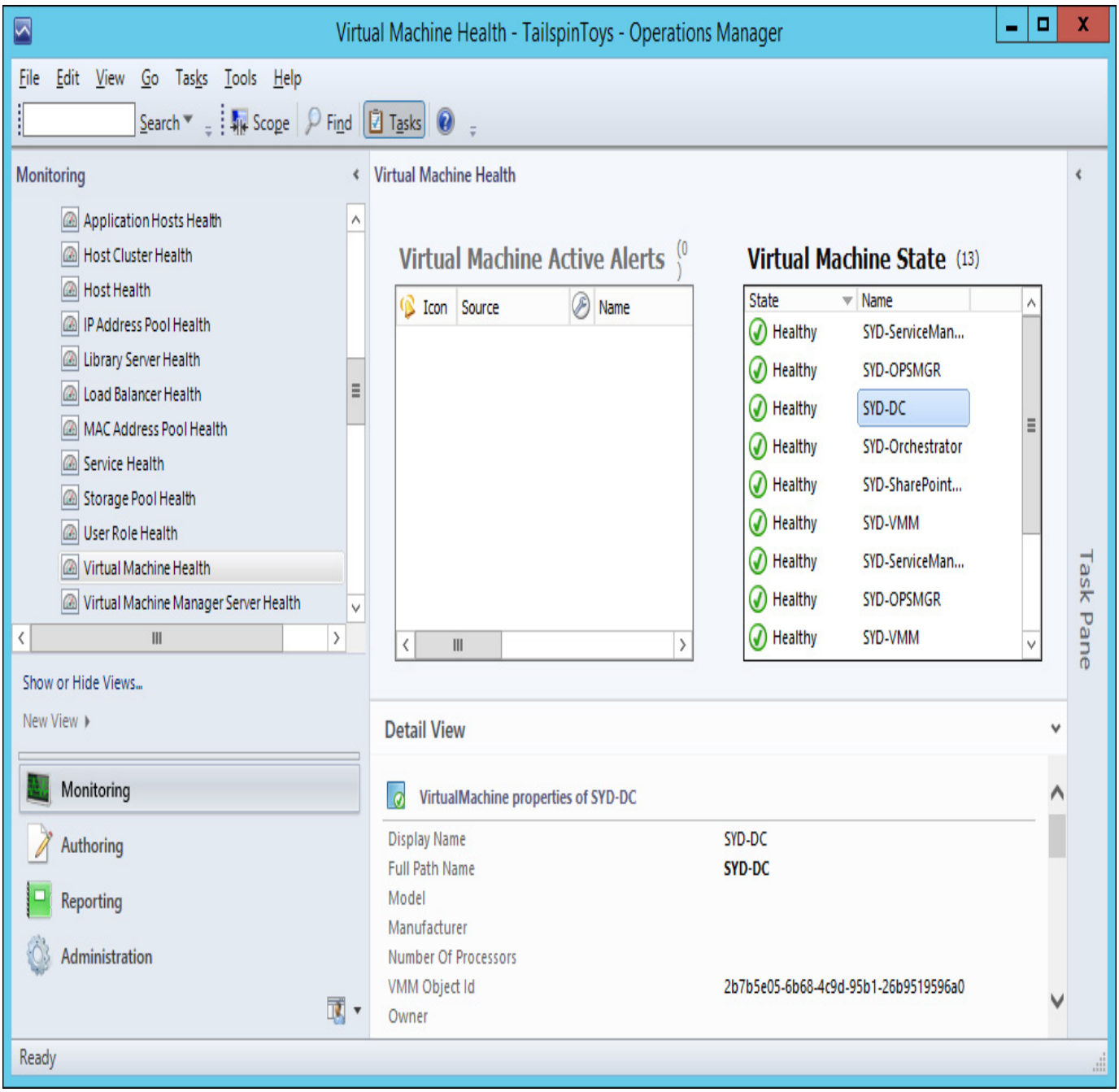

FIGURE 3-45 Virtual Machine Health

Integrating Operations Manager and Virtual Machine Manager also allows you to view the following performance information:

- Cloud Performance
- Host Cluster Performance
- Host Performance
- IP Address Pool Performance
- MAC Address Pool Performance
- Service Performance
- Storage Pool Performance
- Virtual Machine Performance

Figure 3-46 shows the Virtual Machine Performance view.

