System Center 2012 R2 Lab 5: Application Management

Hands-On Lab | Step-by-Step Guide

For the VMs use the following credentials:

- Username: **Contoso\Administrator**
- Password: **Passw0rd!**

Version: 1.5.5

Last updated: March 28, 2014

Please share any feedback with the IT Camps Planning Team:
ITCampPlan@Microsoft.com

5 - Application Management

1. **100 minutes optional (1:40 total)**

2. SCAC, SCOM & SCA: Application Management Components (25 mins)

3. SCAC: Manage Applications through Self-Service (10 mins)

4. SCOM: Monitor Applications (15 mins)

5. SCOM: Review Application Performance Monitoring (40 mins)

6. SCA: Monitor Applications with Advisor (10 mins)

5.1 - SCAC, SCOM & SCA: Application Management Components

5.1.1 - SCAC: Introduction to App Controller

In this exercise the user will learn about the different workspaces and functions of System Center 2012 R2 App Controller, including Clouds, Services, Virtual Machines, Library , Jobs and Settings. Internet Explorer will be used to connect to App Controller which provides a common self-service experience that can help easily configure, deploy, and manage virtual machines and services across private clouds (through SCVMM) and public clouds (through Azure).

Estimated time to complete: 5 minutes
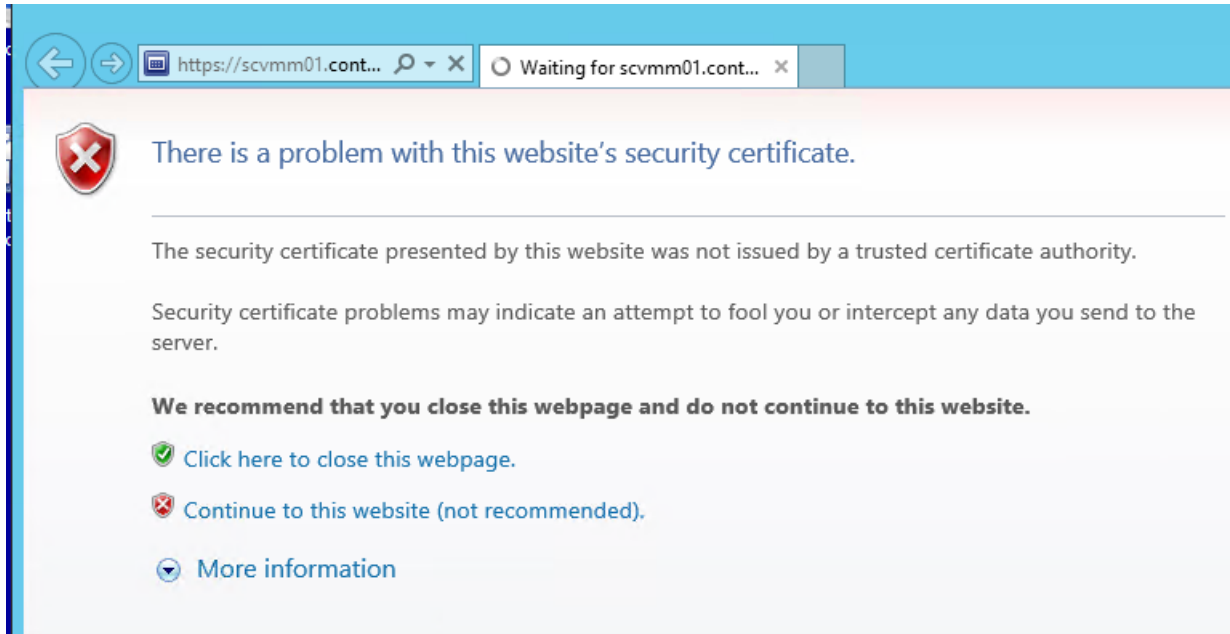
Perform the following on **SCVMM01**

1. From **SCVMM01**, open **App Controller** by selecting the **Internet Explorer** icon from the taskbar.

2. If the site does not open, browse to **https://SCVMM01.contoso.com**.

3. If a notification appears about the certificate, click **Continue to this website (not recommended)**.

4. When prompted to sign in, enter **contoso\administrator** for the user name and **Passw0rd!** for the password. Click the **Sign In** button.


5. Navigate to the **Overview** workspace. This shows the overall status view of the clouds in the infrastructure. This is the location to add new clouds to monitor, these include clouds from VMM, Azure and other hosting providers.
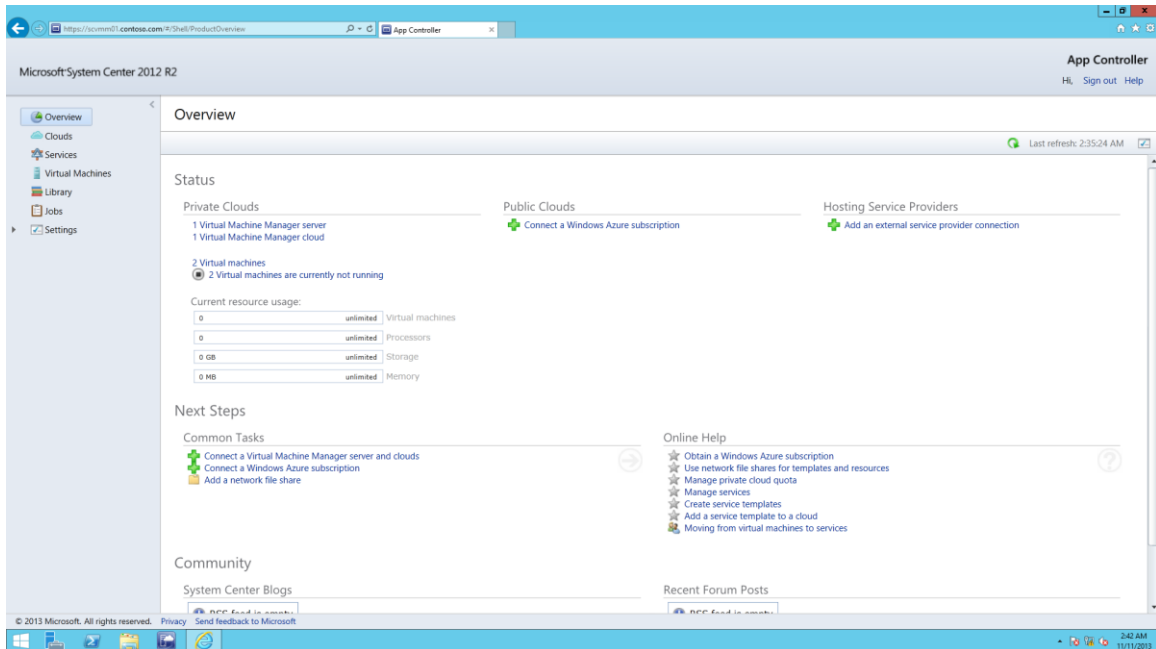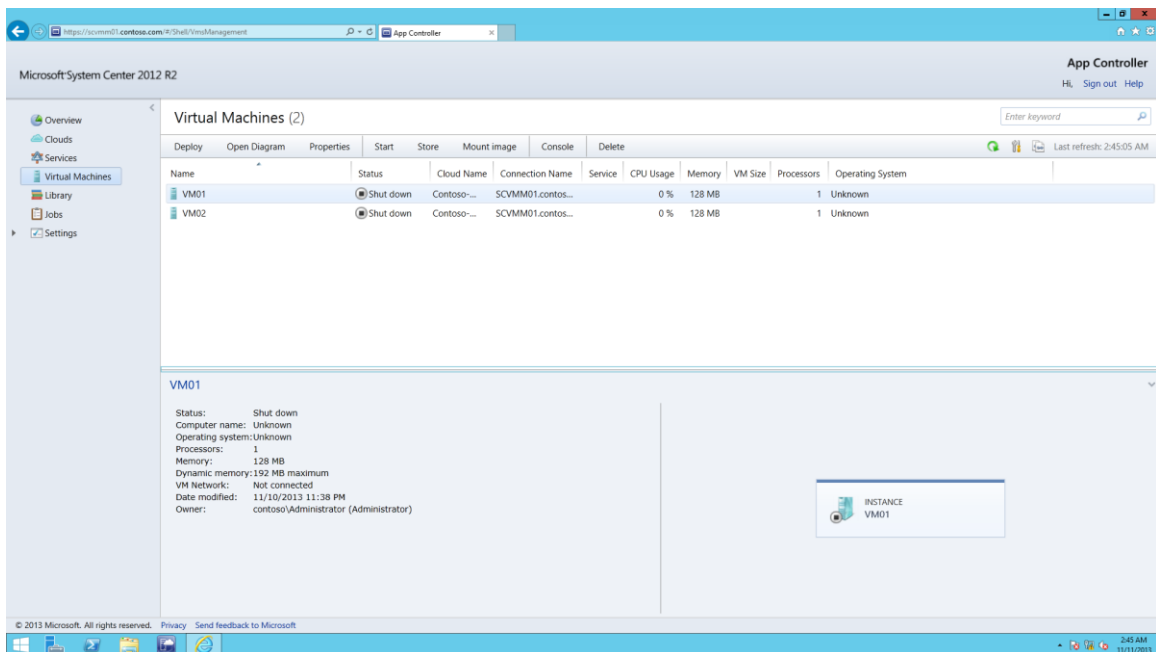
6. Navigate to the **Clouds** workspace. This page is used to connect to and manage public and private clouds, and to deploy services to them. Users who manage public and private clouds must be members of the **Administrator** user role.
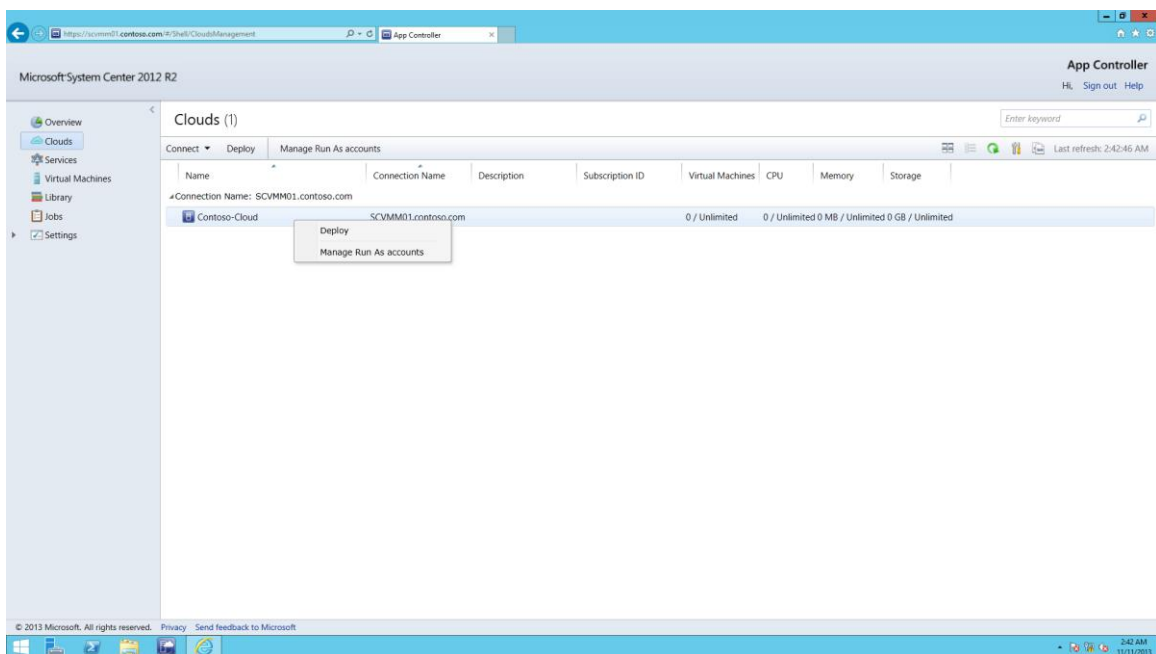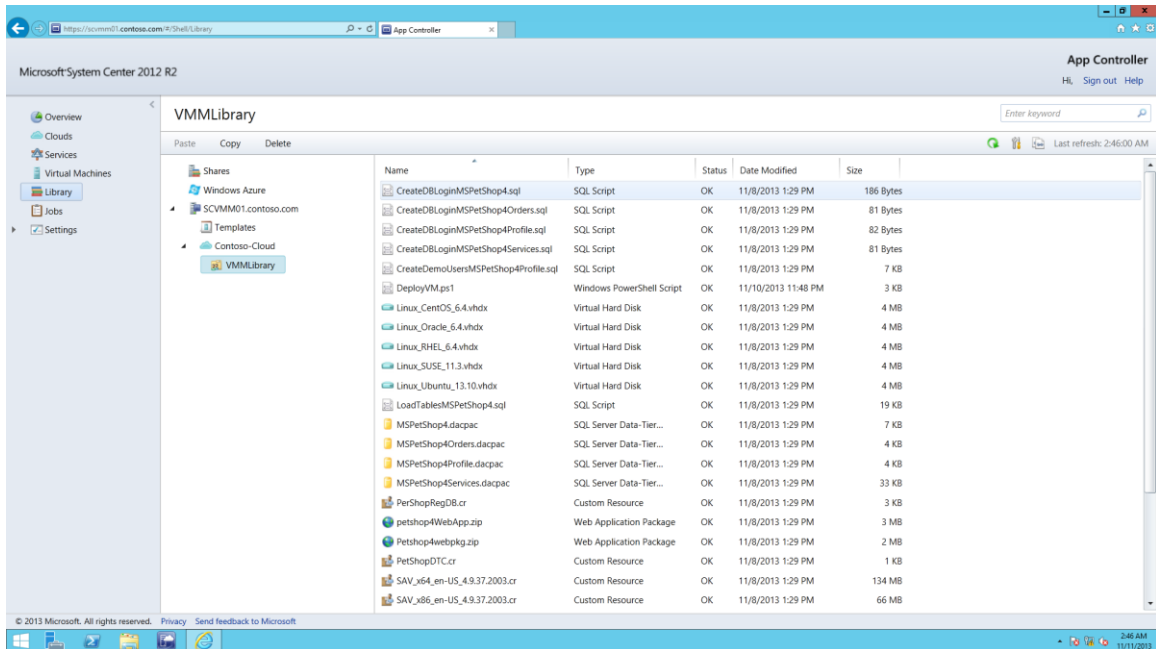

7. Navigate to the **Services** workspace. This workspace is used deploy new services to public and private clouds, or to change the properties of services already deployed.
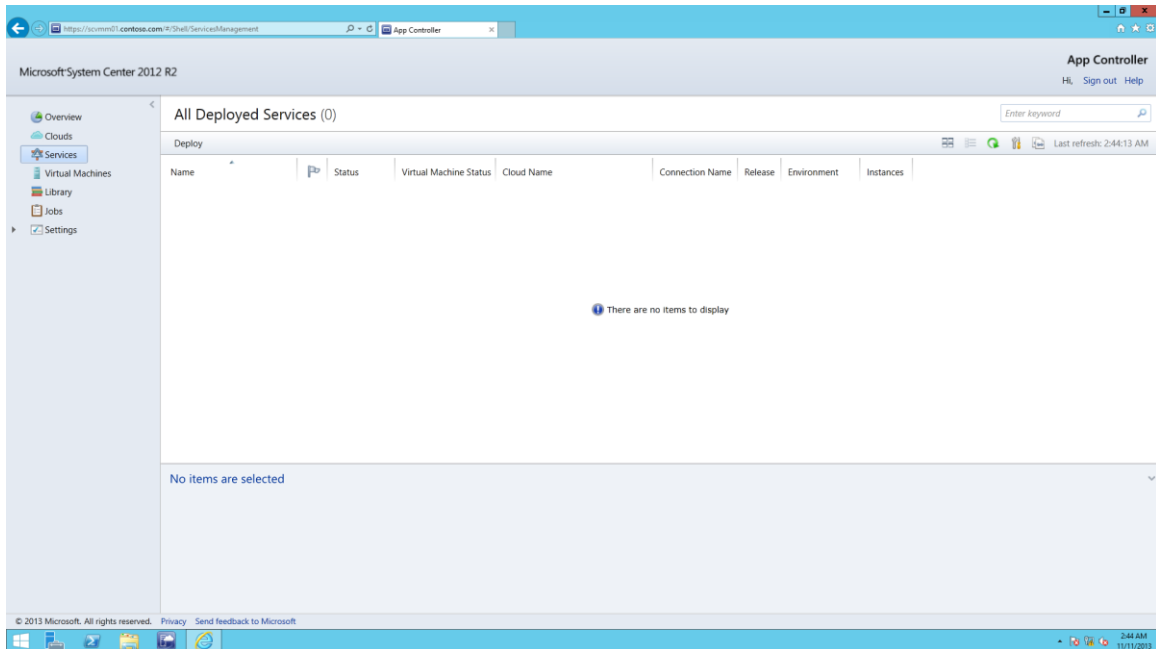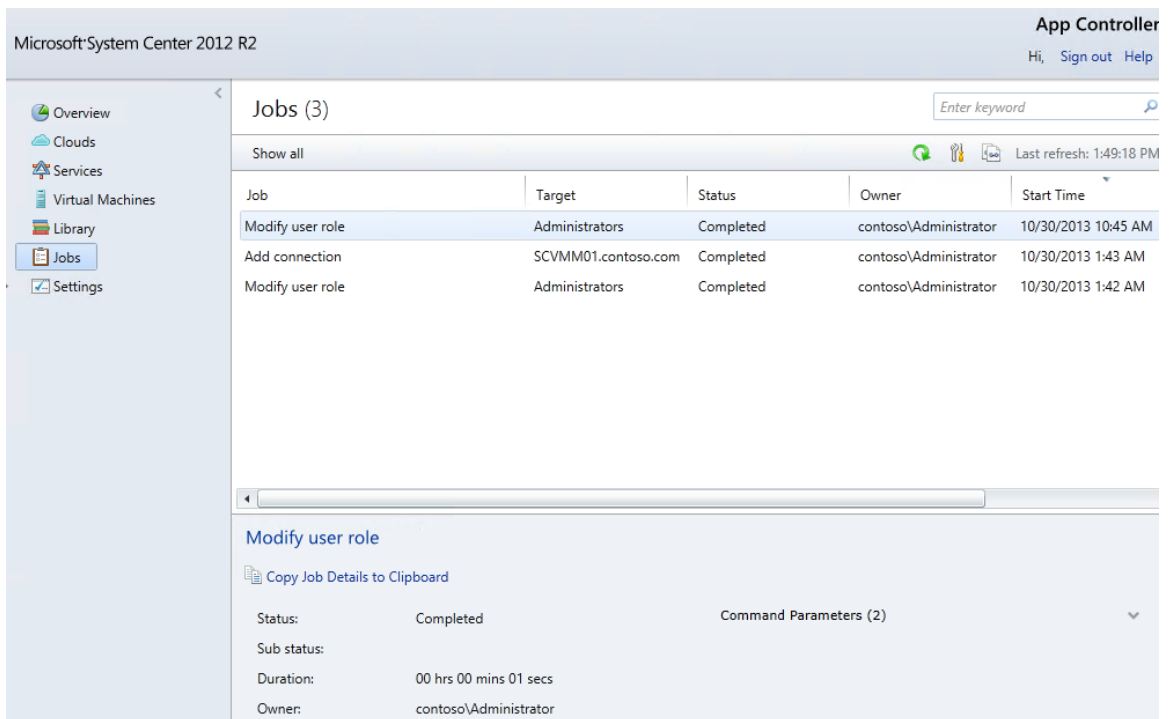
8. Navigate to the **Virtual Machines** workspace. This is the location to deploy virtual machines to clouds, Azure or other hosting providers.

9. Navigate to the **Library** workspace. This page is used to manage file shares, templates, and resources for both System Center 2012 – Virtual Machine Manager (VMM) and Windows Azure.

10. Navigate to the **Jobs** workspace. The Jobs page is used to view the status of all the jobs that have run in App Controller. For example, these jobs include changing user roles, adding or removing cloud connections and deploying services.