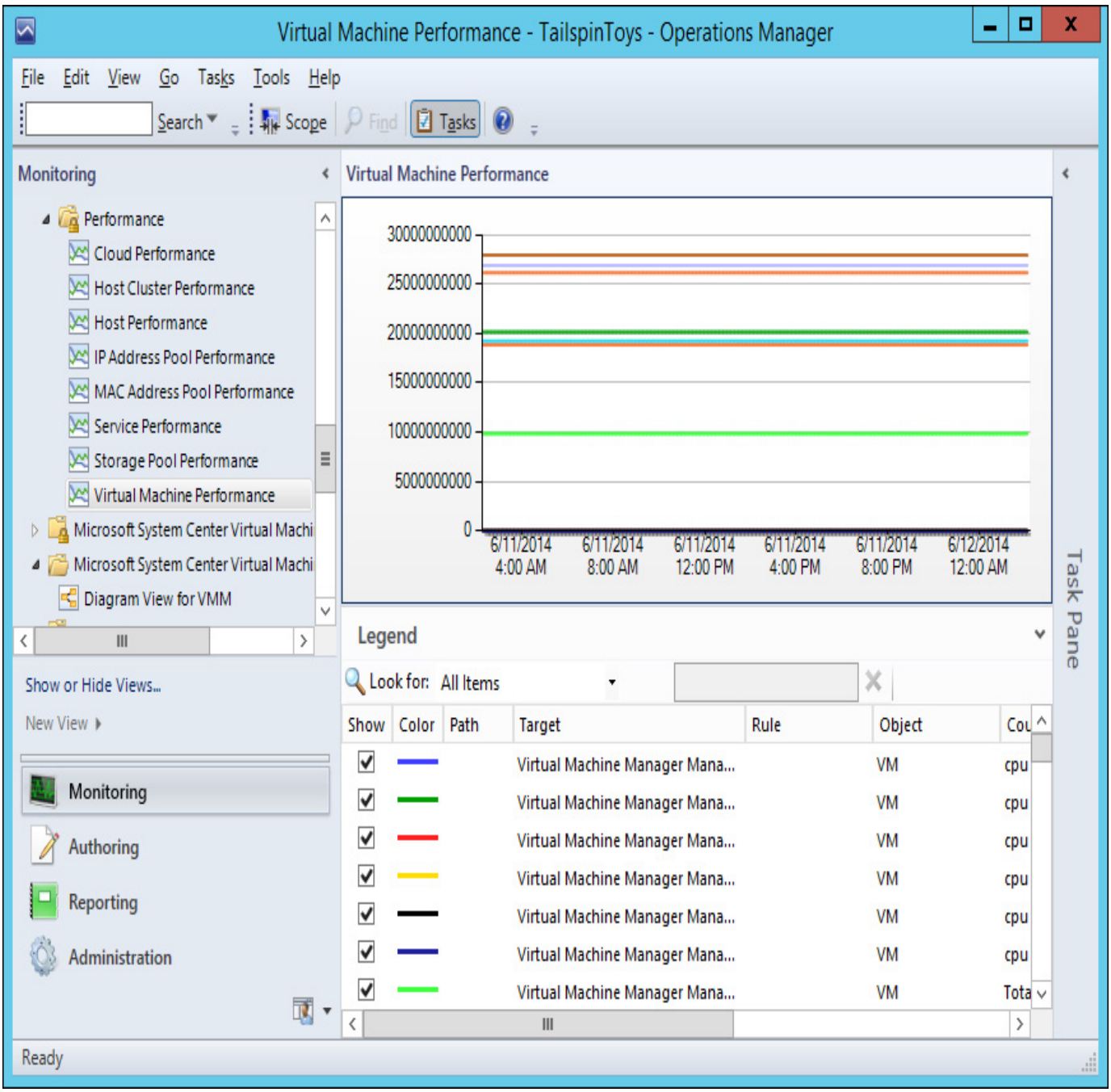

FIGURE 3-46 Virtual Machine Performance

To integrate Operations Manager with Virtual Machine Manager, you need to configure the connector between VMM and Operations Manager. Prior to configuring the connection between VMM and Operations Manager, you need to ensure you perform the following prerequisite configuration tasks:

- Install the Operations Manager console on the VMM server.
- Install the following Operations Manager management packs on the Operations Manager server:
  - SQL Server Core Library version 6.0.5000.0 or later
  - Windows Server Internet Information Services Library version 6.0.5000.0 or later
  - Windows Server Internet Information Services 2003 version 6.0.5000.0 or later
  - Windows Server 2008 Internet Information Services 7 version 6.0.6539.0 or later

To link VMM and Operations Manager, you need the credentials of an account that is a member of the Operations Manager Administrators user role, and the credentials of an account that is a member of the VMM Administrator user role. These can be separate accounts or the same accounts. To configure a connection between VMM and Operations Manager, perform the following steps:

1. In the Settings workspace of the VMM console, click System Center Settings, and then click Operations Manager Server.

2. On the ribbon, click Properties.
3. On the Connection To.. page of the Add Operations Manager Wizard, type the name of the Operations Manager server and a Run As account that has the appropriate permissions, as shown in Figure 3-47.

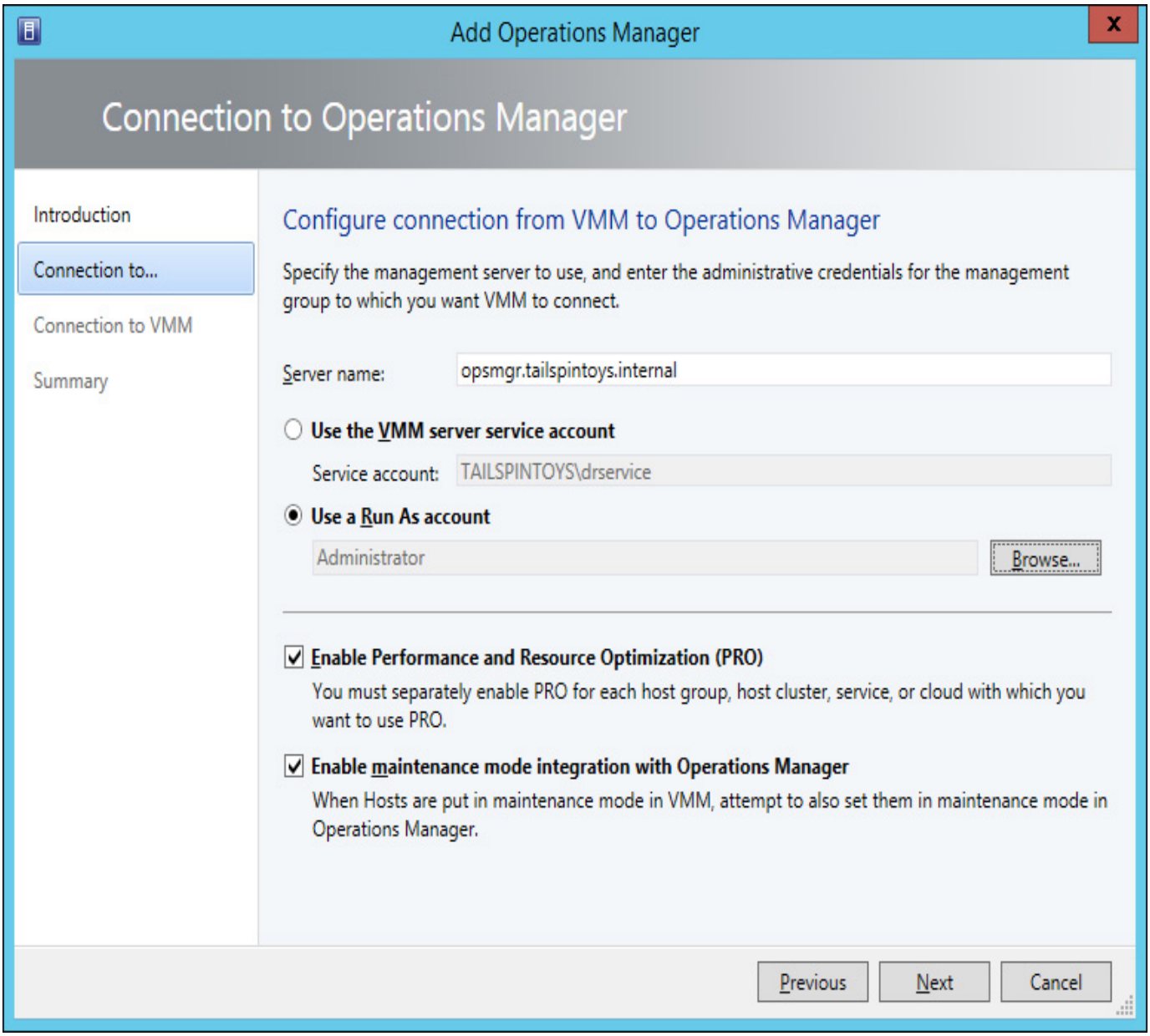

FIGURE 3-47 Connection to Operations Manager

4. On the Connection To VMM page, specify the credentials of the account that will be used by Operations Manger to connect to the VMM server.
5. Complete the wizard.

Configuring the connection between Operations Manager and VMM automatically loads the Management Packs, shown in Figure 3-48, which allow you to monitor the health and performance of your private cloud's virtualization layer.

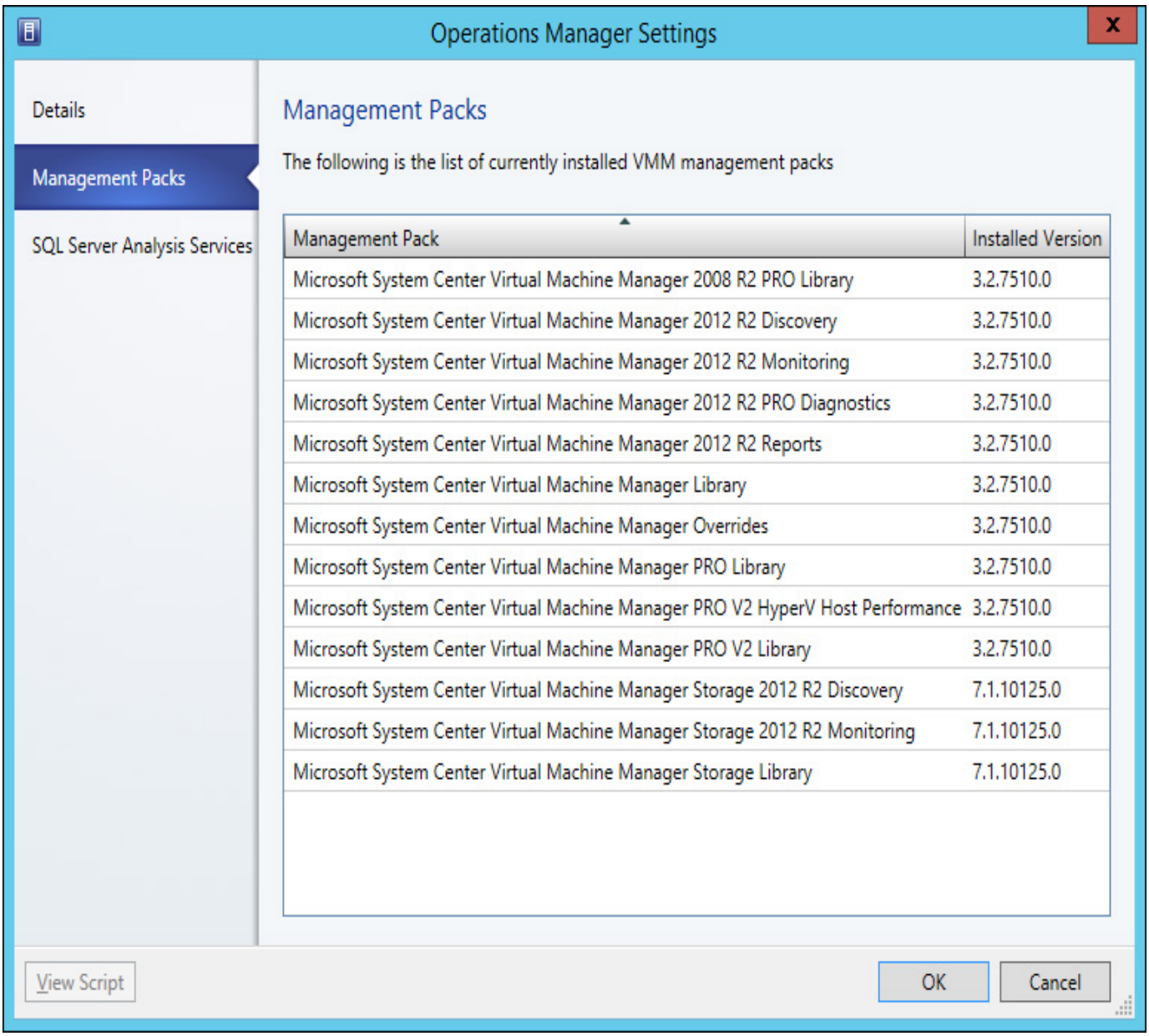

FIGURE 3-48 Management Packs

More Info: **Operations Manager Integration with VMM**

You can learn more about configuring Operations Manager integration with VMM at *http://technet.microsoft.com/library/hh427287.aspx*.

Using the Fabric Health Dashboard

You use the Fabric Health Dashboard to view detailed information about the health of VMM private clouds and the infrastructure, sometimes termed fabric, which supports them. Fabric Health Dashboard is available from the Cloud Health node and provides you with information about:

- Host State
- Storage Pools State
- File Share and LUN State
- Network Node State
- Instance Details
- Activity Alerts

Figure 3-49 shows the Fabric Health Dashboard scoped to the TailspinToys cloud.