11. Navigate to the **Settings** workspace and click **Connections**. This manages the connection settings to different clouds. This provides the options to connect to a server running System Center

Virtual Machine Manager, Windows Azure, or a service provider. This is also the location to
import certificates or set specify proxy settings.
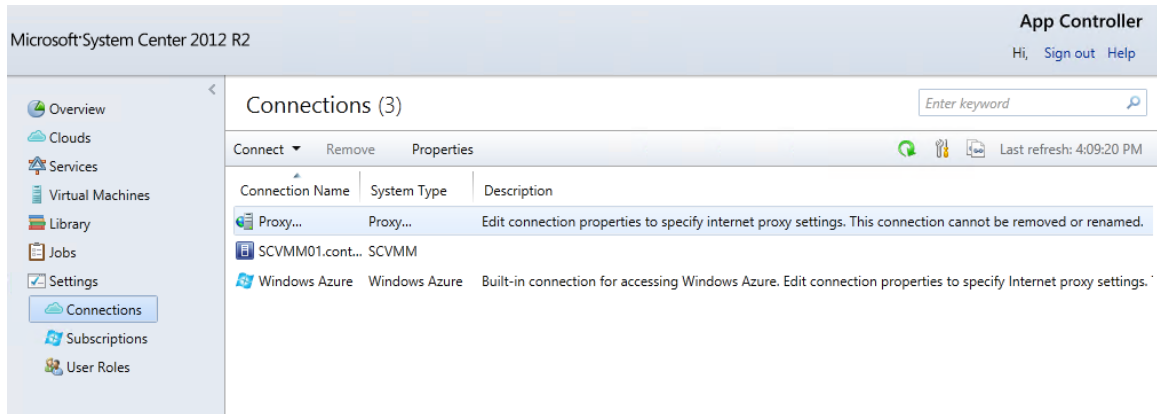
5.1.2 - SCOM: Introduction to Operations Manager

**In this exercise the user will learn about the different workspaces and functions of System Center
2012 R2 Operations Manager, including Monitoring, Authoring, Reporting, and Administration.**

Estimated time to complete: 15 minutes

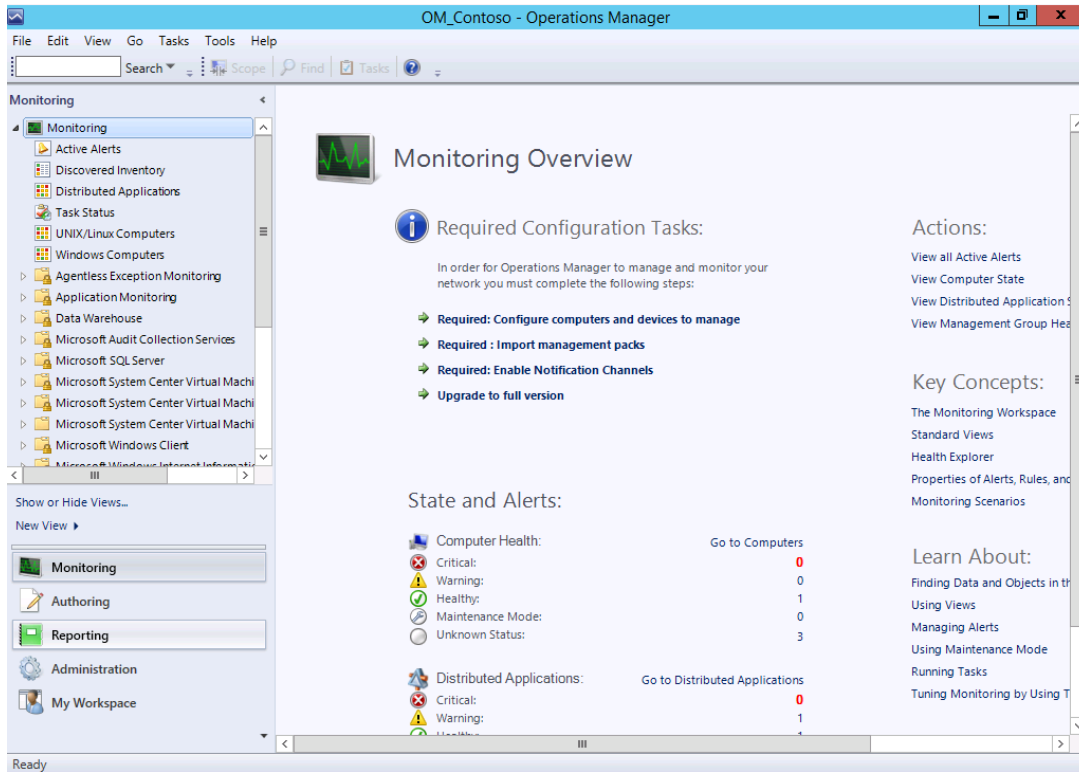*Perform the following on SCOM01*

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.


2. Navigate to the **Monitoring** workspace.

3. This workspace is used to see what is going in the monitoring environment and is the primary workspace for operators. It contains views, diagrams, and dashboard views that compile and present useful information that Operations Manager has gathered.

4. Click the **Active Alerts** view. This view shows all alerts that are active (not closed).

5. In this view, select an alert to view its details, such as the rule or monitor that generated the alert and the managed object that has the problem.

6. Double-click an alert to open its properties.

7. Select an alert and click Health Explorer in the Tasks pane to open Health Explorer in the context of this alert.

8. When appropriate, the user can close the alert from this view by clicking Close Alert in the Tasks pane.

9. Click **Discovered Inventory**. This view shows all objects that have been discovered and their states.

10. Click **Change Target Type** in the Tasks pane to filter the discovered inventory list to a single type of object. The target type determines the type of information that will be displayed in the details pane for a selected object.

11. Click **Cancel**.
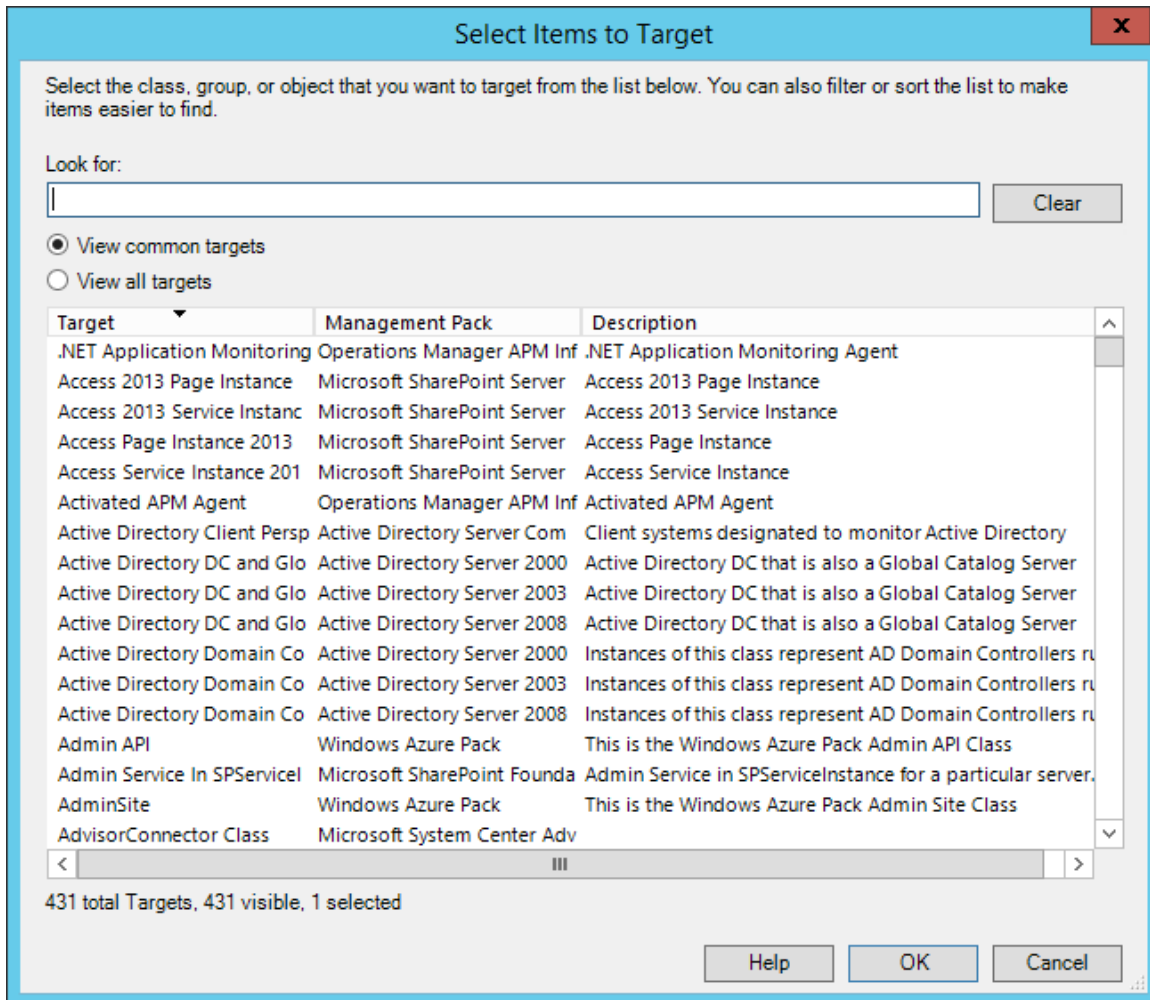
12. Click **Task Status**. This view shows the output from tasks that have been executed in the console. The Task Status view shows when a task is completed, finished, and the user who executed this specific task.

13. Click **Windows Computers**. This view shows the state of the following aspects of discovered Windows computers: Overall state of the computer, State of the agent on the computer, if an agent is installed, State of the management server role, if the computer is a management server, State of the Windows operating system.

14. To see information that is collected for a computer, select the computer Name field for a specific computer.

15. The properties in the tasks pane can be clicked to display all of the information that is collected.

16. To open other views for a computer, right-click the computer, select Open, and click a view to open.

17. Expand **Microsoft SQL Server** and click **Active Alerts** to view the alerts specific to SQL Server.
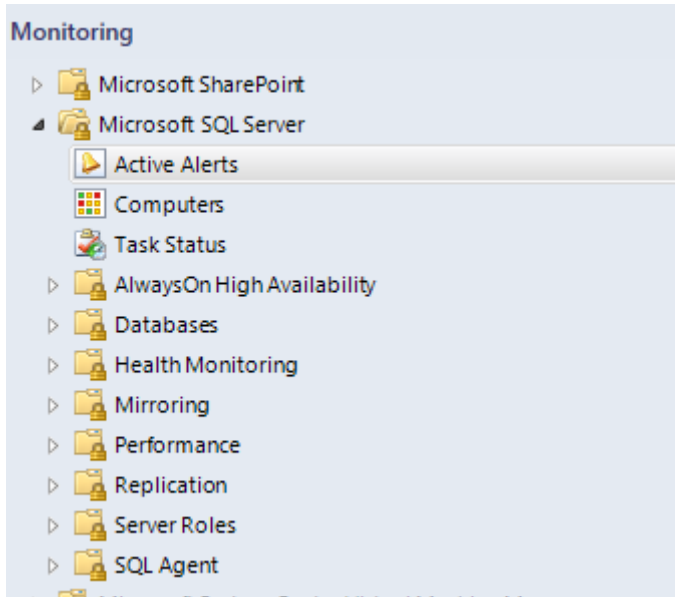
18. Click the **Authoring** workspace.
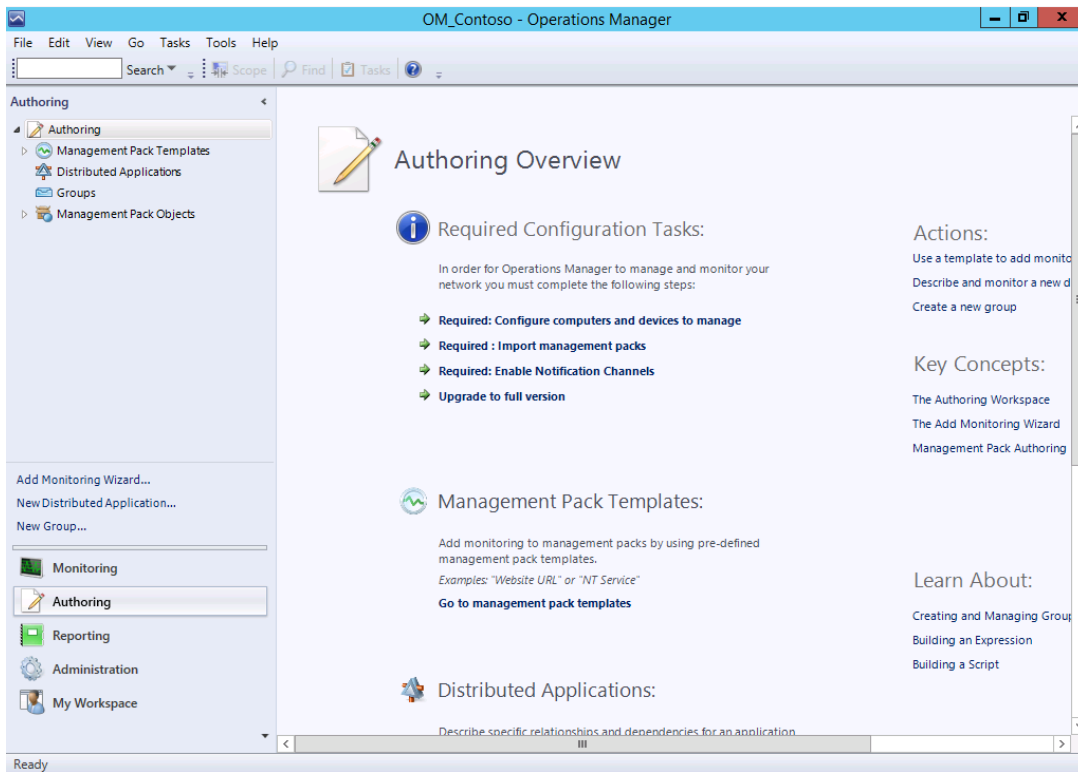
19. This workspace is used to create new monitoring scenarios. Existing management packs can be added or changed or new management packs can be created for applications that do not have one.

20. Click **Management Pack Templates**. Management packs contain settings that enable agents to monitor a specific service or application in System Center 2012 – Operations Manager. These settings include discovery information that allows management servers to automatically detect and begin monitoring objects, a knowledge base that contains error and troubleshooting information, rules and monitors that generate alerts, and reports. Management packs might also contain tasks, diagnostics, and recovery tools and guidance to help fix problems.
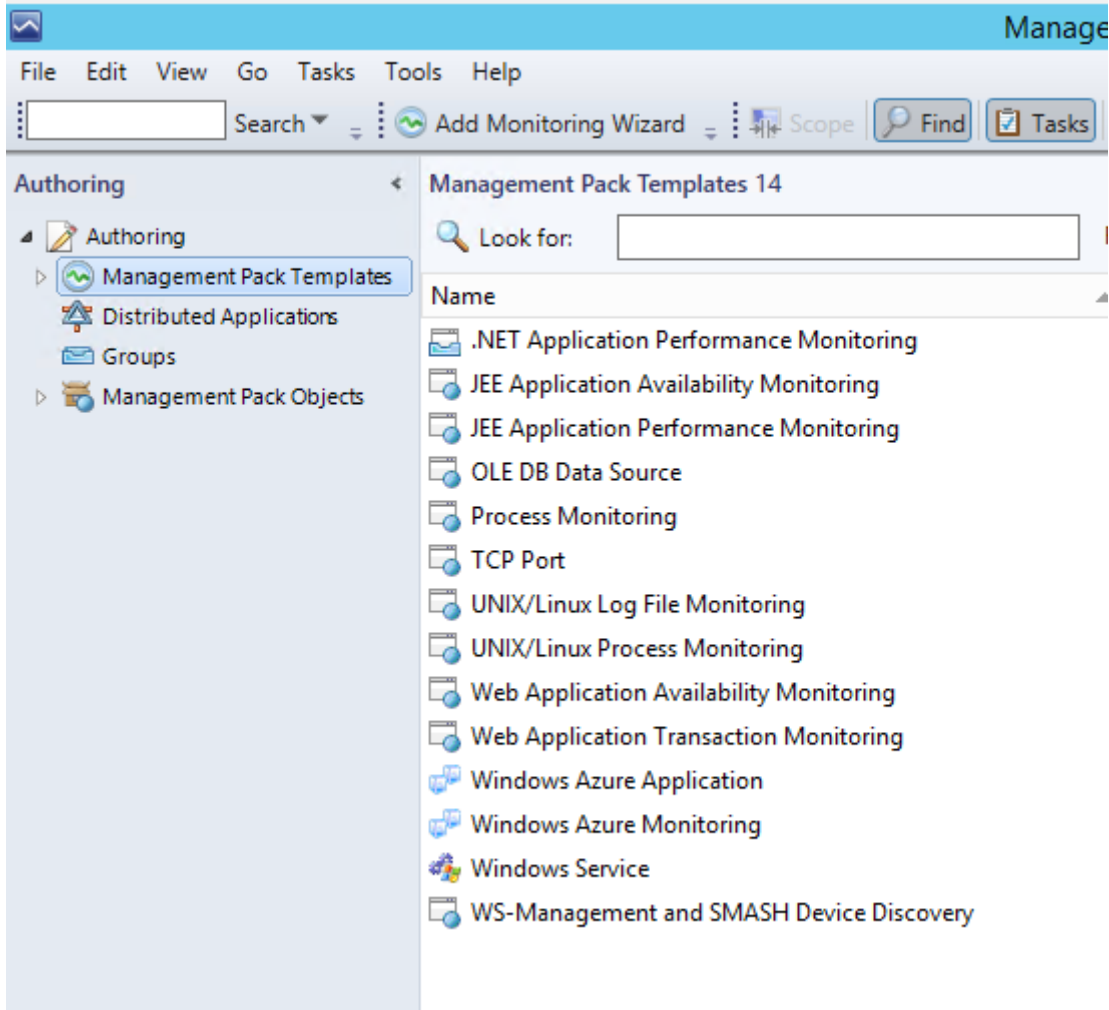
21. Click **Groups**. In System Center 2012 – Operations Manager groups can be used to scope views, reports, overrides, and alert notifications. Groups are created in the Authoring workspace in the Operations console.

22. Click the **Reporting** workspace.
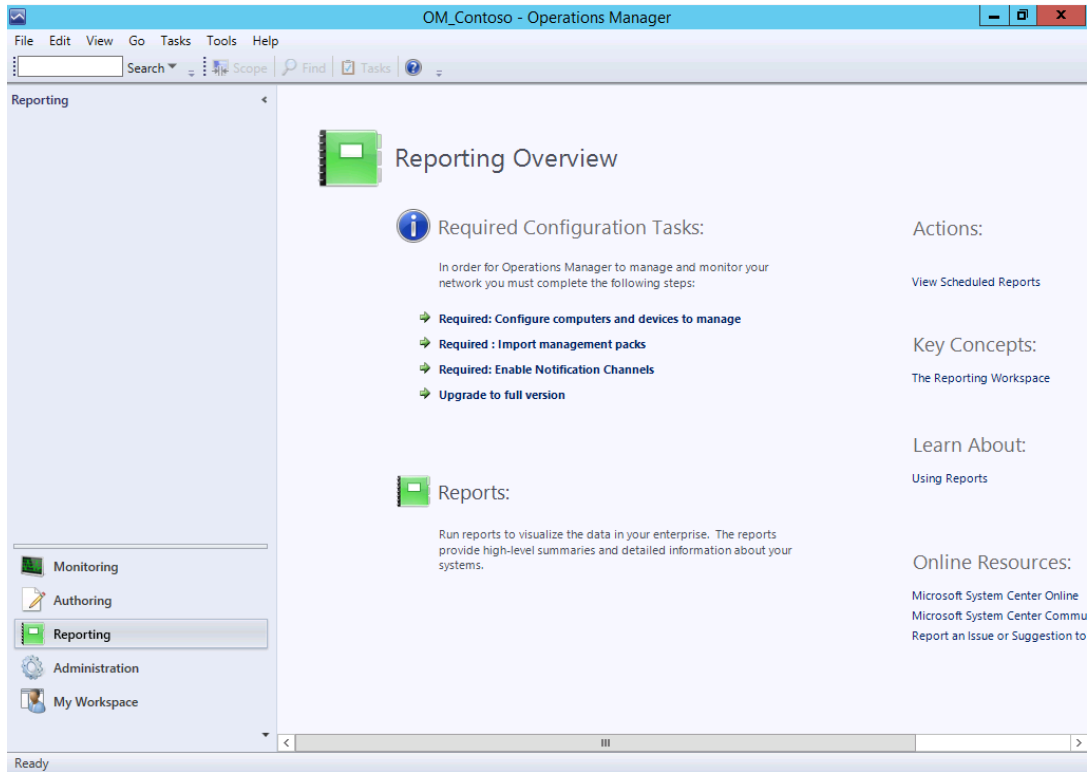
23. Operations Manager provides extensive reporting capabilities, including multiple report libraries that can be selected to customize reports for specific requirements. Reports perform a query against the data warehouse database and return the results in an easy-to-read format.

24. Click the **SQL Server 2012 (Monitoring)** node in the **Reporting** workspace. This view is used to open and schedule reports for various SQL Server tasks.

25. Click the **Administration** workspace.
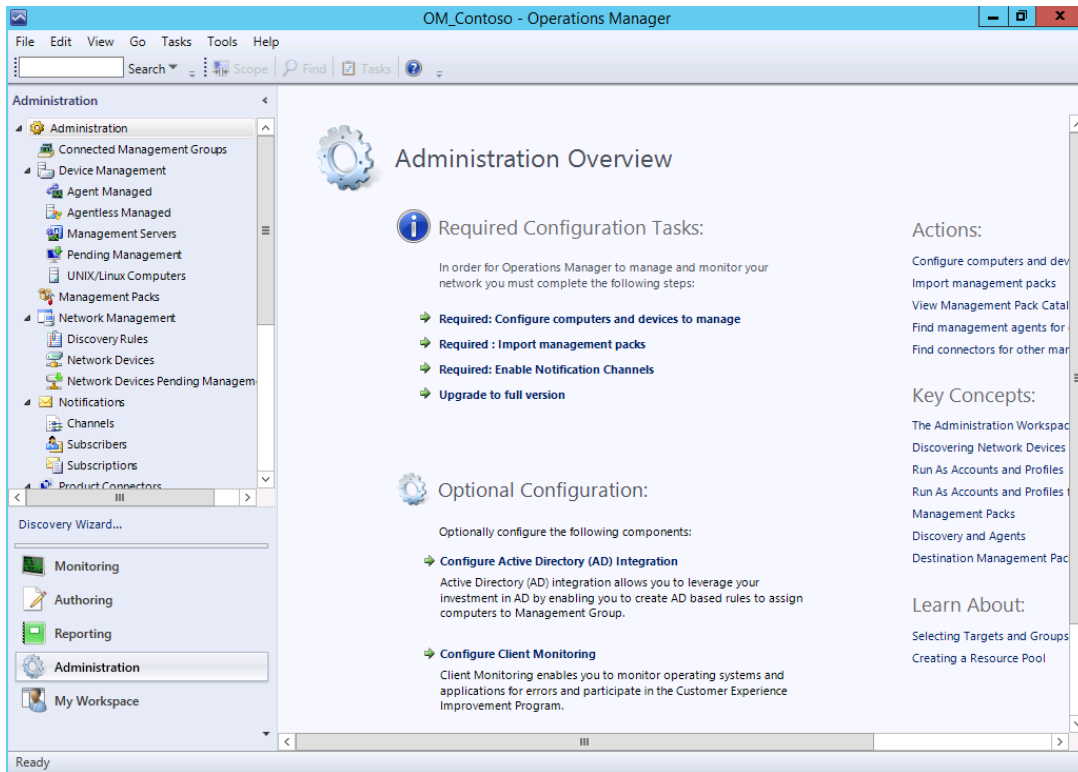
26. The Administration workspace is the primary workspace for administrators. The workspace is used to configure a management group and its managed objects. There are several different options available on this workspace.

27. Expand **Device Management**. Device management is used to perform configuration of specific management servers, agent-managed computers, agentless-managed computers, UNIX servers, and Linux servers.

28. Click **Agent Managed**. Various tasks can be performed on agent-managed computer, these include repairing or uninstalling an agent on a target computer.
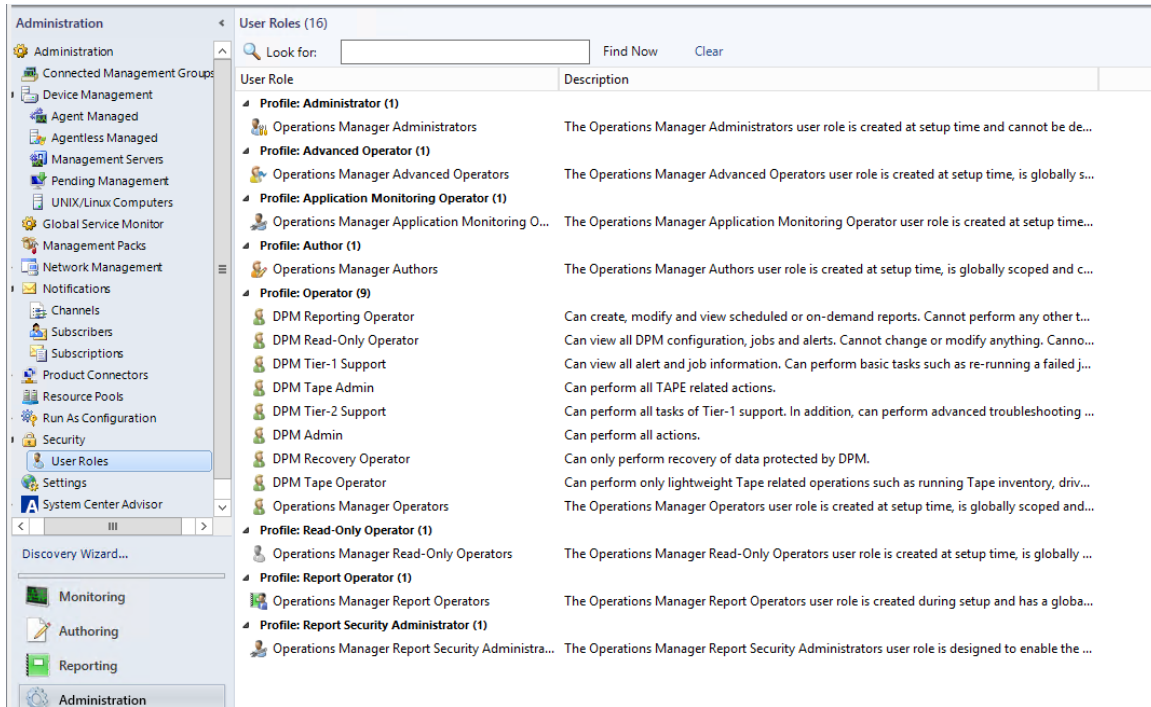
29. Click **Agentless Managed.** An agentless managed machine is a Microsoft Windows-based system in which an agent cannot be installed can be managed without an agent. Not all management packs support agentless management, for example the Active Directory management pack and the Microsoft Exchange Server 2003 management pack do not support agentless management.

30. Click **Management Packs**. This is a listing of all the management packs imported into the management group.

31. Right clicking an individual management pack in the results gives additional options such as viewing its properties, deleting the pack, or export any customizations to another management group.

32. Links in the tasks pane are used to create, import, and download management packs.

33. Click **Product Connectors**. Product connectors are used to synchronize Operations Manager data with other management systems such as those that monitor non-Windows computers or create trouble-tickets. Product connectors can integrate a deployment of Operations Manager into another management platform or connect other management systems into a full Operations Manager management solution. Any product connectors that the user integrates with Operations Manager will be displayed in this section of the Administration workspace.

34. Expand **Security** and click **User Roles**. In Operations Manager, operations such as resolving alerts, running tasks, overriding monitors, viewing alerts, viewing events, and so on have been grouped into user roles, with each user role representing a particular job function. Role-based security allows administrators to limit privileges that users have for various aspects of Operations Manager.

User Roles (16)	
Look for:	Find Now Clear
User Role	**Description**
◢ Profile: Administrator (1)	
Operations Manager Administrators	The Operations Manager Administrators user role is created at setup time and cannot be de…
◢ Profile: Advanced Operator (1)	
Operations Manager Advanced Operators	The Operations Manager Advanced Operators user role is created at setup time, is globally s…
◢ Profile: Application Monitoring Operator (1)	
Operations Manager Application Monitoring O…	The Operations Manager Application Monitoring Operator user role is created at setup time…
◢ Profile: Author (1)	
Operations Manager Authors	The Operations Manager Authors user role is created at setup time, is globally scoped and c…
◢ Profile: Operator (9)	
DPM Reporting Operator	Can create, modify and view scheduled or on-demand reports. Cannot perform any other t…
DPM Read-Only Operator	Can view all DPM configuration, jobs and alerts. Cannot change or modify anything. Canno…
DPM Tier-1 Support	Can view all alert and job information. Can perform basic tasks such as re-running a failed j…
DPM Tape Admin	Can perform all TAPE related actions.
DPM Tier-2 Support	Can perform all tasks of Tier-1 support. In addition, can perform advanced troubleshooting …
DPM Admin	Can perform all actions.
DPM Recovery Operator	Can only perform recovery of data protected by DPM.
DPM Tape Operator	Can perform only lightweight Tape related operations such as running Tape inventory, driv…
Operations Manager Operators	The Operations Manager Operators user role is created at setup time, is globally scoped and…
◢ Profile: Read-Only Operator (1)	
Operations Manager Read-Only Operators	The Operations Manager Read-Only Operators user role is created at setup time, is globally …
◢ Profile: Report Operator (1)	
Operations Manager Report Operators	The Operations Manager Report Operators user role is created during setup and has a globa…
◢ Profile: Report Security Administrator (1)	
Operations Manager Report Security Administra…	The Operations Manager Report Security Administrators user role is designed to enable the …

35. Expand **System Center Advisor**, click **Advisor Connection**. System Center Advisor is an online service that analyzes installations of Microsoft SQL Server 2008 (and later versions), and Windows Server 2008 and 2008 R2, and Lync Server 2010. Advisor collects data from the installations, analyzes it, and generates Alerts that identify potential issues (such as missing security patches) or deviations from identified best practices with regard to configuration and usage. Advisor also provides both current and historical views of the configuration of servers in an environment. This service is not available to explore as there is no Internet connection in the lab.

36. Click the **My Workspace** workspace. This workspace provides an area that can be customized for specific needs. Users can create folders to organize the workspace, add shortcuts to favorite views, save useful searches, and create views.
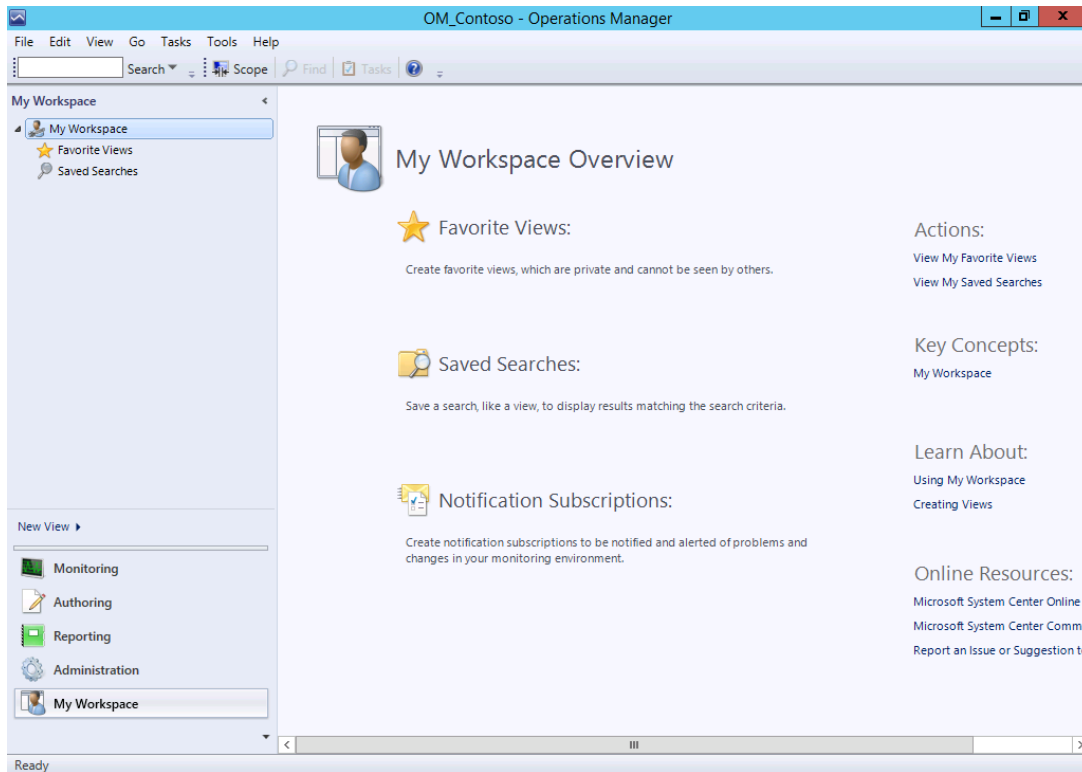
5.1.3 - SCA: Introduction to Advisor

In this exercise the user will learn about the different workspaces and functions of System Center Advisor, integrated with System Center 2012 R2 Operations Manager. Advisor is a free cloud service which offers proactive monitoring and best practice recommendations to reduce downtime and resolve issues faster. Advisor collects information about the servers and applications, then sends it to Azure for analysis. The resulting best practice recommendations can be viewed a web interface or integrated into System Center 2012 R2 Operations Manager. Sign up for free at www.SystemCenterAdvisor.com.

Estimated time to complete: 5 minutes

Perform the following on **SCOM01**

1. From **SCOM01** minimize the **Operations Manager Console** if it is open.

2. Double-click on the folder on the Desktop called **Advisor Solutions**.
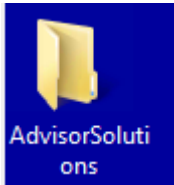
3. Double-click on the document entitled **System Center Advisor**. This is the System Center Advisor homepage where it is possible to sign up for a free account using a Microsoft ID. This lab does not have a connection to the Internet, so all of the websites which are displayed are actually all offline copies. This means that the links and other references to Internet locations will not work.

4. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

5. Navigate to the **Administration** workspace.
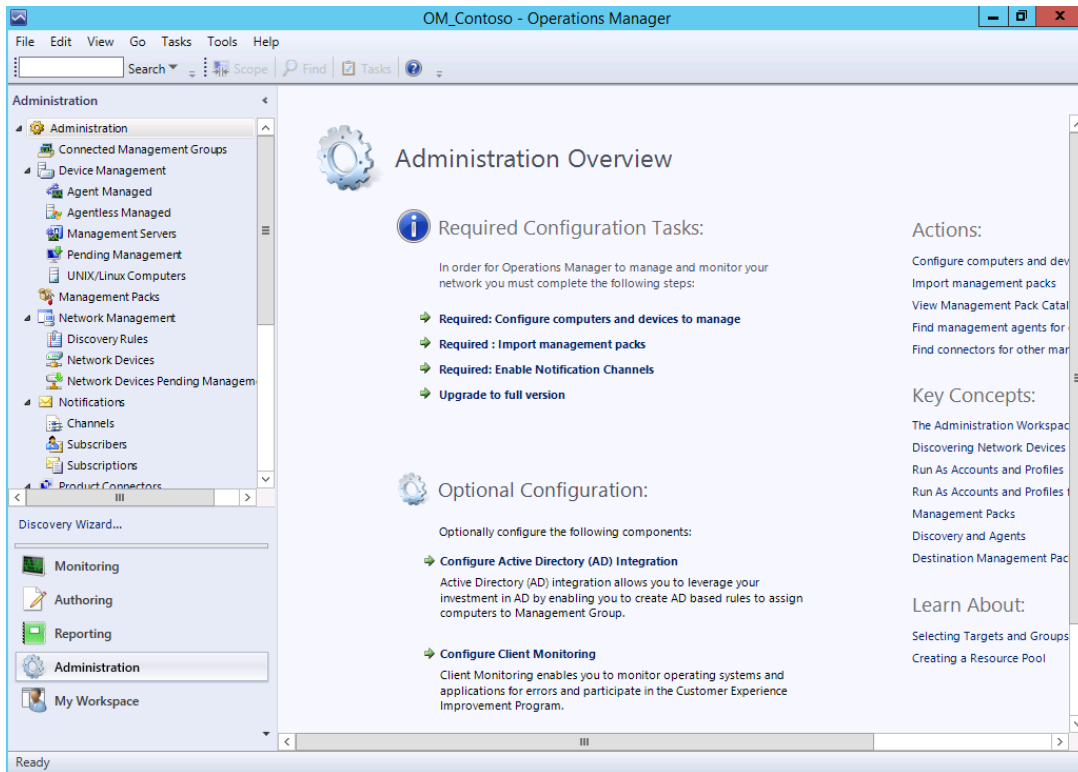
6. Scroll down and expand **System Center Advisor**.

7. Select **Advisor Connection**.

8. Read the information on the screen. In this lab a previous System Center Advisor connection had been established.
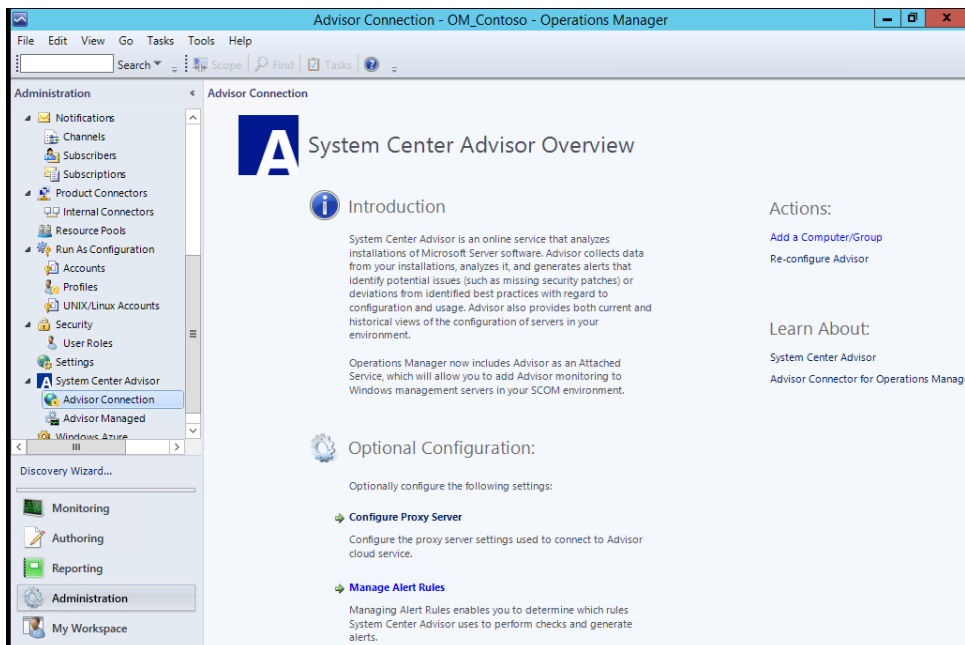
9. Under the **Actions** tab, note the **Add a Computer/Group** link. This is how a new computer would be monitored using Advisor.
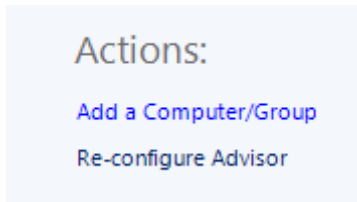
10. On the left navigation pane select **Advisor Managed**. This displays the servers which are currently managed by Advisor.
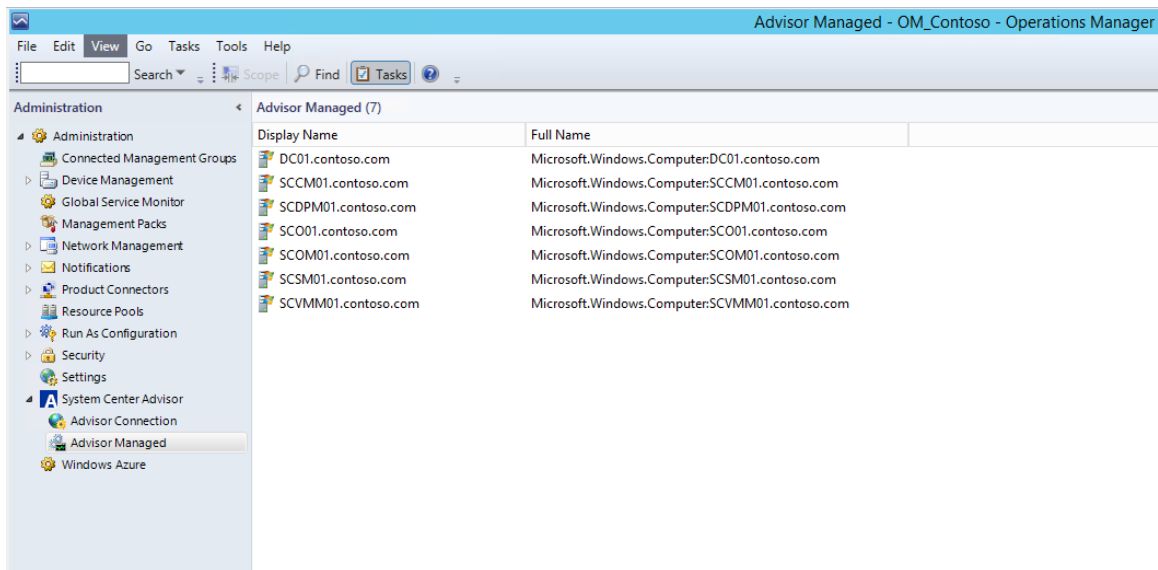
11. Select the **Monitoring** workspace.