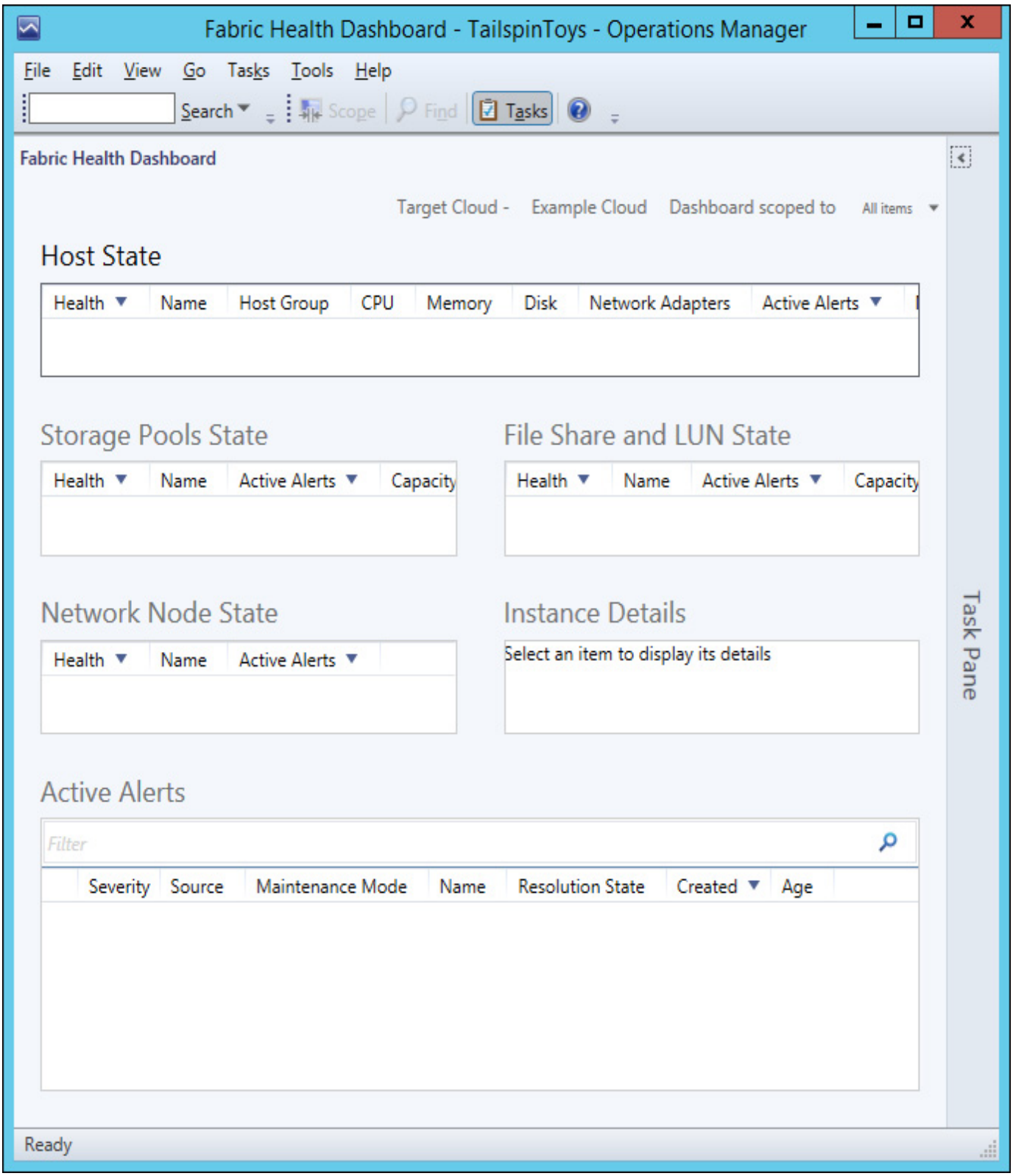

FIGURE 3-49 Fabric Health Dashboard

More Info: **Fabric Health Dashboard**

You can learn more about the Fabric Health Dashboard at *http://technet.microsoft.com/en-us/library/dn458591.aspx*.

Exam Tip

Remember what information you can view through the Fabric Health Dashboard.

Understanding the Fabric Monitoring Diagram view

The Fabric Monitoring Diagram view provides you with a diagram view of the entire infrastructure that VMM manages, and provides you with the health state of each segment that makes up the virtualization fabric. The view is located within the Monitoring workspace of the Operations Manger console when VMM is integrated with Operations Manager. Each node is presented as a roll-up that can be expanded. If a node is displayed as healthy, you can assume that all of the nodes it comprises are also believed by Operations Manager to be healthy. Figure 3-50 shows the Fabric Monitoring Diagram view.