12. On the left navigation pane navigate to **Monitoring** then expand **System Center Advisor**.

13. Select **Advisor Health State**. This shows the health of the management server which is SCOM01 and this also shows the health of the various Advisor agents.
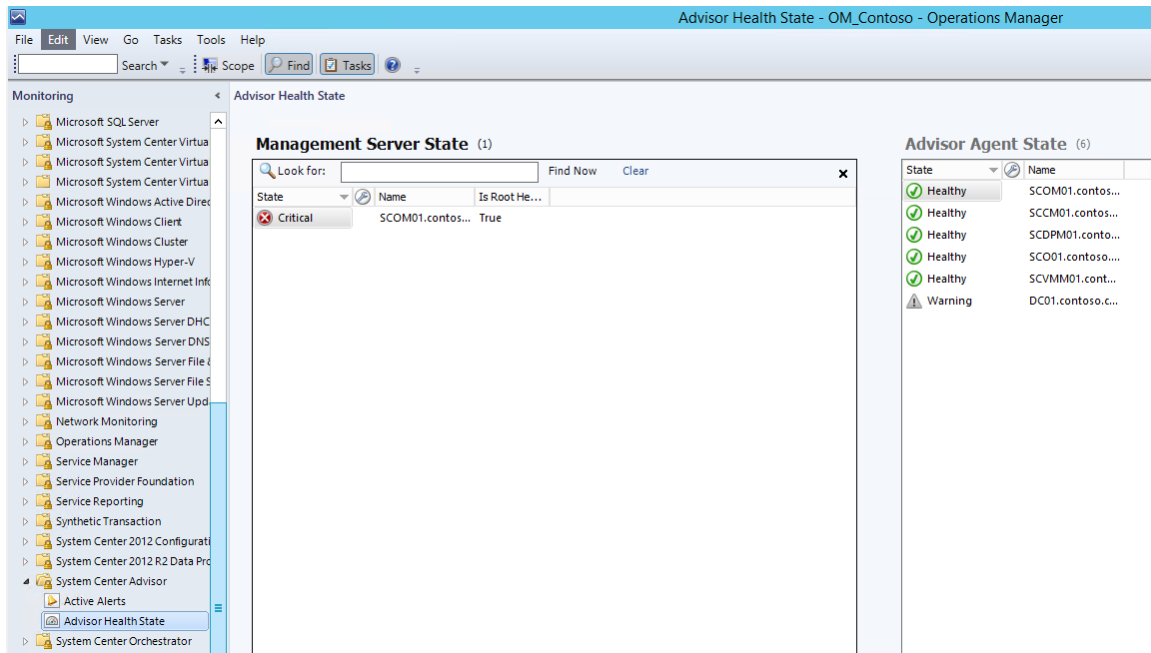
14. In the left navigation pane select **Active Alerts**. This displays all of the alerts for Advisor.

15. Under the list of critical alerts, select the alert with the title **Unsupported SQL Server version used by VMM.**
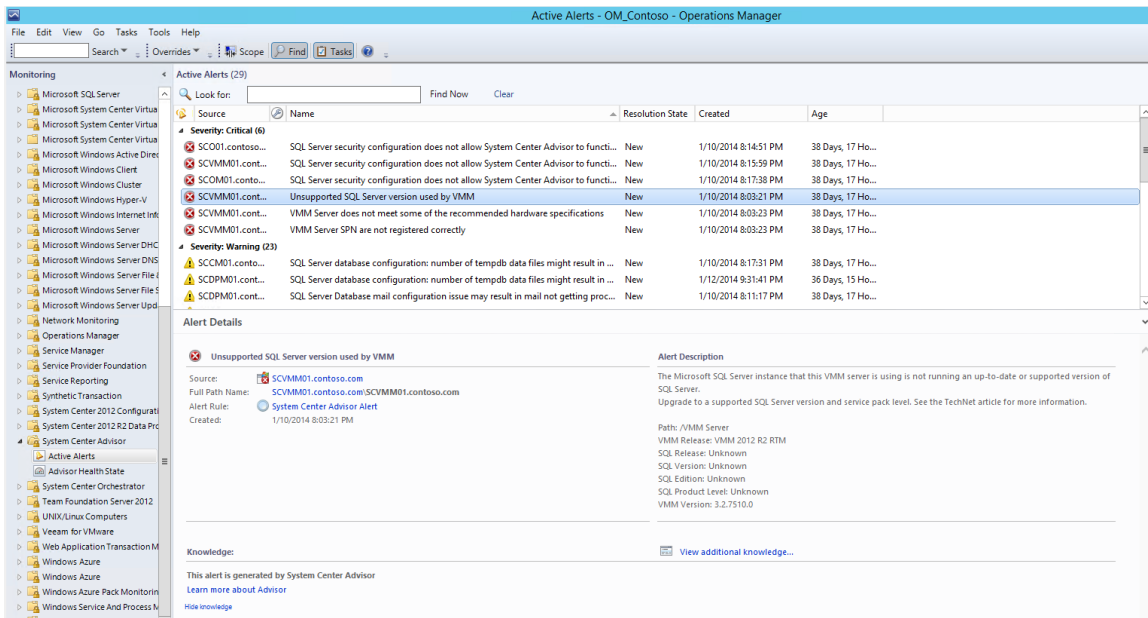
16. On the **Alert Details** in the center pane, read the information about the alert description. **System Center Advisor** provides information about both Windows Server and application issues.

5.2 - SCAC: Manage Applications through Self-Service

5.2.1 - SCAC: Deploy a Virtual Machine through Self-Service

In this exercise a self-service user will deploy a virtual machine from a template using App Controller.

Estimated time to complete: 5 minutes

SCVMM01

*Perform the following on **SCVMM01***

1. From **SCVMM01**, open **App Controller** by selecting the **Internet Explorer** icon from the taskbar.

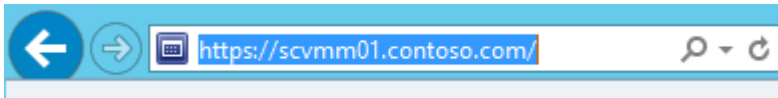2. If the site does not open, browse to **https://SCVMM01.contoso.com**.

3. If a notification appears about the certificate, click **Continue to this website (not recommended)**.
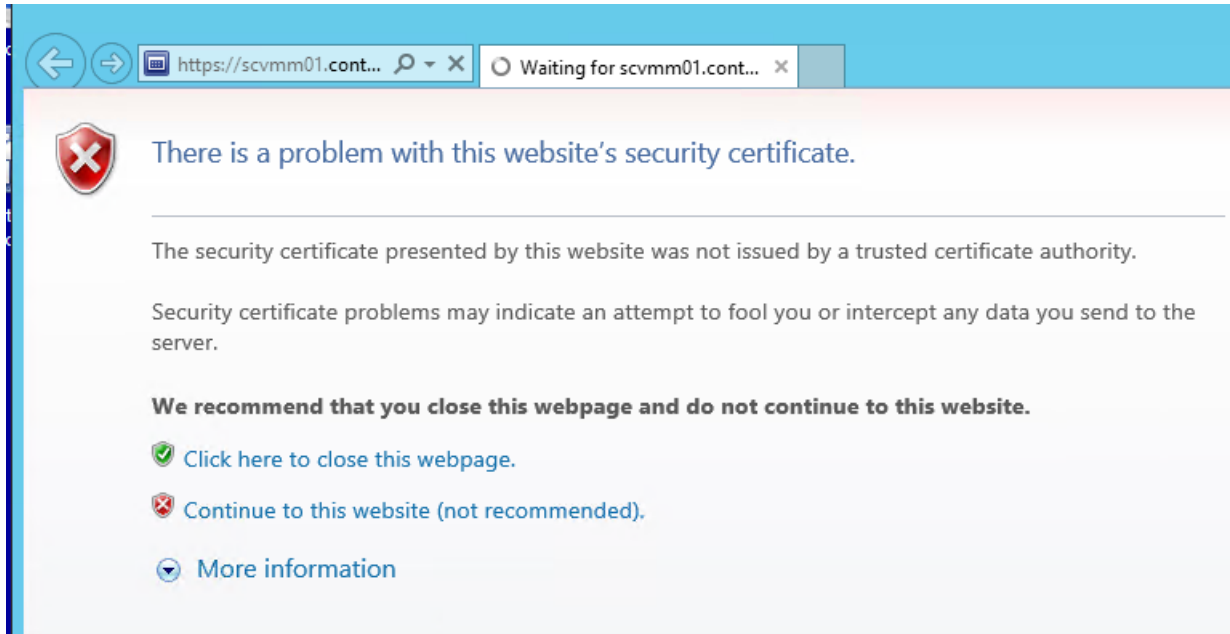
4. When prompted to sign in, enter **contoso\administrator** for the user name and **Passw0rd!** for the password. Click the **Sign In** button.

5. Navigate to the **Overview** workspace and review the information.

6. Select the **Virtual Machines** workspace.

7. Under **Virtual Machines**, click **Deploy**.
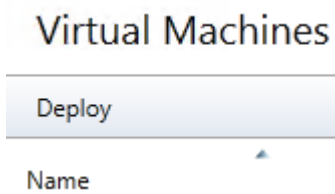
8. Under **New Deployment**, under **CLOUD**, select **Configure**.
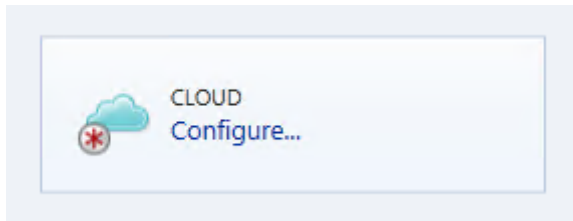
9. Select **Contoso-Cloud** and click **OK**.
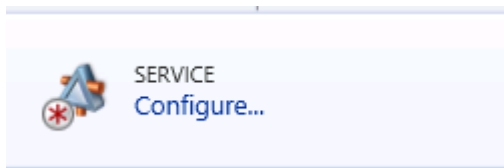

10. In the **TEMPLATE** box, click **Select a Template**.
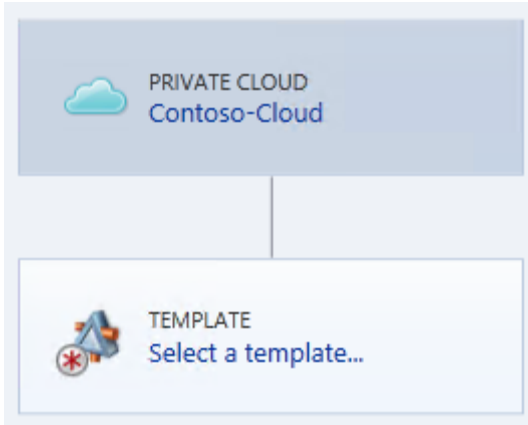
11. Select **VM_PetShop_Web** and click **OK**.

Choose a template

The available quota after the deployment is displayed for the selected template. You cannot deploy a template that exceeds the available quota for the cloud.
Location: SCVMM01.contoso.com\Contoso-Cloud

Filter: *(all)*

Name	Type	Release	Date Modified	Virtual Machines	CPU	Memory	Storage	Custom Quota
VM_PetShop_Web	Virtual Machine		1/28/2014 12:57 PM	1	1	64 MB	30 GB	1
Available Quota remaining after deployment								
Virtual Machines	CPU		Memory	Storage		Custom Quota		

12. In the **VIRTUAL MACHINE** box, click **Configure**.
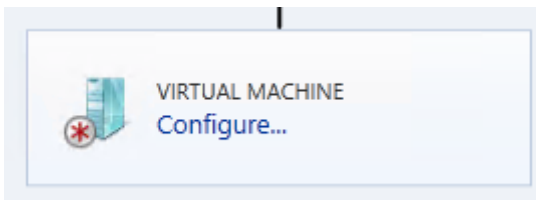
13. In **Virtual machine name**, enter **Contoso-Pet-Web** and review the settings below.

Properties of new virtual machine

Show all
Name and description
Virtual network adapters

Name and description

Virtual machine name: *
Contoso-Pet-Web

To generate a computer name, enter * only.
Computer name:
PetWeb##

Description:
VM Template for PetShop Website

Operating system:
Windows Server 2012 R2 Standard

Memory:
64 MB

14. Click **OK**.

15. In the lower right corner, click **Deploy**. The Virtual Machine deployment will start. Note that the deployment will fail, this is expected due to limitations of the lab environment (nested virtualization).
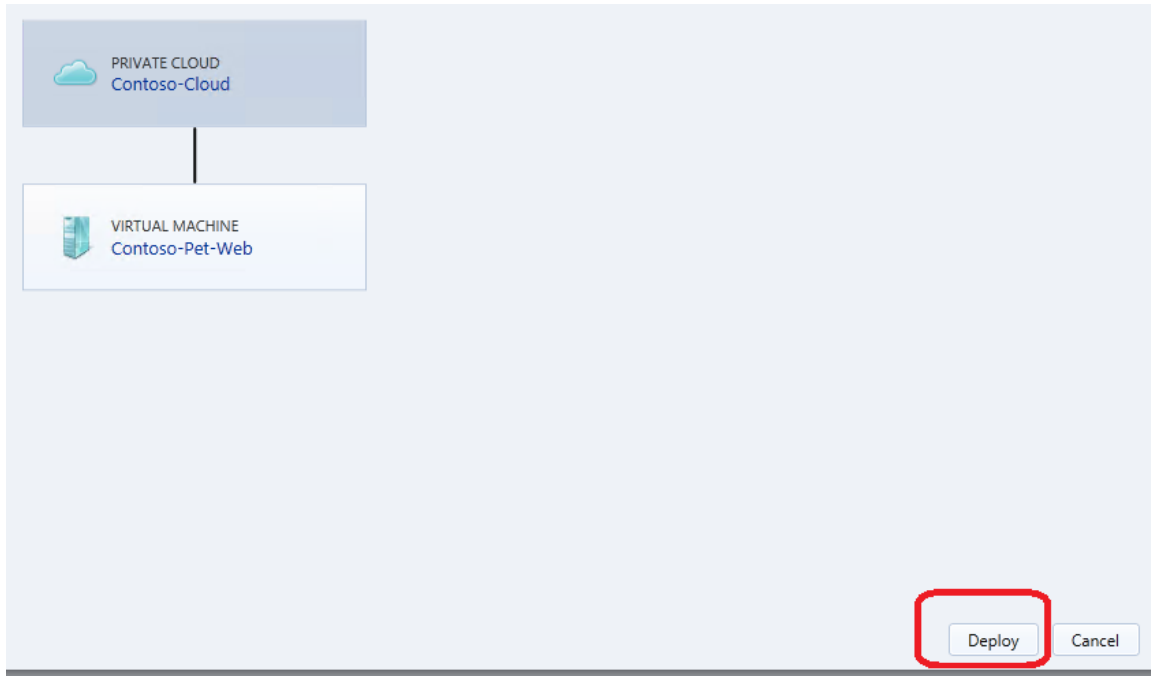
5.2.2 - SCAC: Deploy a Service through Self-Service

In this exercise a self-service user will deploy a service from a template using App Controller.

Estimated time to complete: 5 minutes

Perform the following on SCVMM01

1. From **SCVMM01**, open **App Controller** by selecting the **Internet Explorer** icon from the taskbar.

2. If the site does not open, browse to **https://SCVMM01.contoso.com**.

3. If a notification appears about the certificate, click **Continue to this website (not recommended)**.
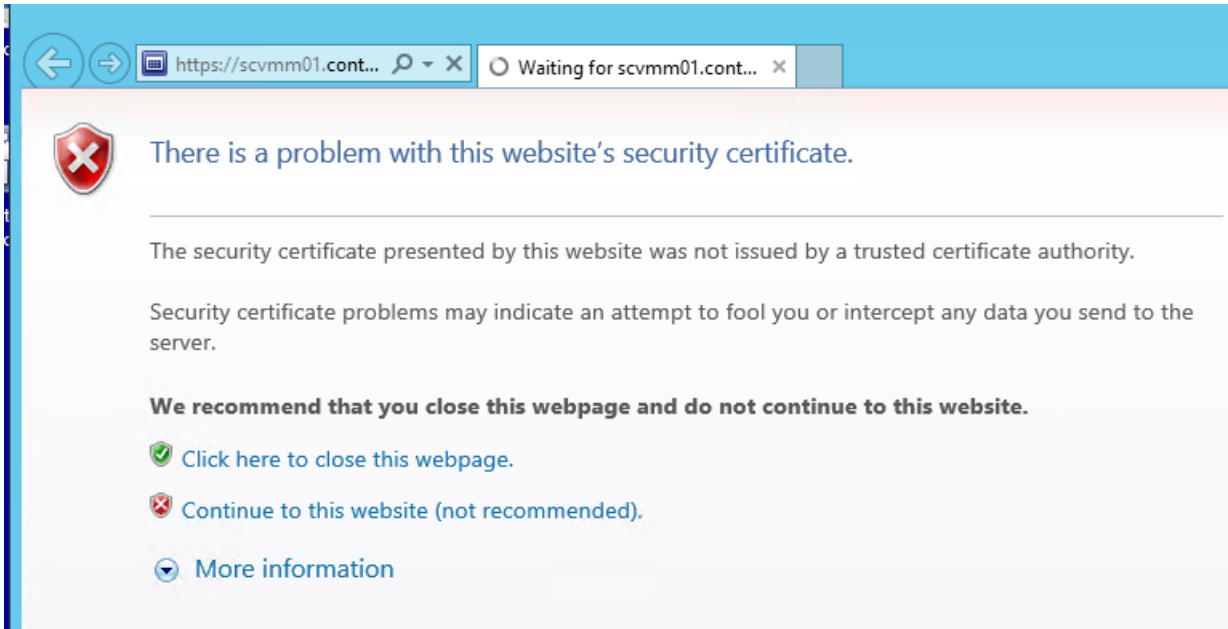
4. When prompted to sign in, enter **contoso\administrator** for the user name and **Passw0rd!** for the password. Click the **Sign In** button.

5. Navigate to the **Services** workspace.

6. Click **Deploy**.
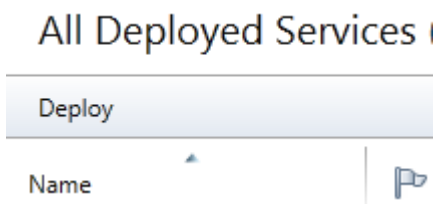
7. On the **New Deployment** page, under **Cloud**, click **Configure**.
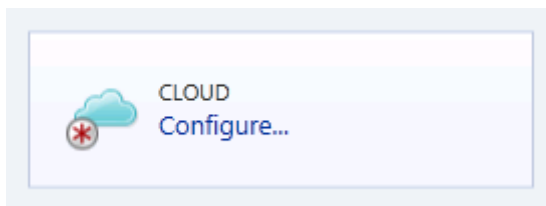
8. Select **Contoso-Cloud** and click **OK**.

9. In the **TEMPLATE** box, click **Select a template**.
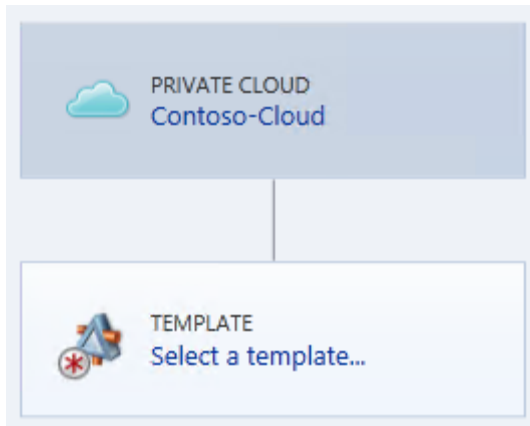
10. Select **PetShop_Service** and click **OK**. This shows the service template configuration.

11. In the **SERVICE** box, click **Configure**.

12. Under **Service name**, enter **PetShopDev**.

13. Under **Priority** select **Low** then click **OK**.

Properties of PetShop_Service service

General

Show all
General

Service name: *

PetShopDev

Description:

Two Tier Application Pattern

Priority:

Low

Cost center:

OK   Cancel

14. Under the **VM_PetShop_SQL** tier in the upper **INSTANCE** box, click **Configure**.

15. For **Computer name**, enter **PetSQL1A** and scroll down to review the settings.

16. Click **OK**.

17. In the **INSTANCE** box in the lower left, click **Configure**.

18. For **Computer name,** enter **PetSQL1B** and click **OK**.

19. Under the **VM_PetShop_Web** tier in the upper **INSTANCE** box, click **Configure**.

20. In the **Computer name**, enter **PetWeb1A** and click **OK**.

21. Click **Configure** for the **INSTANCE** in the lower right.

22. In the **Computer** name, enter **PetWeb1B** and click **OK**.

Computer name:

PetWeb1B

23. In the lower right corner, click **Deploy**.

The Virtual Machine deployment will start. Note that the deployment will fail, this is expected due to limitations of the lab environment (nested virtualization).

5.3 - SCOM: Monitor Applications

5.3.1 - SCOM: Monitor Applications

In this exercise the SQL Server 2012 servers that are used to support System Center 2012 R2 will be monitored and analyzed using Operations Manager. Operations Manager provides real-time monitoring through alerts, as well as other helpful information about the performance, health and capacity of application, hardware, networking components, hypervisors, and virtual machines.

Estimated time to complete: 5 minutes

SCOM01

Perform the following on ***SCOM01***

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

2. Navigate to the **Monitoring** workspace**.**
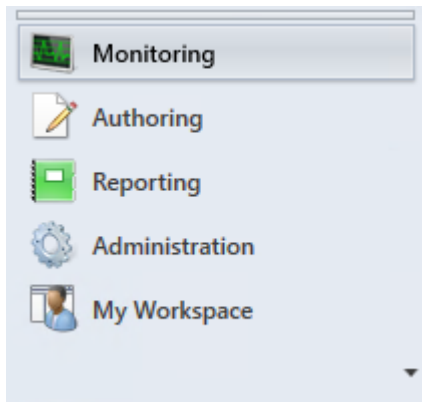
3. Navigate to **Monitoring** > **Microsoft SQL Server** and select **Active Alerts.**
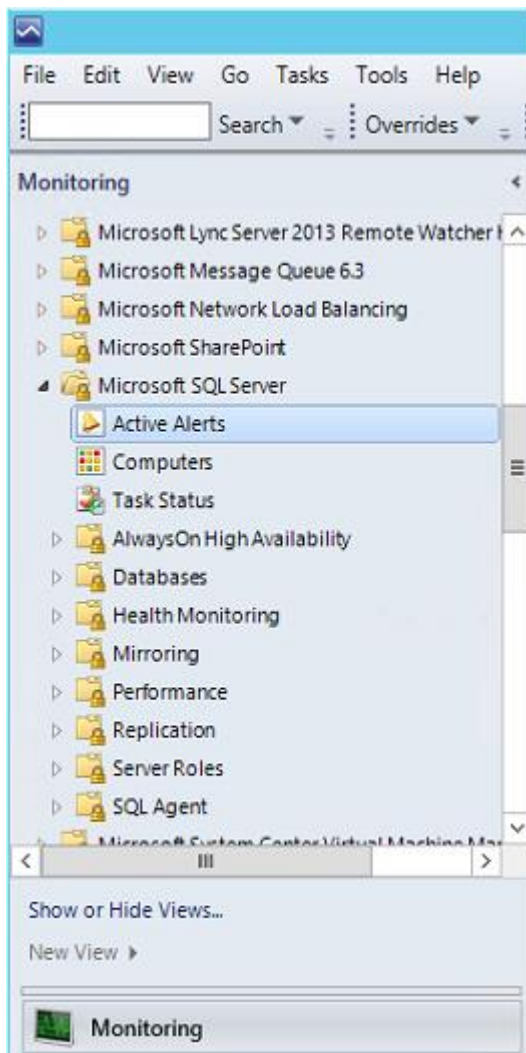
4. **Select** the critical active alert with the name, **Run As Account does not exist on the target system or does not have enough permissions**. The full list of SQL Server alerts may be different than the screenshot below.

5. From the **Tasks** pane, select **Alert Properties**.
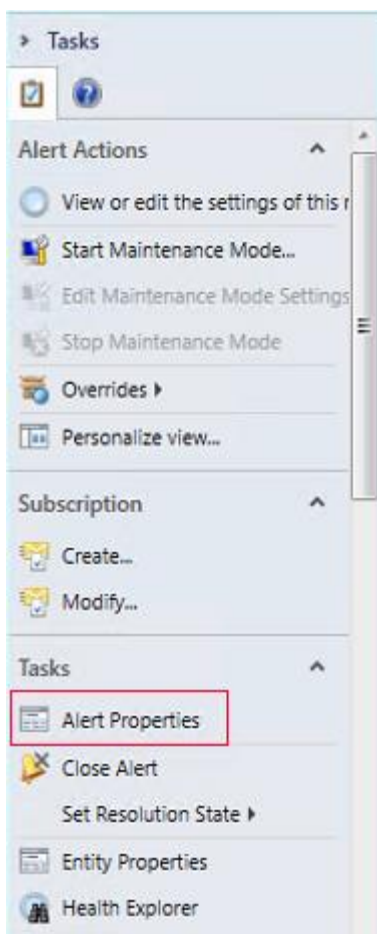
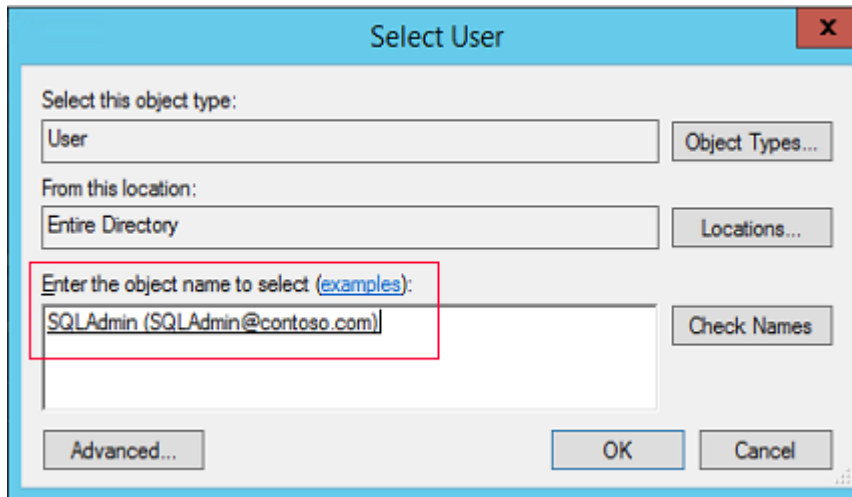6. Under the General tab, for **Owner** click the **Change** button.
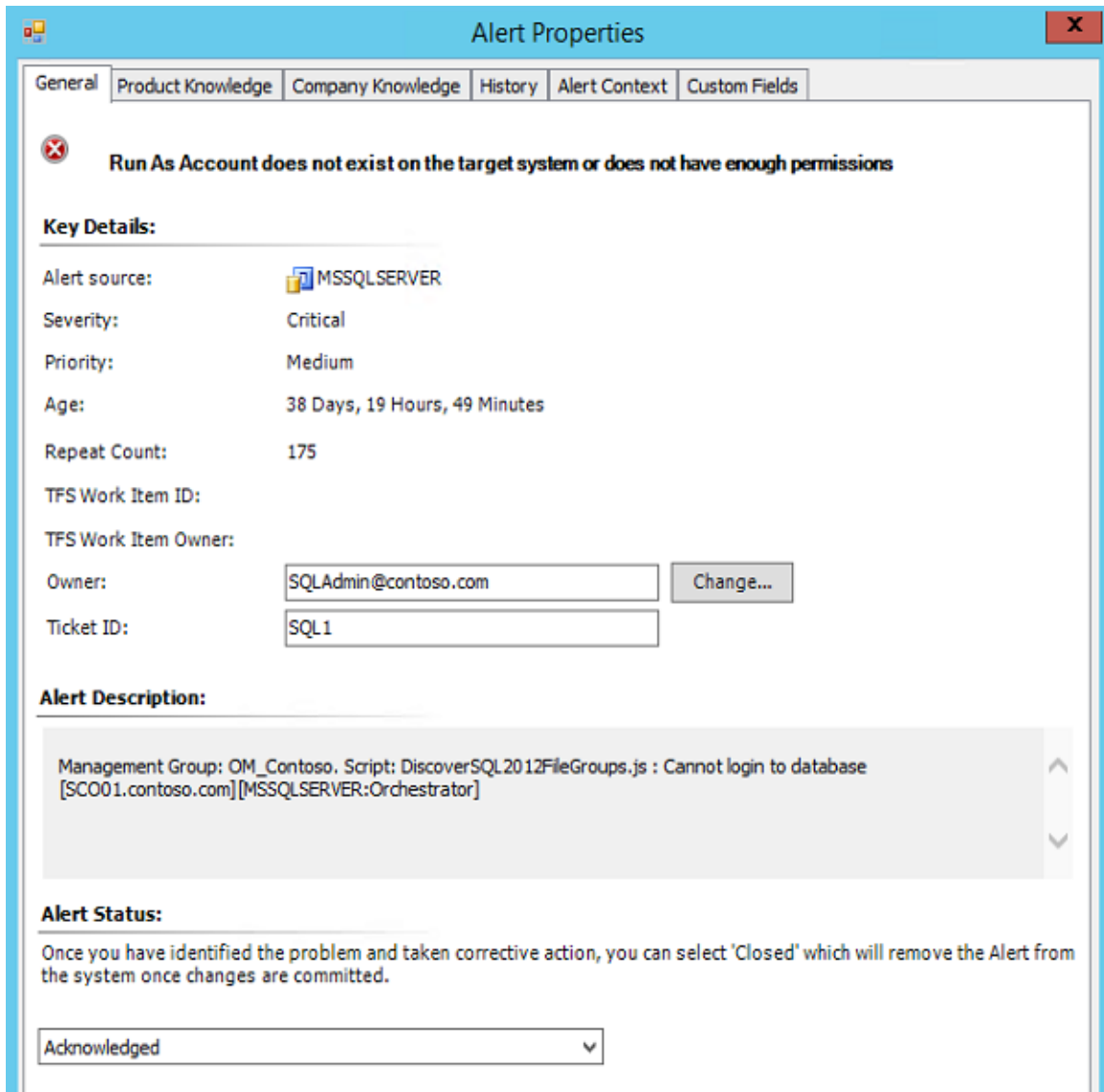
TFS Work Item Owner:

Owner: [   ]   [Change...]

Ticket ID: [   ]

7. In the **Select User** dialog enter **SQLAdmin** and click **Check Name** to have it resolve to **SQLAdmin@Contoso.com**

8. Under Ticket ID enter **SQL1**

9. Under **Alert Status** in the dropdown, choose **Acknowledged**.

10. Click **Apply**.

11. Select the **Product Knowledge** tab and review the information.
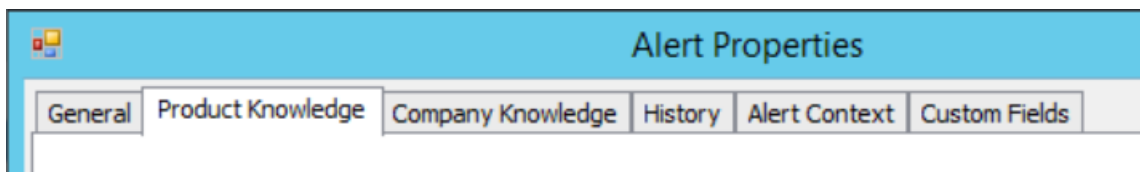
12. Select the **Alert Context** tab and review the information.
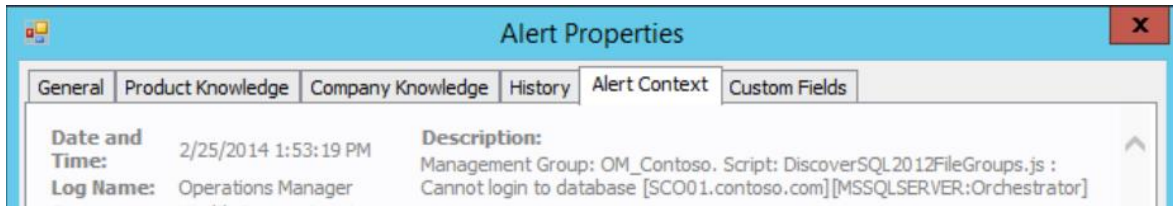
13. Click **OK**.

14. From the left navigation pane, select the **Computers** tab.
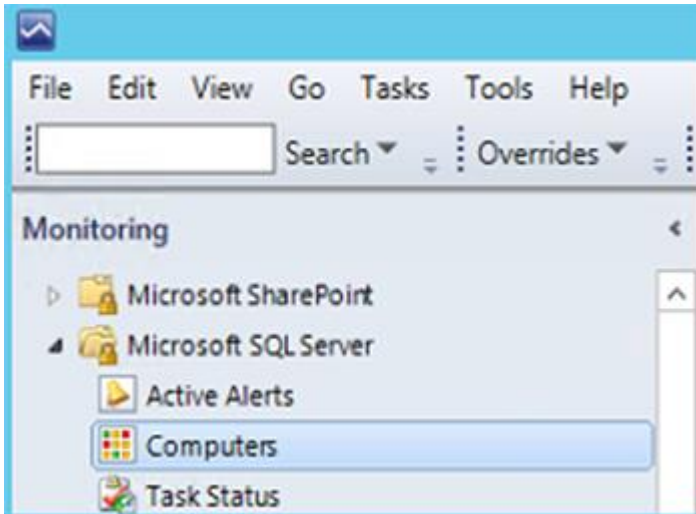
15. Select any of the computers which are being monitored.

16. On the **Task** pane, under **Windows Computer Tasks**, select **Ping Computer**.
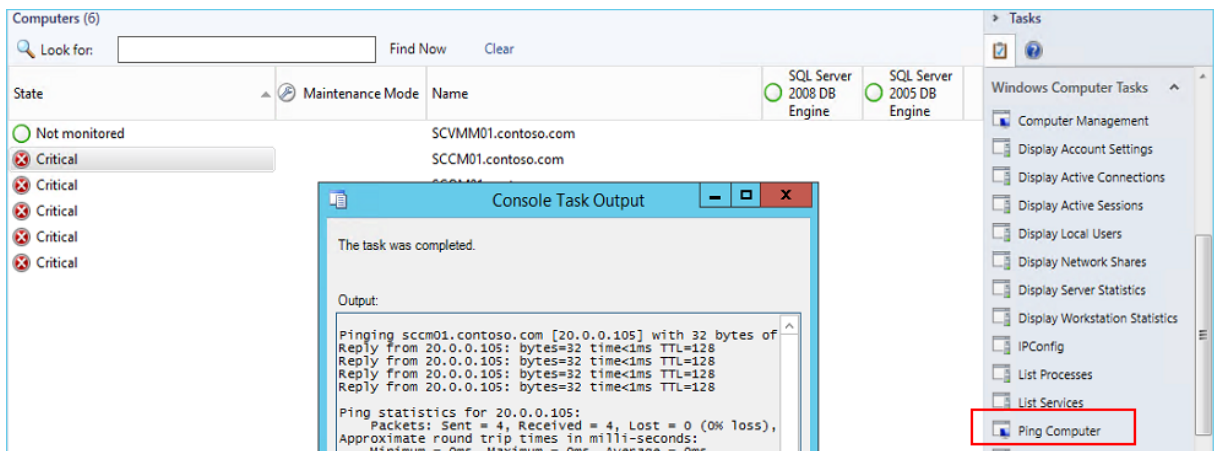
17. Once the output completes, **close** the console task output.

18. On the **Task** pane, under **Windows Computer Tasks**, select **List Services**.

Windows Computer Tasks ^

- 🖥 Computer Management
- 🗒 Display Account Settings
- 🗒 Display Active Connections
- 🗒 Display Active Sessions
- 🗒 Display Local Users
- 🗒 Display Network Shares
- 🗒 Display Server Statistics
- 🗒 Display Workstation Statistics
- 🗒 IPConfig
- 🗒 List Processes
- 🗒 List Services
- 🖥 Ping Computer
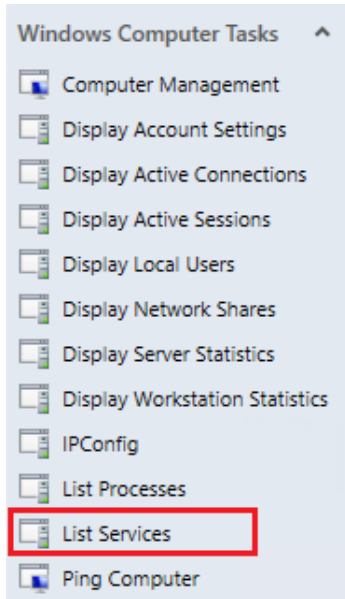
19. On the **Run Task - List Services** dialog, select **Run**.
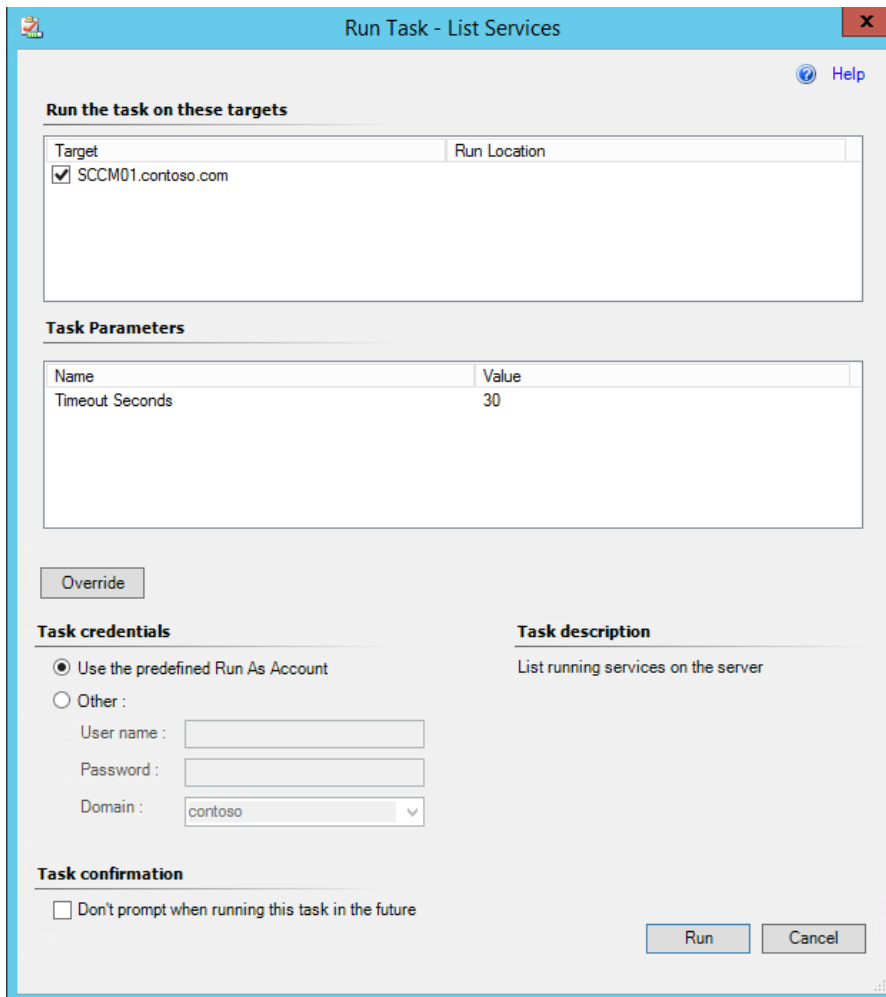
20. When the Task Output appears, expand the dialog box and review the information.

21. Click **Close**.
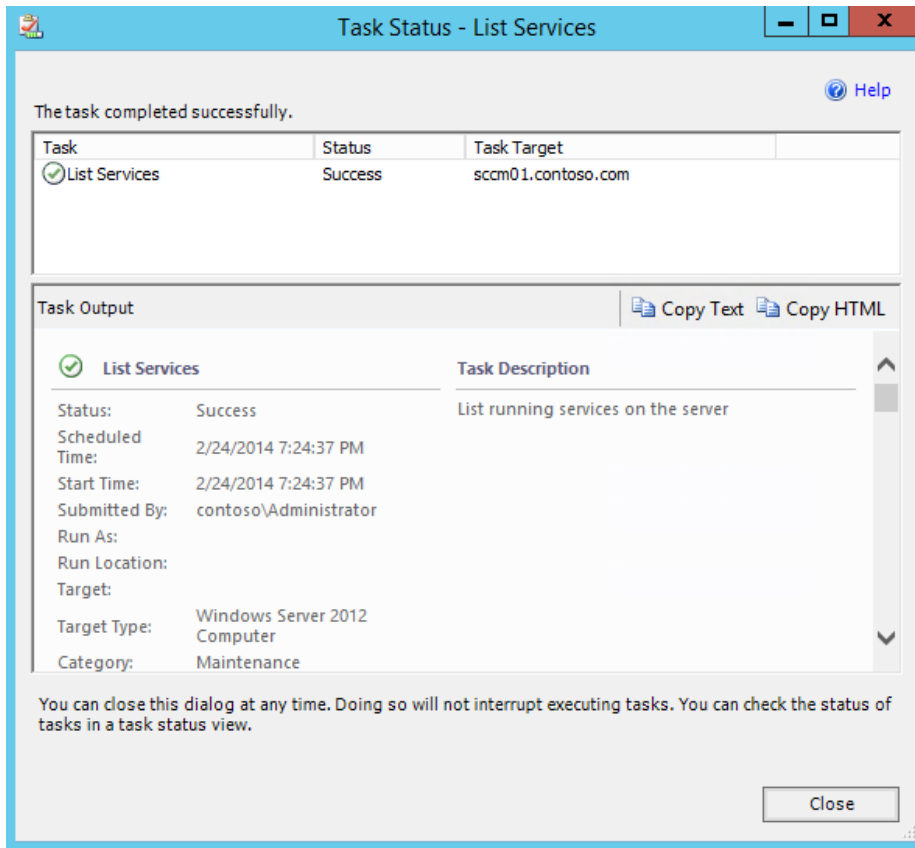
22. On the left navigation pane select **Microsoft SQL Server | Databases | Database State**.