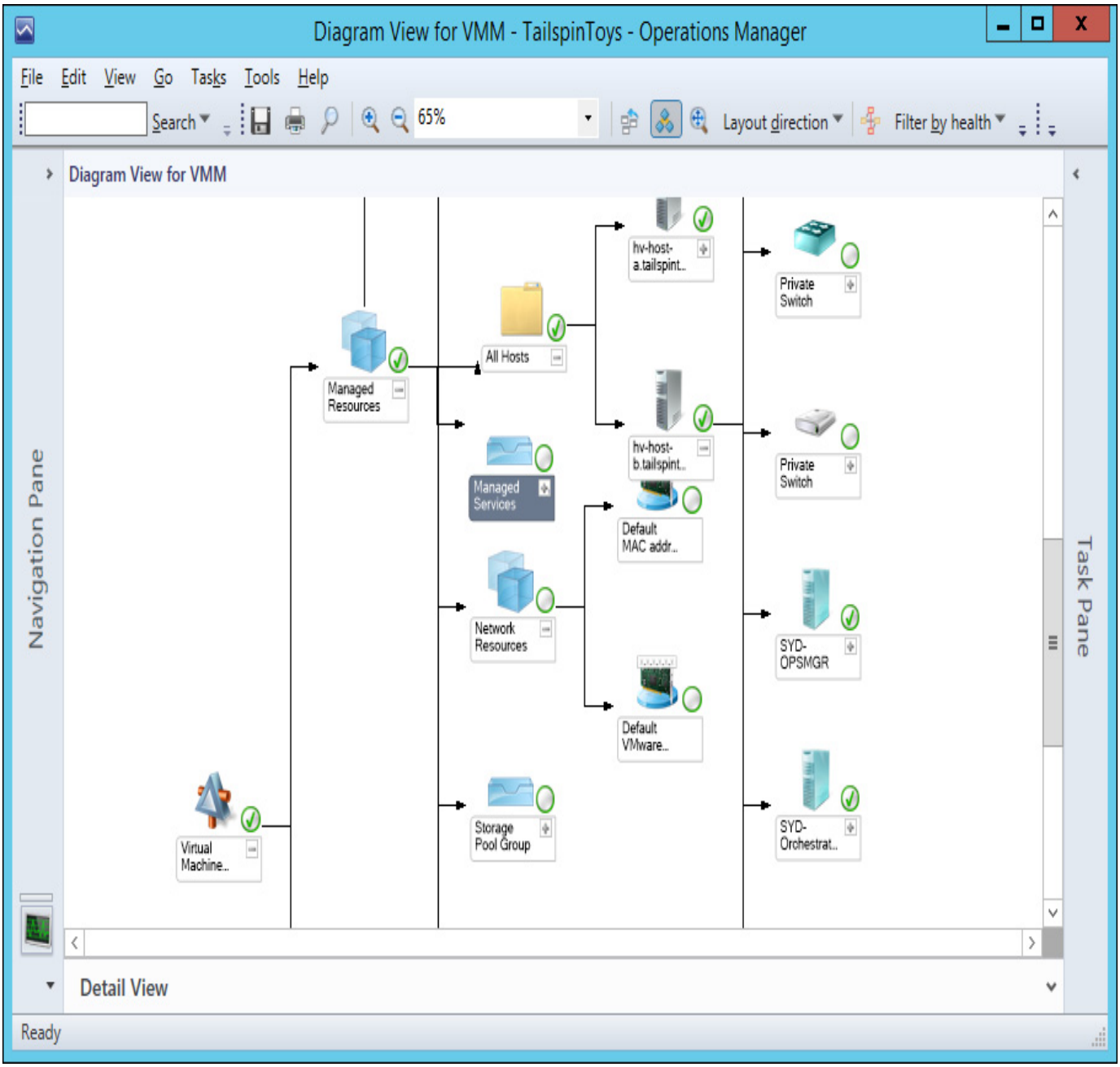

FIGURE 3-50 Diagram View

Where a node shows is displayed as unhealthy, you are able to expand it until you locate the monitored segment that is causing the unhealthy state.

More Info: **Fabric Diagram View**

You can learn more about Fabric Diagram view at *http://technet.microsoft.com/en-us/library/dn458593.aspx*.

***Thought experiment*: Virtualization layer monitoring at Wingtip Toys**

You are planning to integrate Operations Manager with VMM so that you can use Operations Manager to monitor your organization's virtualization segments. As part of this process, you are familiarizing yourself with the steps that you need to take to integrate these segments, and the functionality that integration will provide. With this information in mind, answer the following questions:

1. On which server must you install the additional console?
2. Which Operations Manager tool should you use to view the health state of all of the segments managed by VMM as part of a diagram?

Objective summary

- To integrate Operations Manager with Virtual Machine Manager, you need to install the Operations Manager console on the VMM server. You also need to ensure that the appropriate SQL Server and Internet Information Services management packs are installed.
- The Fabric Health Dashboard allows you to view detailed information about the health of VMM private clouds and infrastructure.
- The Fabric Monitoring Diagram view allows you to view the health state of the entire virtualization fabric managed by VMM.

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 Operations Manager dashboards would you use to determine the health state of virtual machines hosted on virtualization hosts managed by VMM?
   - **A.** User Role Health
   - **B.** Storage Pool Health
   - **C.** Virtual Machine Manager Server Health
   - **D.** Virtual Machine Health
2. You are setting up integration between Operations Manager and Virtual Machine Manager. Which of the following credentials do you need, to configure this integration?
   - **A.** An account that is a member of the Operations Manager Administrators user role.
   - **B.** An account that is a member of the VMM Administrator user role.
   - **C.** An account that is a member of the Domain Admins security group.
   - **D.** An account that is a member of the Local Administrators group on the Operations Manager server.
3. Which of the following is displayed in the Fabric Health Dashboard?
   - **A.** VMM Server Health
   - **B.** Storage Pools State
   - **C.** File Share and LUN State
   - **D.** Domain Controller State

Objective 3.4: Monitor application health

Once you have configured Operations Manager to collect data from applications, you need to configure how Operations Manager displays and interprets that data. This involves configuring appropriate notifications and alerts.

This section covers the following topics:

- Monitoring .NET applications
- Monitoring Java applications

Monitoring .NET applications

Operations Manager allows you to monitor .NET web applications either from the perspective of the server, or from the client. This allows you to collect information about application reliability and performance. Collecting this data allows you to generate reliable information about how frequently a particular application problem is occurring, the performance of the host server when the issue occurred, and any related events. Two of the most important tools that you use to monitor .NET applications are the Application Diagnostics console, and Application Advisor.

More Info: **Monitoring .NET Applications**

You can learn more about monitoring .NET applications at *http://technet.microsoft.com/en-us/library/hh212856.aspx*

Application Diagnostics console

The Application Diagnostics console allows you to monitor .NET applications for failures, faults, and slowdowns. To use the Application Diagnostics console, the Operations Manager web console must be installed on the Operations Manager management server. The Application Diagnostics console is available at the address *http://hostname/AppDiagnostics,* and is shown in Figure 3-51.