23. **Review** the various databases which are monitored across this lab.
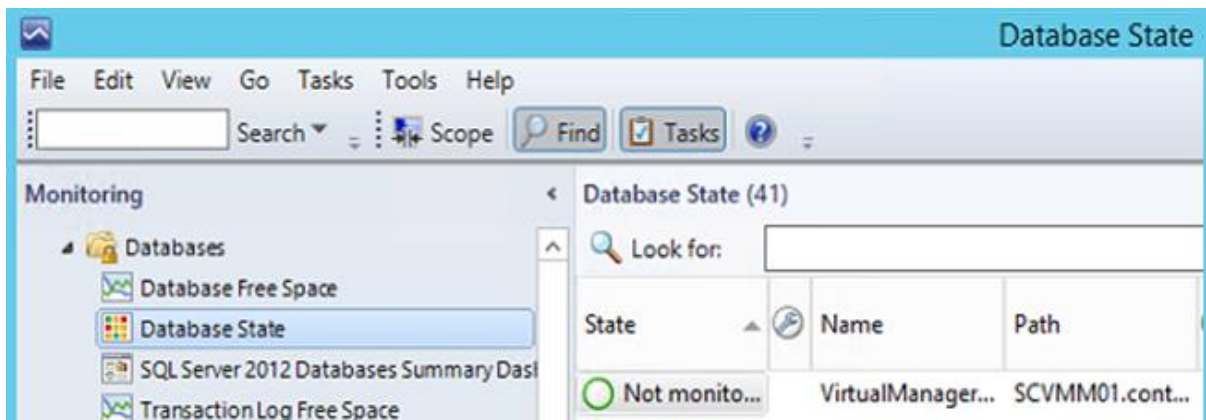
24. On the left navigation pane select **Microsoft SQL Server | Health Monitoring | Agent Health** and review the information.
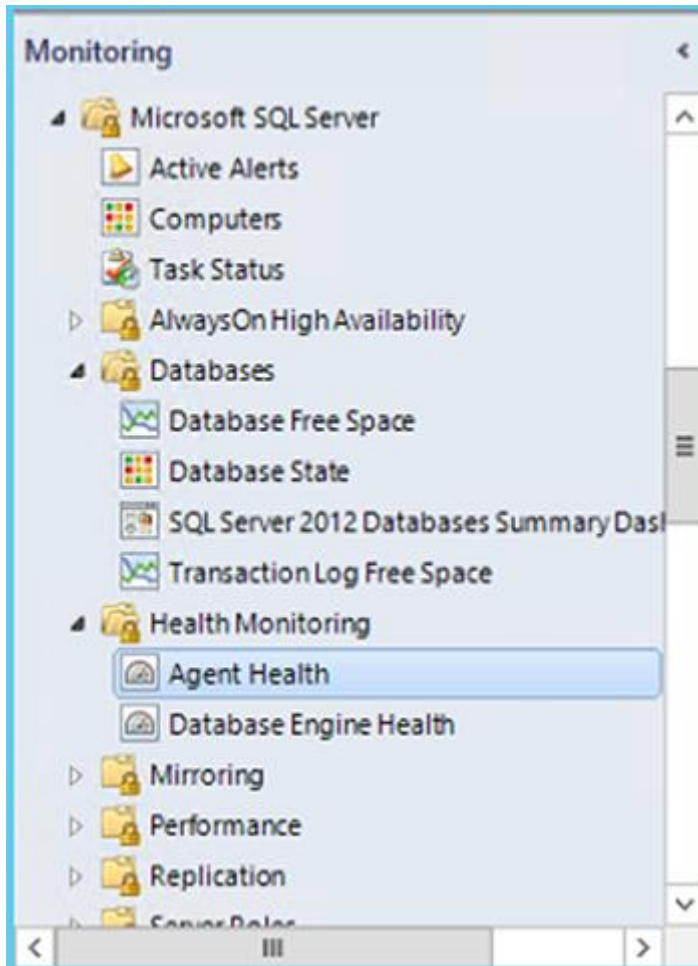

25. Under **Health Monitoring**, navigate to **Database Engine Health** and review the information.
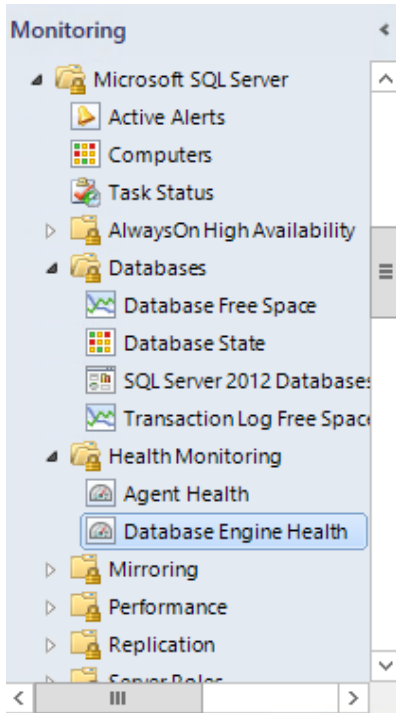
26. Navigate to **Microsoft SQL Server | Server Roles | Analysis Services**.
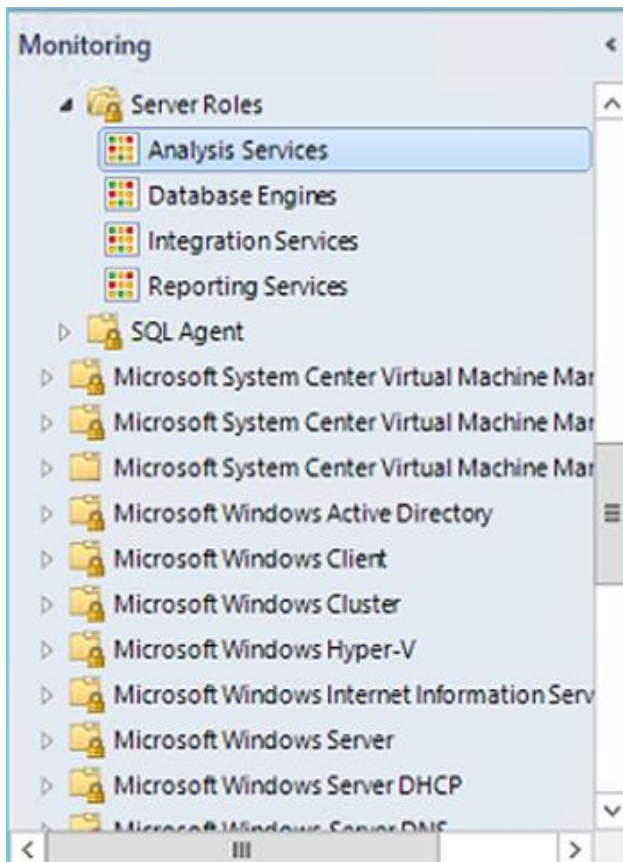
27. Select **MSSQLSERVER** under the path **SCOM01.contoso.com** and review the information in the detail view.

28. Select **Server Roles | Database Engines**.

29. Select the database engine named **MSSQLSERVER** for **SCVMM01.contoso.com** and review the information in the detail view.

30. Navigate to **Microsoft SQL Server | Server Roles | Reporting Services**.

31. Select **MSSSQLSERVER SCCM01.contoso.com** and review the information.

32. Navigate to **Microsoft SQL Server | SQL Agent | SQL Agent State**.
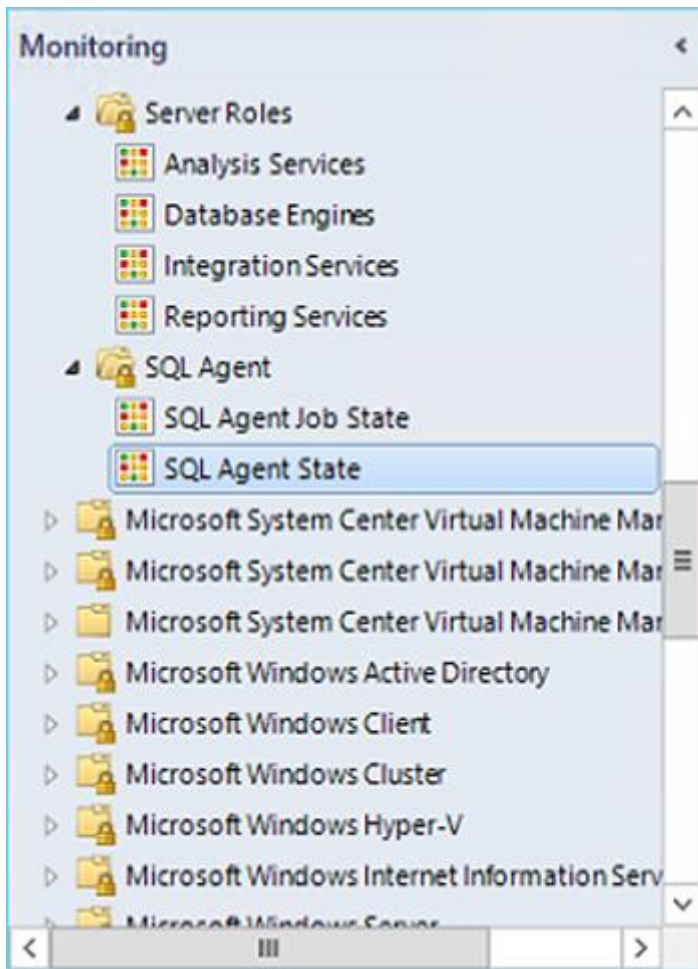
33. Select the **SQLSERVERAGENT** for **SCOM01.contoso.com** and review the information in the **Detail View**.

34. Feel free to browse some of the other application monitoring views. This lab includes views that do not contain any data, as not all applications are deployed within this lab.

    Other application views include:

35. Forefront Endpoint Protection

36. Microsoft BizTalk RFID

37. Microsoft BizTalk Server 2013

38. Microsoft Dynamics NAV 2013

39. Microsoft Exchange Server 2013

40. Microsoft Lync Server 2013 Health

41. Microsoft SharePoint

42. Team Foundation Server 2013

43. Windows Azure

44. Windows Service And Process Monitoring

5.3.2 - SCOM: Monitor a Distributed Application

In this exercise a distributed application will be configured, which allows a collection of objects to be viewed as related and interconnected services through Operations Manager. A two-tier Distributed Application will be designed which represents the Service Manager Console and SQL database (SCSM01) and the IIS website for the self-service portal (SCSM02).

Estimated time to complete: 10 minutes

Perform the following on **SCOM01**

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

2. Navigate to the **Authoring** workspace.

3. Expand **Authoring** and select **Distributed Applications**.
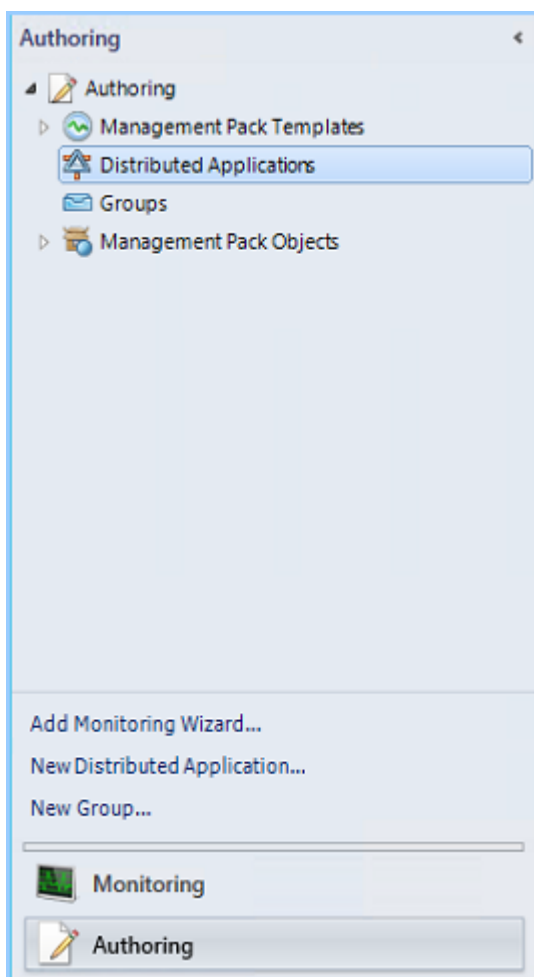
4. From the upper ribbon select **Create a New Distributed Application**.

5. Under **Name** enter **Service Manager Portal**.

6. Under **Template** select: **Line of Business Web Application.**

7. Under **Management Pack** select **Default Management Pack.**

8. Click **OK**.

9. The **Distributed Application Designer** should appear. Maximize the designer.

10. Select the upper box that says **Service Manager Portal Web Application Web Sites**.

11. On the top ribbon bar, click **Save**. This will take several minutes to complete.

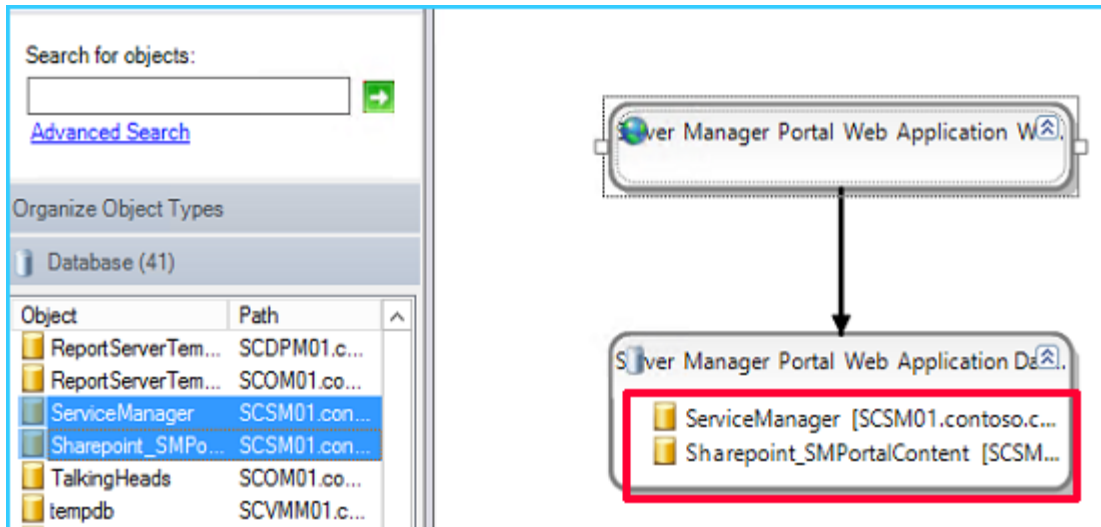12. Select the object called **Service Manager Portal Web Application Databases**.
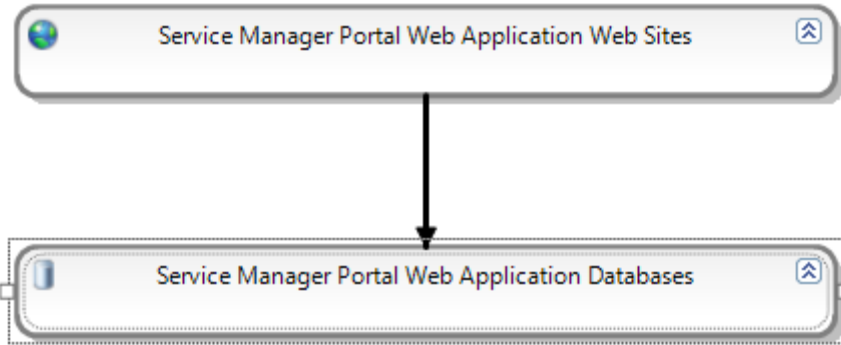
13. From the lower left corner select the **Database** group.

14. From the databases, select the database called **ServiceManager**. Hold **Ctrl** and also select the database called **SharePointP_SMPortal**.
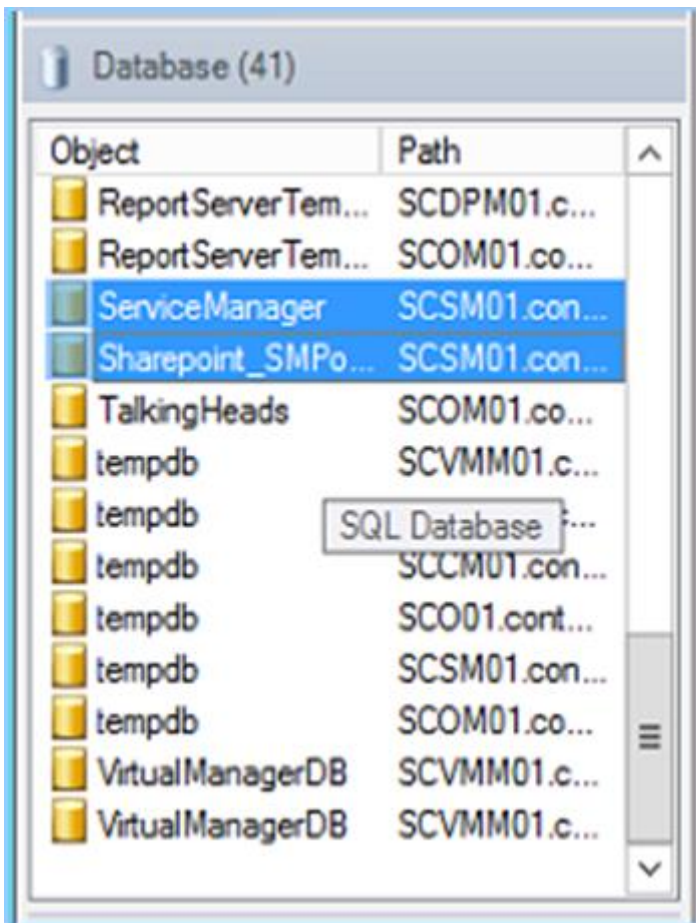
15. Right-click the 2 databases. Select **Add to** > **Service Manager Portal Web Application Databases**.

16. Select the **Service Manager Portal Web Application Web Sites.**
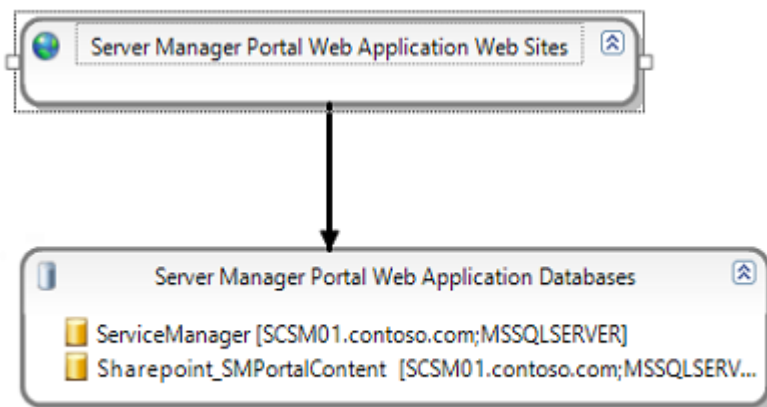
17. Click on **Web Site** in the lower left corner.

18. Select the **Default Web Site SCSM01.contoso.com**. Hold **Ctrl** and also select **SCSMWebContentServer** .

Objects

Search for objects:

Advanced Search

Organize Object Types

Database (41)

Distributed Application Component

Service

Web Site (12)

Object	Path
AppController	SCVMM01.contoso.com
Default Web Site	SCDPM01.contoso.com
Default Web Site	SCOM01.contoso.com
Default Web Site	SCSM01.contoso.com
Default Web Site	SCO01.contoso.com
Default Web Site	SCCM01.contoso.com
Default Web Site	DC01.contoso.com
Default Web Site	SCVMM01.contoso.com
Microsoft System Center ...	SCO01.contoso.com
Microsoft System Center ...	SCO01.contoso.com
SCSMWebContentServer	SCSM01.contoso.com
WSUS Administration	SCCM01.contoso.com

19. **Right-click** on one of the selected and choose **Add to** > **Service Manger Portal Web Application Web Sites**.
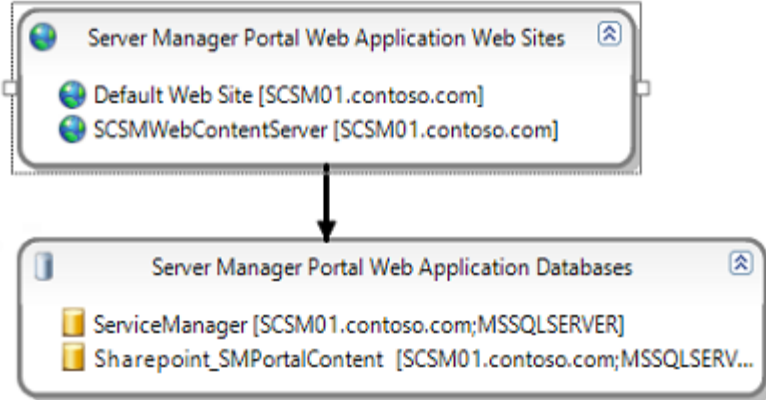
20. On the top ribbon bar, click **Add Component**.

21. Under **Name your component group** enter **IIS Web Site**.

22. In the **Create New Component Group** select the button **Objects of the following type(s).**
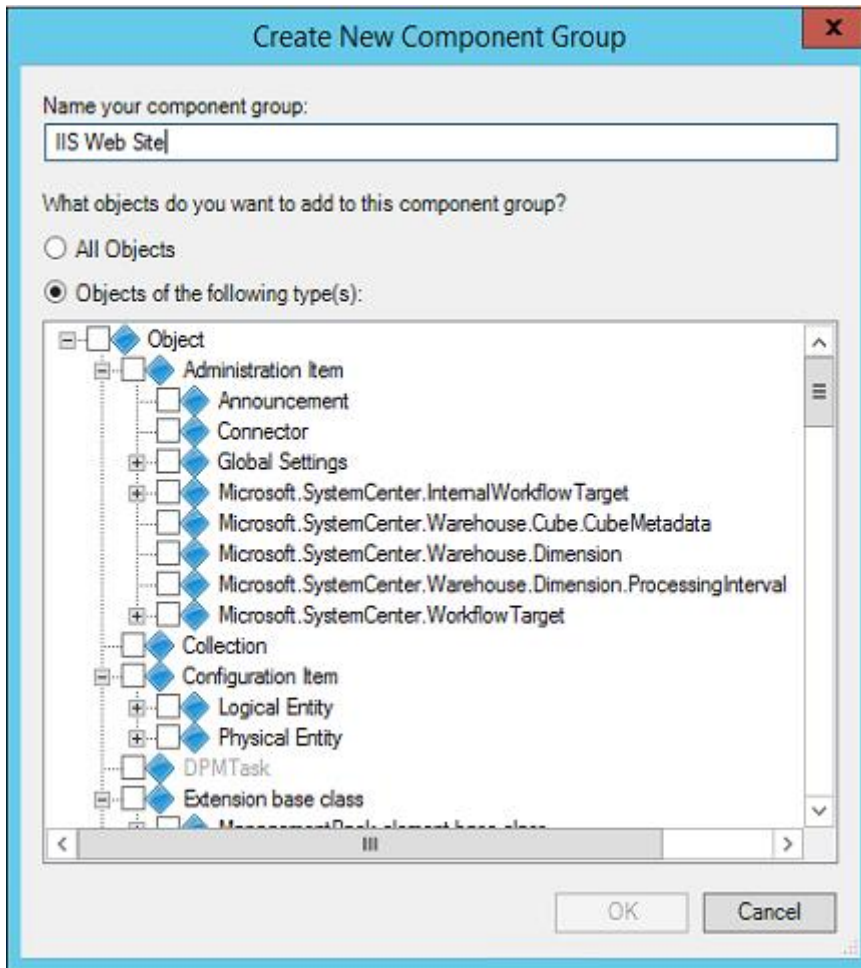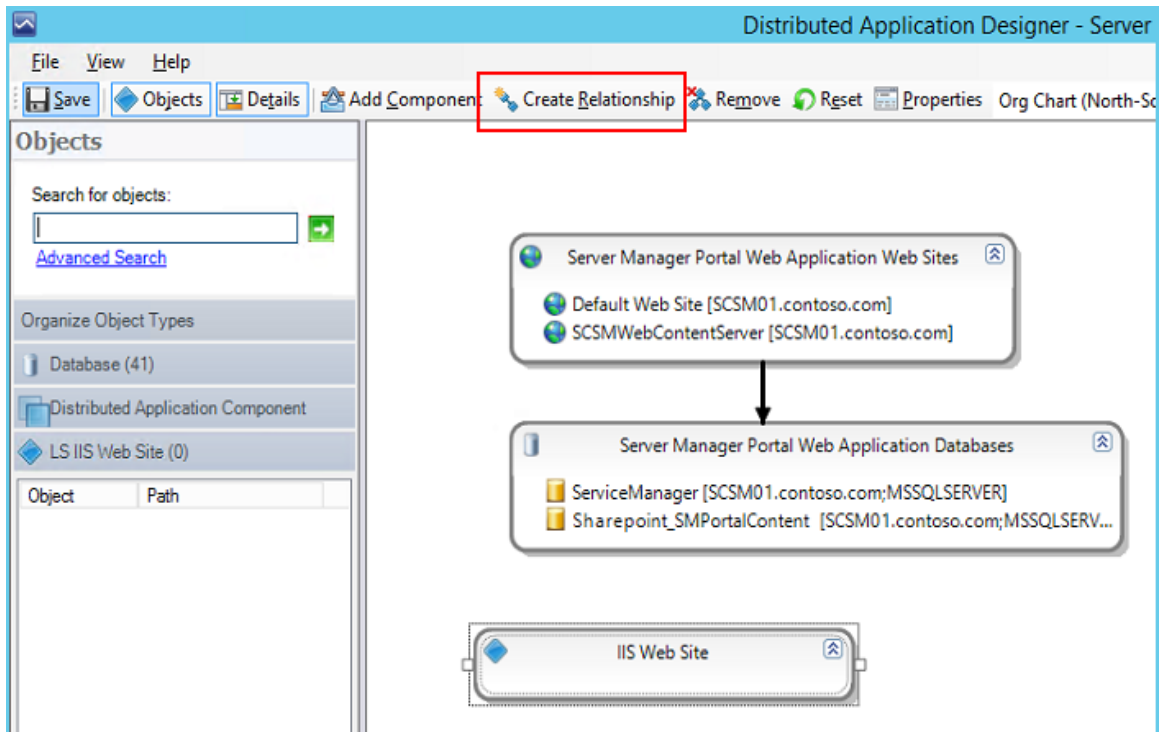
23. Scroll down and select **LS IIS Web Site** and also **LS IIS Web Application.**
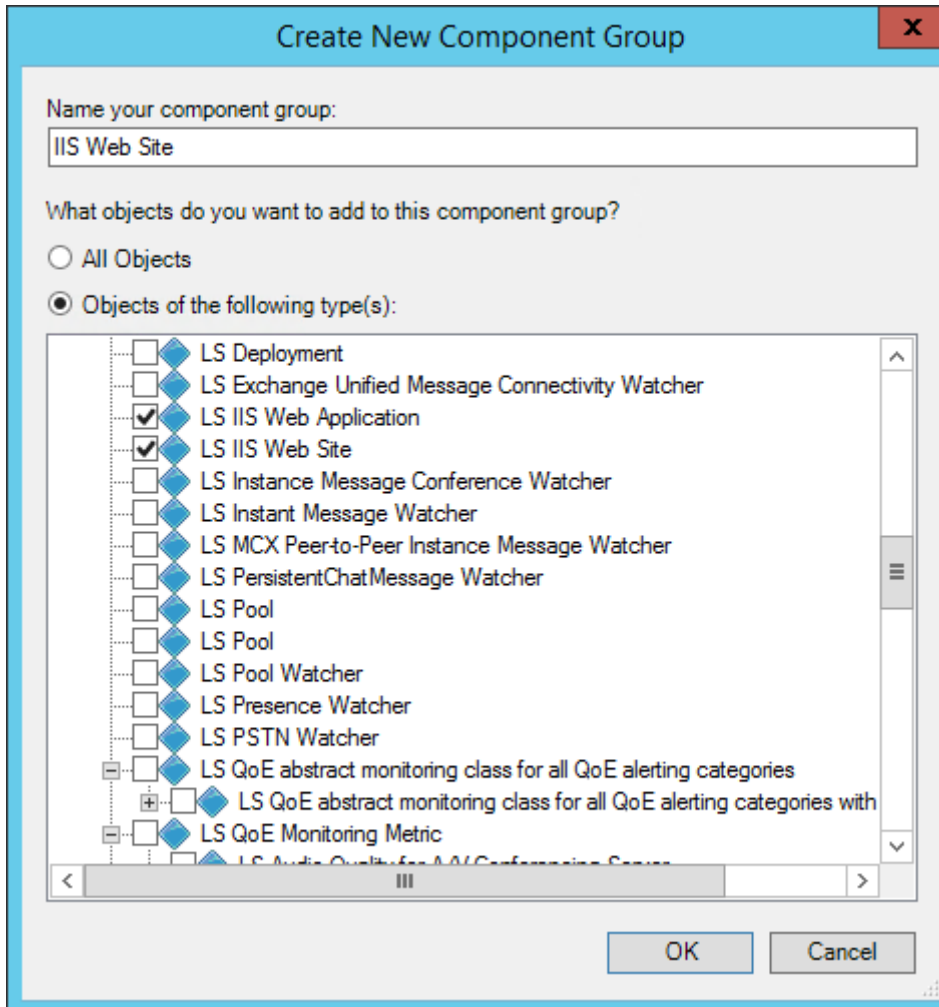
24. Click **OK.**

25. Select the **LS IIS Web Site** group in the lower left corner.

26. On the top toolbar, click the **Create Relationship** button.

27. Under **Service Manager Portal Web Application Web Sites** select **Default Web Site (SCSM01.contoso.com)** and move the dashed pointer to the newly created **IIS Web Site** object**. Click OK** and **de-select** the **Create Relationship** button**.**
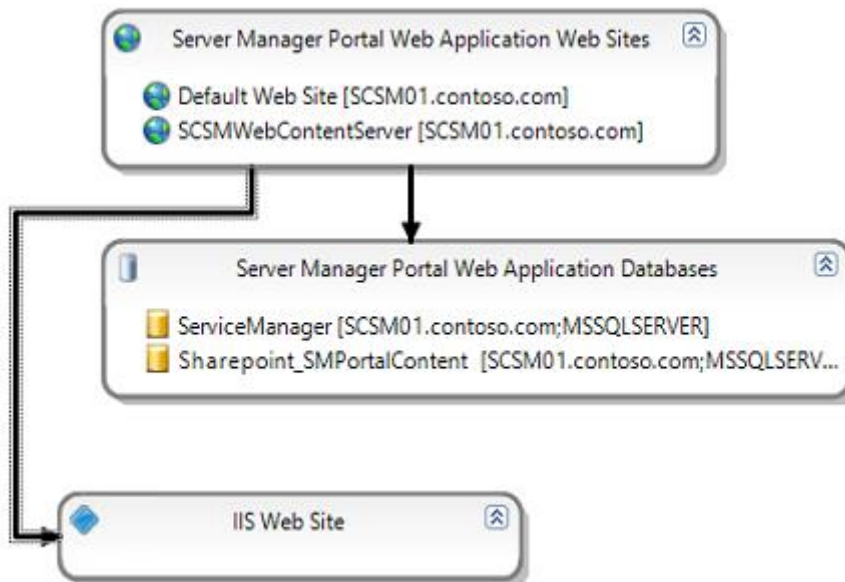
28. Click **Save**. This will take up to 10 minutes to save. You may open a second Operations Manager console if you wish to continue to other Operations Manager exercises. This exercise is effectively complete.

29. Click **Close**.

30. Navigate to the **Monitoring** workspace, then select the **Distributed Applications** view.

31. Andrew this just took me a couple of minutes to save so Corey's rig must be faster than yours: -)

5.4 - SCOM: Review Application Performance Monitoring

5.4.1 - SCOM: Install a Management Pack

In this exercise Application Performance Monitoring (APM) for a .NET web application will be configured to identify code bugs and performance issues. This website, Talking Heads, is a simulated social network which some purposely placed code bugs to trigger Operations Manager alerts.

Estimated time to complete: 5 minutes

Perform the following on SCOM01

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

2. Navigate to the **Administration** workspace**.**
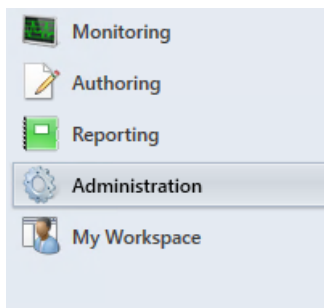
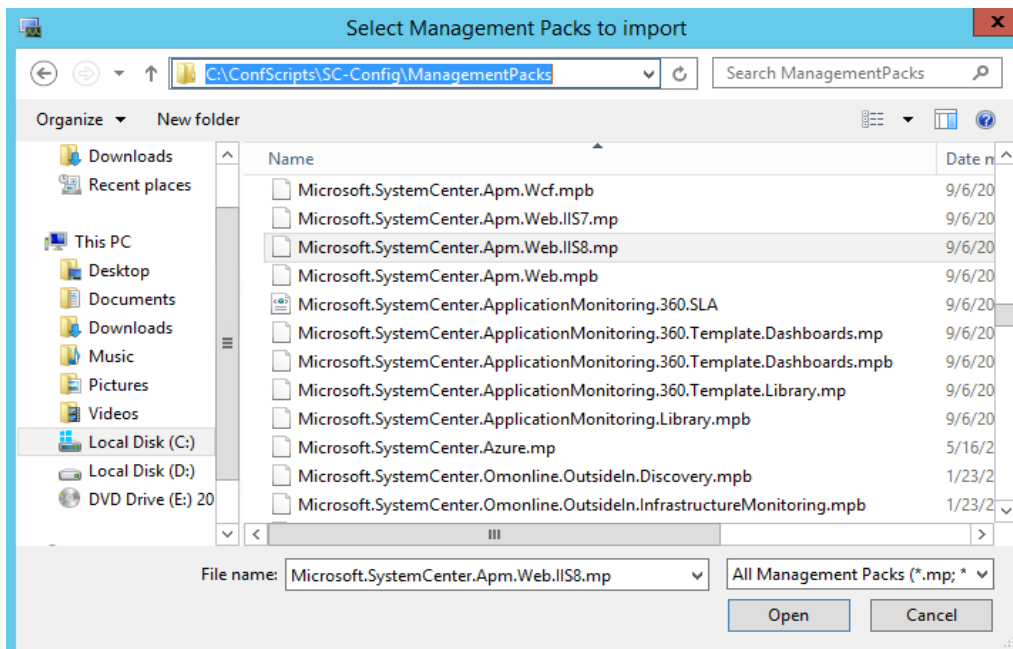3. Select **Management Packs**.

4. From the **Tasks** pane, select **Import Management Packs**.
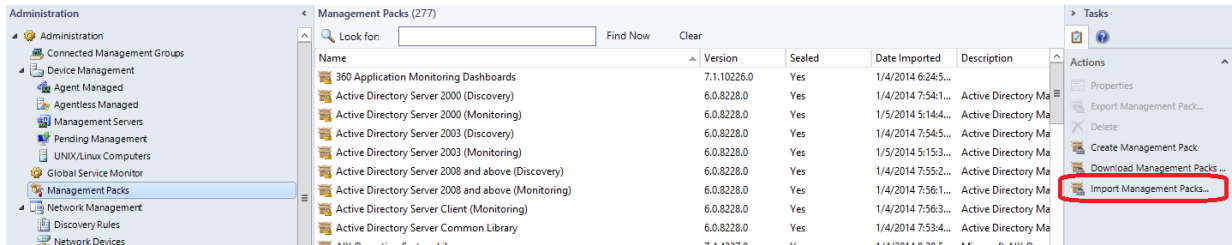
5. On the **Select Management Packs** screen, click **Add | Add from disk**.
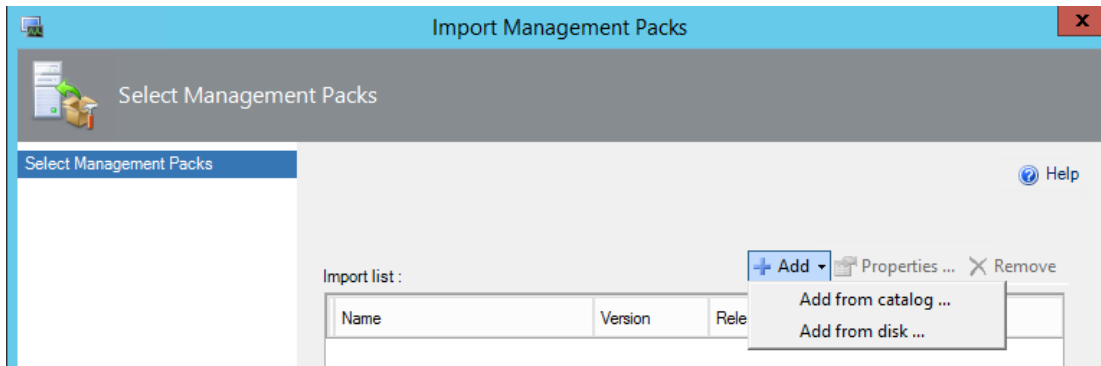
6. On the **Online Catalog Connection** prompt, click **No**.

7. On the **Select Manage Packs to import** prompt, navigate to **C:\ConfScripts\SC-Config\ManagementPacks**.

8. Select the files named **Microsoft.SystemCenter.Apm.Web.IIS7.mp** and **Microsoft.SystemCenter.Apm.Web.IIS8.mp,** then click **Open**.
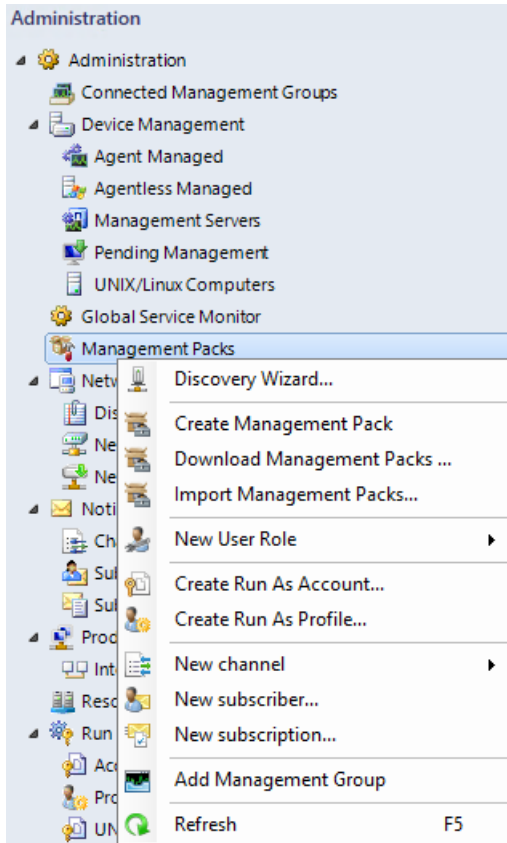
9. After returning to the Select Manage Packs page, click **Install**. This will take a minute to complete.
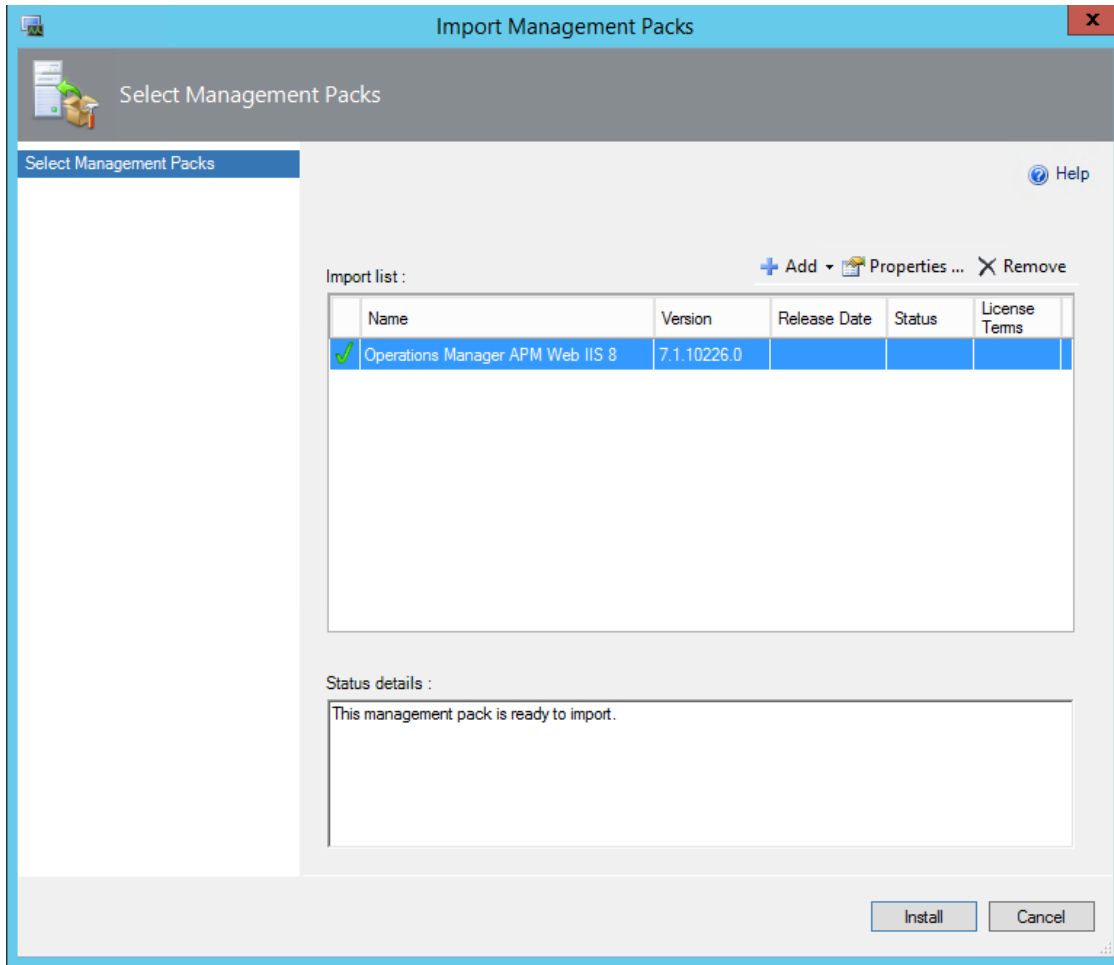
10. Click **Close**.