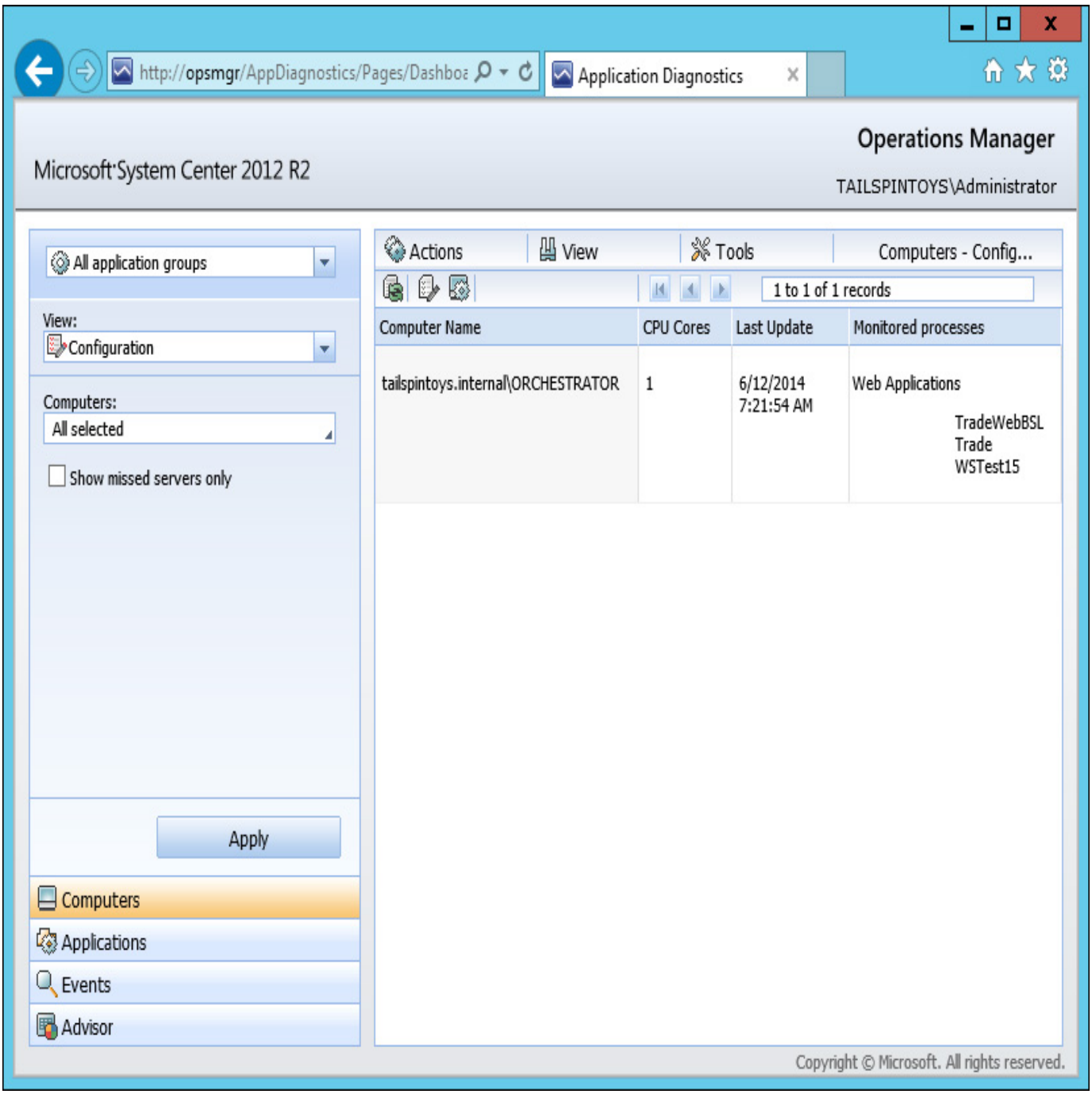

FIGURE 3-51 Application Diagnostics console

The Application Diagnostics console allows you to view events related to application performance and events related to application failures and errors. Application failures and errors can be displayed based on connectivity, security, and failure issues.

More Info: **Application Diagnostic Console**

You can learn more about the Application Diagnostics console at *http://technet.microsoft.com/en-us/library/hh530058.aspx*.

Application Advisor

Application Advisor is a tool that you use with .NET APM to manage and prioritize application related alerts. Application Advisor allows you to run reports that allow you to determine which applications are triggering the most alerts. Application Advisor is a web application that you can use if you have installed the Operations Manager web console. The address of the Application Advisor is *http://hostname/AppAdvisor*. The Application Advisor console is shown in Figure 3-52.

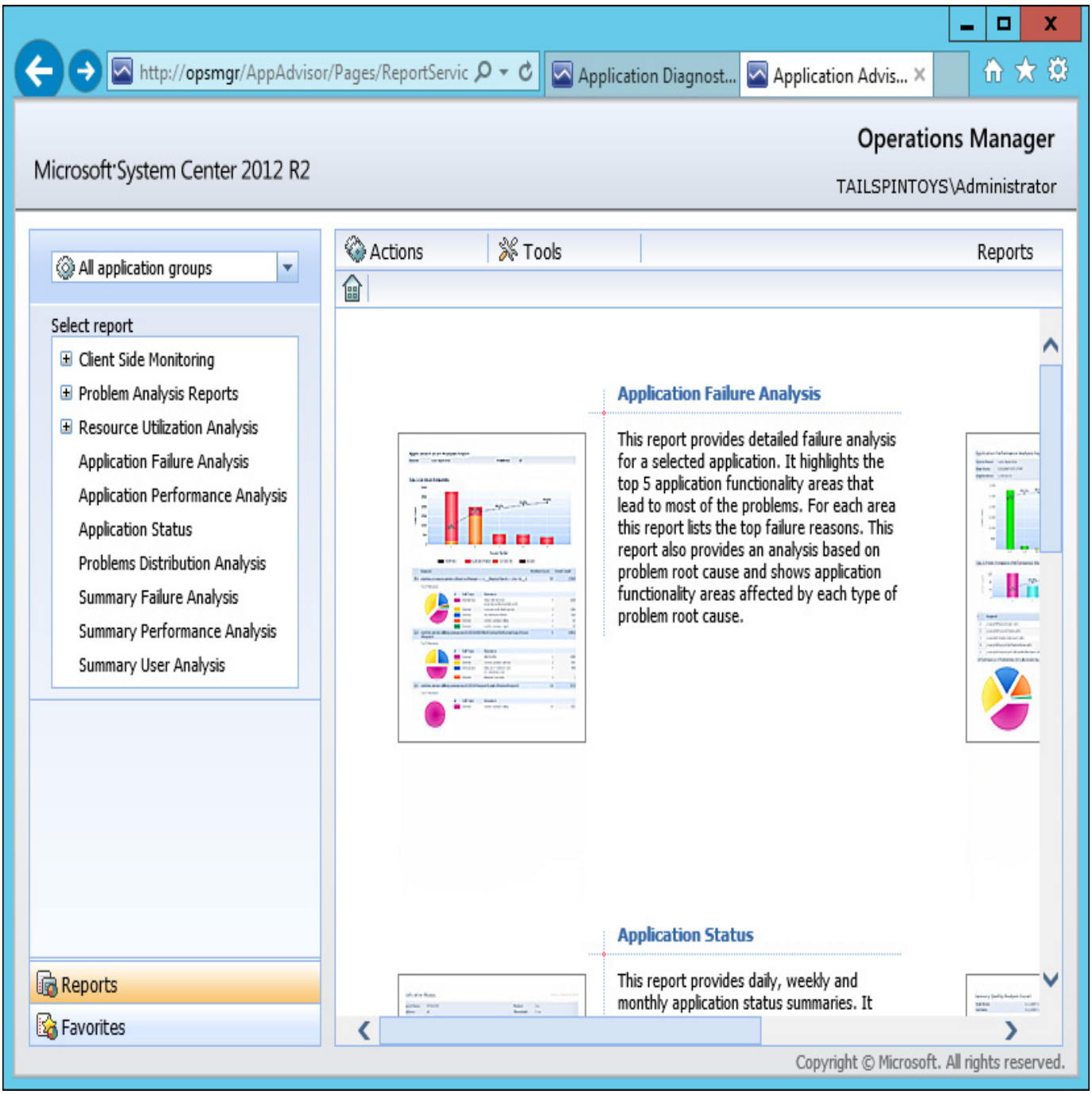

FIGURE 3-52 Application Advisor

Application Advisor provides client side monitoring, problem analysis, and resource utilization analysis reports. The client side monitoring reports are as follows:

- Application AJAX Calls Analysis
- Application Analysis
- Application Status
- Client Latency Distribution
- Load Time Analysis Based On Subnet
- Summary Performance Analysis
- Summary Size Analysis
- Summary User Analysis

The problem analysis reports provided by Application Advisor are as follows:

- Application Activity Breakdown
- Application Daily Activity
- Application Failure Breakdown By Functionality

- Application Failure Breakdown By Resources
- Application Heavy Resources Analysis
- Application Slow Request Analysis
- Day Of Week Utilization
- Hour Of Day Utilization
- Utilization Trend

The resource utilization analysis reports provided by Application Advisor are as follows:

- Application CPU Utilization Analysis
- Application IO Utilization Analysis
- Application Memory Utilization Analysis
- Computer Application Load Analysis
- Computer CPU Utilization Analysis
- Computer IO Utilization Analysis
- Computer Memory Utilization Analysis

Application Advisor also provides the following general reports:

- Application Failure Analysis
- Application Performance Analysis
- Application Status
- Problems Distribution Analysis
- Summary Failure Analysis
- Summary Performance Analysis
- Summary User Analysis

More Info: **Application Advisor**

You can learn more about the Application Advisor at *http://technet.microsoft.com/en-us/library/hh322034.aspx*

Monitoring Java applications

Operations Manager 2012 R2 supports Java Application Performance Monitoring (APM). Java APM allows you to monitor Java applications, providing you with information about the application's performance and details of exception events that allow you, or the application owners, to determine the root cause of application issues. You do this by using Operations Manager Application Advisor.

Operations Manager Application Advisor allows you to perform the following tasks:

- Investigate method and resource timing for performance events
- Perform stack traces for exception events
- Monitor Java specific counters for events (including Average Request Time, Requests Per Second, JVM Memory, and Class Loader)

Java APM supports the following configurations:

- Tomcat 5, Tomcat 6, Tomcat 7
  - Windows
  - Linux
- Java JDK 5, Java JDK 6
- Web Technologies
  - GenericServlet
  - Struts

- Struts2
- Axis2

Exam Tip

Remember which configurations are supported for .NET and Java APM.

The Java APM management pack requires the management pack for Java Enterprise Edition, which you must configure for deep monitoring. You use Application Advisor reports, for example the Application Performance Analysis report, to view the performance of Java applications in the same way that you monitor .NET applications.

More Info: **Monitoring Java Applications**

You can learn more about monitoring Java applications at *http://technet.microsoft.com/en-us/library/dn440936.aspx*.

***Thought experiment*: Application Performance Monitoring at Contoso**

You are in the process of writing documentation to support the monitoring of .NET application performance at Contoso using System Center 2012 R2 operations monitor. As part of the process, you need to answer the following questions:

1. Which tool would you use to view events related to application performance and events related to application failures and errors?
2. Which tool do you use to manage and prioritize application related alerts?

Objective summary

- The Application Diagnostics console allows you to monitor .NET applications for failures, faults, and slowdowns.
- To use the Application Diagnostics console, the Operations Manager web console must be installed on the Operations Manager management server.
- Application Advisor is a tool that you use with .NET APM to manage and prioritize application related alerts.
- Application Advisor is a web application that you can use if you have installed the Operations Manager web console.

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 must be installed before you can access the Application Advisor functionality of Operations Manager?
   - **A.** Operations Manager web console
   - **B.** Orchestrator connector for Service Manager
   - **C.** SQL Server Analysis Services
   - **D.** Operations Manager connector for Service Manager
2. Which of the following tools would you use to view an application performance monitoring

report that provided client application load time analysis on a per-subnet basis?

A. Application Advisor

B. Application Diagnostics Console

C. Operations Manager Web Console

D. Operations Manager Console

3. Which of the following tools can you use with Operations Manager application performance monitoring to view events related to application errors?

A. Application Advisor

B. Application Diagnostics Console

C. Operations Manager Web Console

D. Operations Manager Console

Answers

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

Objective 3.1: Thought experiment

1. You would use the Network Summary dashboard to view the list of network device interfaces in the organization that had the most send errors.
2. You would use the Network Node Dashboard View to view the availability statistics of a particular network device over the last seven days.
3. You would use the Network Interface Dashboard view, to view the number of bytes sent on a specific router interface.

Objective 3.1: Review

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

   A. **Correct**: Alerts will be generated when the health state changes from healthy to critical.

   B. **Incorrect:** Alerts are not generated when the health state changes from critical to healthy.

   C. **Incorrect:** Alerts are not generated when the health state changes from warning to healthy.

   D. **Correct:** Alerts are generated when the health state changes from healthy to warning.

2. **Correct answer:** D

   A. **Incorrect:** You need to configure an override for the Auto-Resolve Alert parameter to ensure that the alert was automatically resolved.

   B. **Incorrect**: You need to configure an override for the Auto-Resolve Alert parameter to ensure that the alert was automatically resolved.

   C. **Incorrect**: You need to configure an override for the Auto-Resolve Alert parameter to ensure that the alert was automatically resolved.

   D. **Correct**: You need to configure an override for the Auto-Resolve Alert parameter to ensure that the alert was automatically resolved.

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

   A. **Incorrect**: A monitor only sends an alert when a state change occurs, from either healthy to warning, healthy to critical, or warning to critical.

   B. **Correct**: A rule will continue to generate alerts as long as the condition that triggers the alert persists.

   C. **Correct**: A monitor only sends an alert when a state change occurs, from either healthy to warning, healthy to critical, or warning to critical.

   D. **Incorrect**: A rule will continue to generate alerts as long as the condition that triggers the alert persists.

4. **Correct answer:** D
   A. **Incorrect**: The Network Summary Dashboard will show information about all monitored network devices.
   B. **Incorrect**: The Network Node Dashboard view will display information, including performance information, about a specific monitored device.
   C. **Incorrect**: The Network Interface Dashboard view will show information about a specific network device interface.
   D. **Correct**: The Network Vicinity Dashboard view will show monitored devices and computers that are connected to a monitored network device.
5. **Correct answer:** B
   A. **Incorrect**: The Network Vicinity Dashboard view will show monitored devices and computers that are connected to a monitored network device.
   B. **Correct:** The Network Interface Dashboard view will show information about a specific network device interface.
   C. **Incorrect:** The Network Node Dashboard view will display information, including performance information about a specific monitored device.
   D. **Incorrect**: The Network Summary Dashboard will show information about all monitored network devices.

Objective 3.2: Thought experiment

1. You need to install the Windows Server 2012 R2 management packs to change the status from not monitored.
2. You should check the status of the Microsoft monitoring agent service as a failure of this service can cause a server to be shown with a gray agent status.

Objective 3.2: Review

1. **Correct answer:** B
   A. **Incorrect:** A Health Service Heartbeat Failure alert that doesn't have a corresponding Failed To Connect To Computer alert indicates that the computer can be pinged by the Operations Manager management server, but that heartbeat traffic is not occurring. A likely cause is that there is a problem with the Operations Manager agent.
   B. **Correct**: A Health Service Heartbeat Failure alert that doesn't have a corresponding Failed To Connect To Computer alert indicates that the computer can be pinged by the Operations Manager management server, but that heartbeat traffic is not occurring. A likely cause is that there is a problem with the Operations Manager agent.
   C. **Incorrect**: A Health Service Heartbeat Failure alert that doesn't have a corresponding Failed To Connect To Computer alert indicates that the computer can be pinged by the Operations Manager management server, but that heartbeat traffic is not occurring. A likely cause is that there is a problem with the Operations Manager agent.
   D. **Incorrect**: A Health Service Heartbeat Failure alert that doesn't have a corresponding Failed To Connect To Computer alert indicates that the computer can be pinged by the Operations Manager management server, but that heartbeat traffic is not occurring.
2. **Correct answers:** A and D
   A. **Correct:** ACS forwarders send security event log data to the ACS collector.
   B. **Incorrect**: The domain controllers should be configured as ACS forwarders.
   C. **Incorrect**: As ACS1 is not generating the initial security log events, it should not function as an ACS forwarder.
   D. **Correct**: ACS1 should function as the ACS collector.
3. **Correct answers:** B and C

A. **Incorrect**: No services on the monitored service will be disabled when the server is placed into monitoring mode on the Operations Manager server.

B. **Correct:** Rules and monitors related to the monitored server will be suspended while the server is in maintenance mode.

C. **Correct**: New alerts from the monitored server will be suspended while the server is in maintenance mode.

D. **Incorrect**: No services on the monitored service will be disabled when the server is placed into monitoring mode on the Operations Manager server.

Objective 3.3: Thought experiment

1. You must in stall the Operations Manager console on the VMM server.
2. The Fabric Monitoring Diagram view allows you to view the health state of all of the segments managed by VMM as part of a diagram.

Objective 3.3: Review

1. **Correct answer:** D

   A. **Incorrect**: User Role Health will display the health of user roles.

   B. **Incorrect**: Storage Pool Health will display the health of storage managed by VMM.

   C. **Incorrect**: Virtual Machine Manager Server Health will show the health status of VMM servers.

   D. **Correct**: Virtual Machine Health allows you to view the health status of virtual machines hosted on virtualization hosts managed by VMM.

2. **Correct answer:** A and B

   A. **Correct**: You need access to an account that is a member of the Operations Manager Administrator user role and an account that is a member of the VMM Administrator role.

   B. **Correct**: You need access to an account that is a member of the Operations Manager Administrator user role and an account that is a member of the VMM Administrator role.

   C. **Incorrect:** You need access to an account that is a member of the Operations Manager Administrator user role and an account that is a member of the VMM Administrator role.

   D. **Incorrect**: You need access to an account that is a member of the Operations Manager Administrator user role and an account that is a member of the VMM Administrator role.

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

   A. **Incorrect**: The Fabric Health Dashboard does not display VMM Server Health.

   B. **Correct**: The Fabric Health Dashboard does display Storage Pools State.

   C. **Correct**: The Fabric Health Dashboard does display File Share and LUN State.

   D. **Incorrect:** The Fabric Health Dashboard does not display Domain Controller Health.

Objective 3.4: Thought experiment

1. The Application Diagnostics console allows you to view events related to application performance and events related to application failures and errors.
2. Application Advisor is a tool that you can use to manage and prioritize application related alerts.

Objective 3.4: Review

1. **Correct answer:** A

   A. **Correct:** The Operations Manager web console must be installed before you can access the Application Advisor functionality of Operations Manager.

   B. **Incorrect:** You do not have to have the Orchestrator connector for Service Manager, or Service Manager, installed to access the Application Advisor.

   C. **Incorrect:** You do not have to have SQL Server Analysis Services installed to access the

Application Advisor.

D. **Incorrect:** You do not have to have the Operations Manager connector for Service Manager, or Service Manager, installed to access the Application Advisor.

2. **Correct answer:** A

A. **Correct:** You can use the application diagnostics console to view a load time analysis based on subnet report.

B. **Incorrect:** You cannot use the application diagnostics console to view a load time analysis based on subnet report.

C. **Incorrect:** You cannot use the Operations Manager Web console to view a load time analysis based on subnet report.

D. **Incorrect:** You cannot use the Operations Manager console to view a load time analysis based on subnet report.

3. **Correct answer:** B

A. **Incorrect:** You can use the application diagnostics console to view events related to application errors.

B. **Correct:** You can use the application diagnostics console to view events related to application errors.

C. **Incorrect:** You can use the application diagnostics console to view events related to application errors.

D. **Incorrect:** You can use the application diagnostics console to view events related to application errors.

Prev
Chapter 2. Deploy resource monitoring
Next
Chapter 4. Configure and maintain service management