11. After returning to the Operations Manager Console, right-click Management Packs, and select **Refresh**.

12. Verify that there are **279** Management Packs and that the **Operations Manager APM Web IIS 7** and **Operations Manager APM Web IIS 8** Management Packs are available.
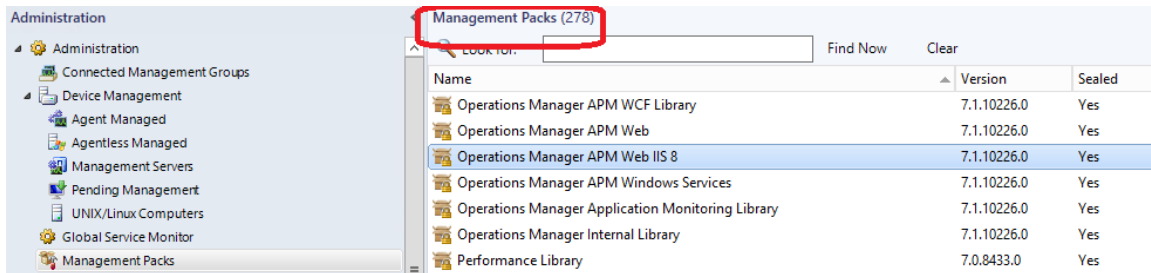
# 5.4.2 - SCOM: Configure Application Performance Monitoring

In this exercise Application Performance Monitoring (APM) will be configured for a .NET web application to identify code bugs and performance issues. This website, Talking Heads, is a simulated social network which some purposely placed code bugs to trigger Operations Manager alerts.

Estimated time to complete: 20 minutes

SCOM01

*Perform the following on **SCOM01***

1. From **SCOM01**, select **Internet Explorer** from the taskbar.

2. Select the tab for the T**alking Heads** website. If it does not open automatically, navigate to http://SCOM01.contoso.com/TalkingHeads.
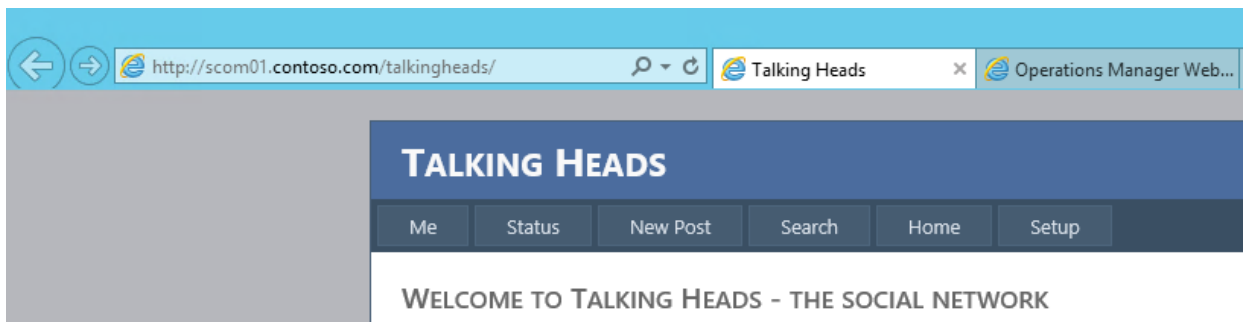
3. Click the **Home** tab to ensure that the .NET web application is running and the application is responsive. The webpage will refresh, but appear the same.
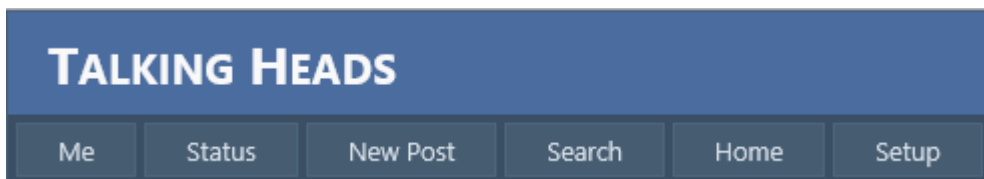

4. Open the **Operations Manager Console** by clicking the icon in the taskbar.

5. Navigate to the **Monitoring** workspace.

6. Expand the **Microsoft Windows Internet Information Services** folder.
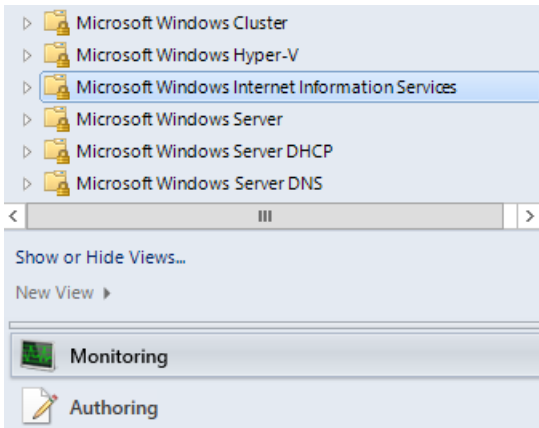
7. Click on the **Application Pool State** node and confirm that the **DefaultAppPool** on SCOM01 is listed in the results pane, which confirms that the application has been successfully discovered by the Management Pack.
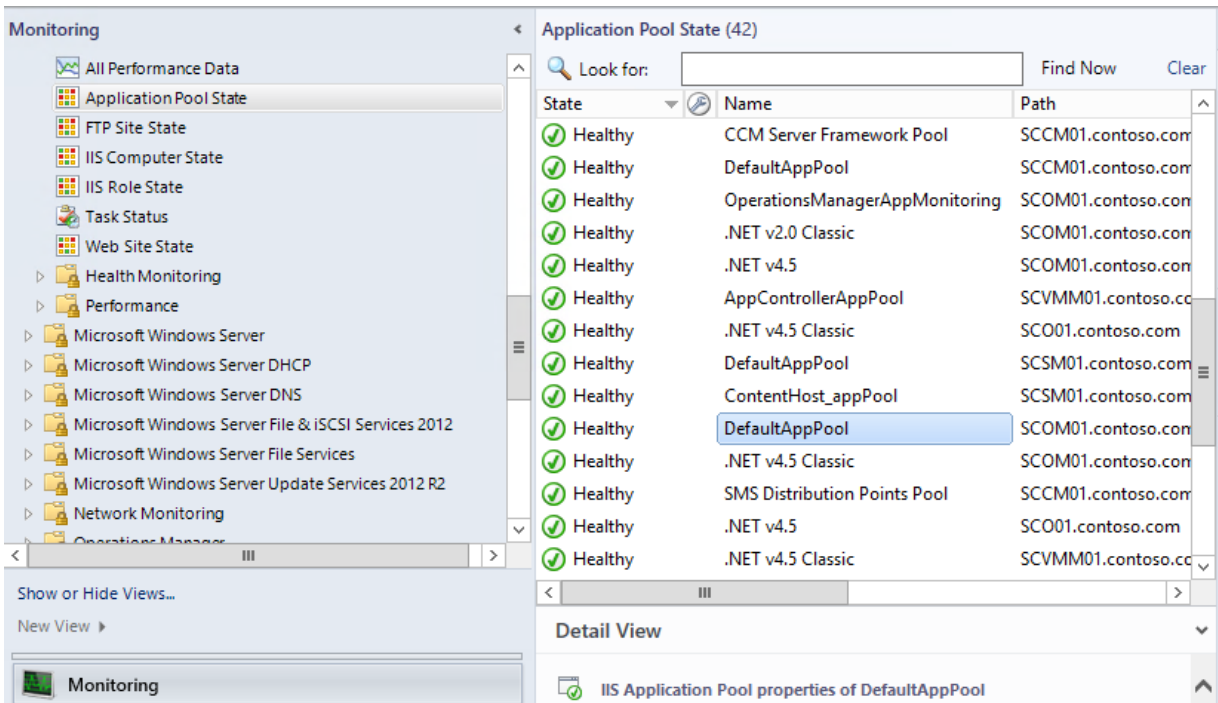

8. Select on the **Authoring** workspace.
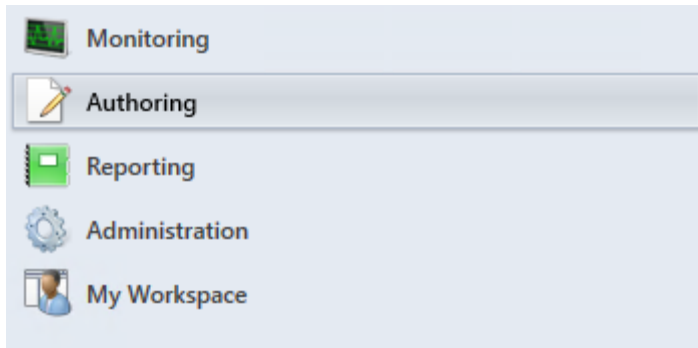
9. Right-click the **Groups** node and then click **Create a new Group**.
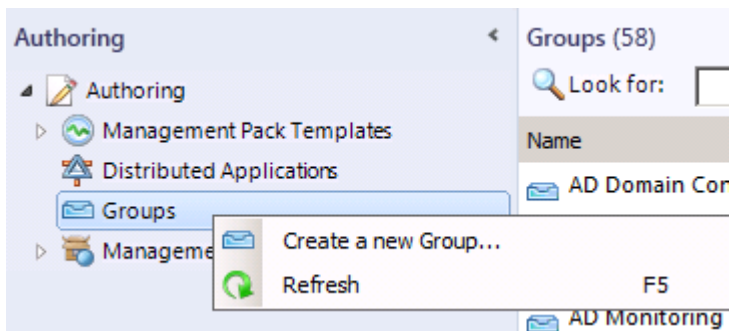
10. On the **Enter a name and description for the new group** page enter the name **TalkingHeads App Server Group**.

11. Under **Management Pack** click the **New...** button.

12. On the **General Properties** page for the new Management Pack, enter a name of **TalkingHeads Management Pack** in the **Name** field and click **Next**.
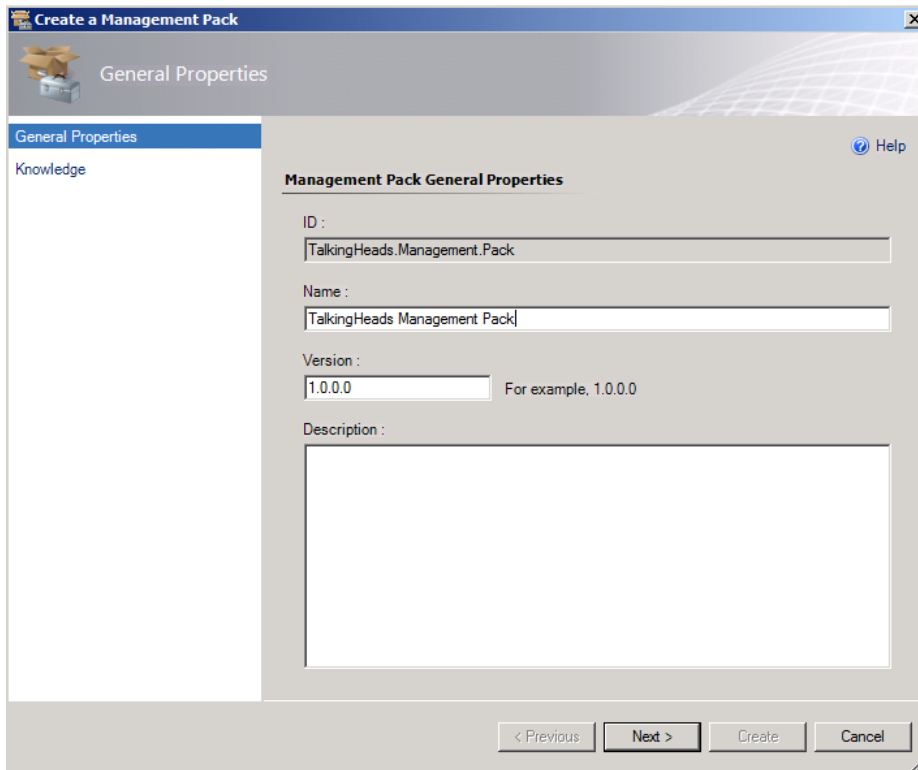
13. On the **Knowledge Article** page click **Create**. This may take a minute to complete.

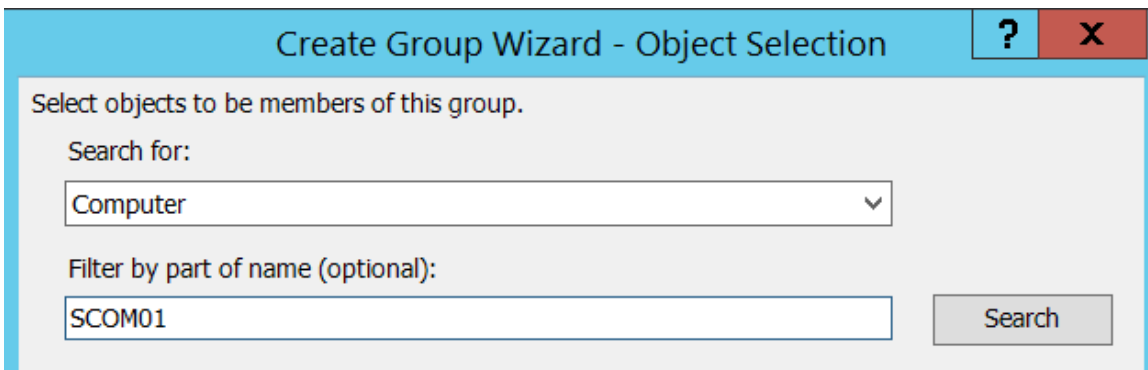14. From the **Create Group Wizard**, click **Next**.
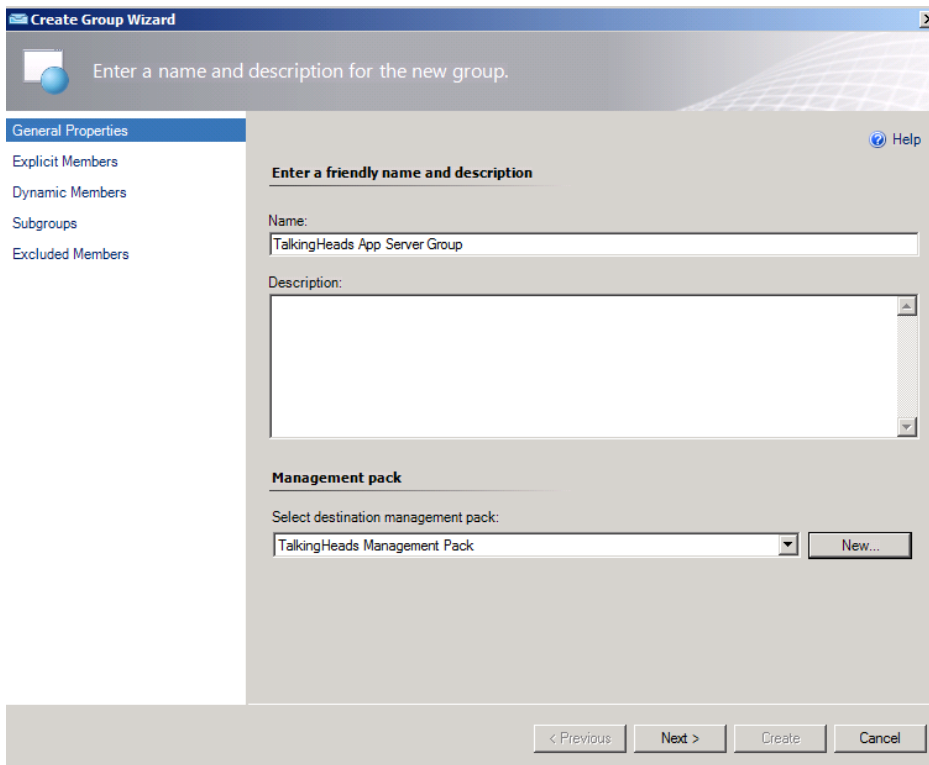
15. Click the **Add/Remove Objects…**button to select the servers to be monitored for this application.

Explicit Group Members (optional)

Choose specific objects that will be members of this group.

Add/Remove Objects

16. In the **Search for** dropdown menu select **Computer**.

17. Enter **SCOM01** in the **Filter by part of name** search box and click the **Search** button.
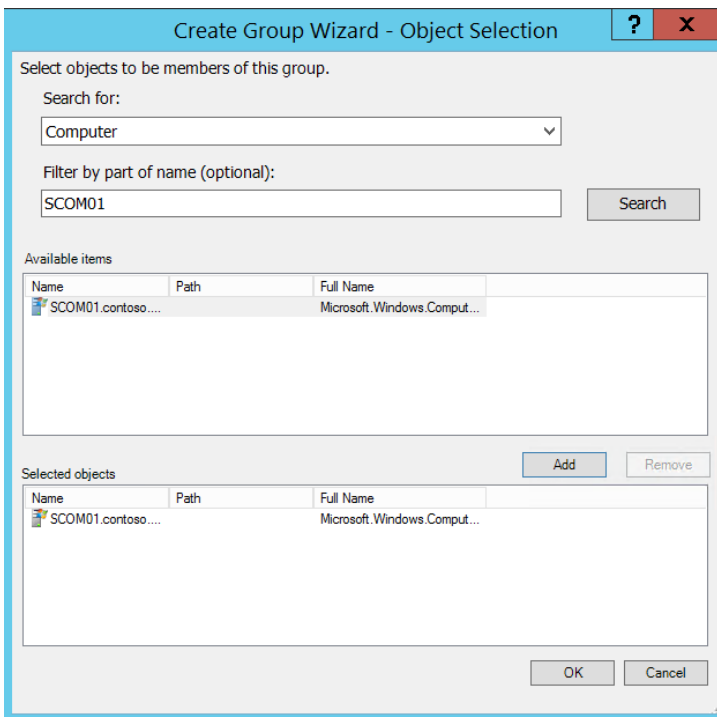
18. Under **Available Items s**elect the **SCOM01.contoso.com** entry.

19. Click the **Add** button and then click **OK** to return to the **Choose Members from a List** page.

20. Click **Next** on the **Choose Members from a List** page.

21. Click **Next** on the **Create a Membership Formula** page to skip dynamic membership rules.

22. Click **Next** on the **Choose Optional Subgroups** page.

23. Click **Create** to commit this new group and unsealed Management Pack to the database. This may take several minutes to complete. Wait until the wizard closes.

24. Using the **Operations Manager Console** click on the **Authoring** workspace and expand the **Management Pack Templates** node.
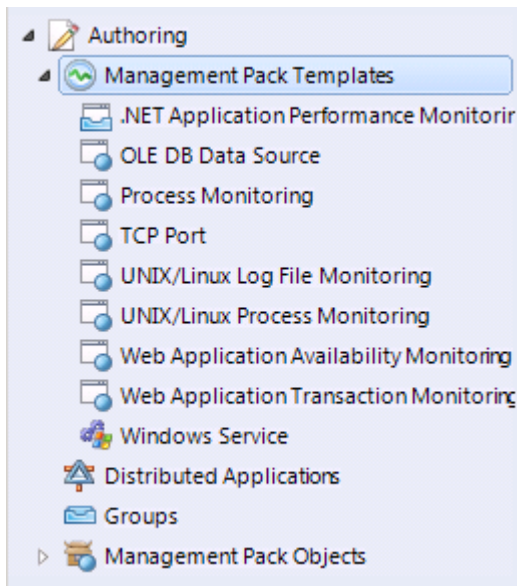

25. Click on the **.NET Application Performance Monitoring** node, then under **Tasks**, select **Add Monitoring Wizard**. To expand the toolbar click, on the **Task Pane**.
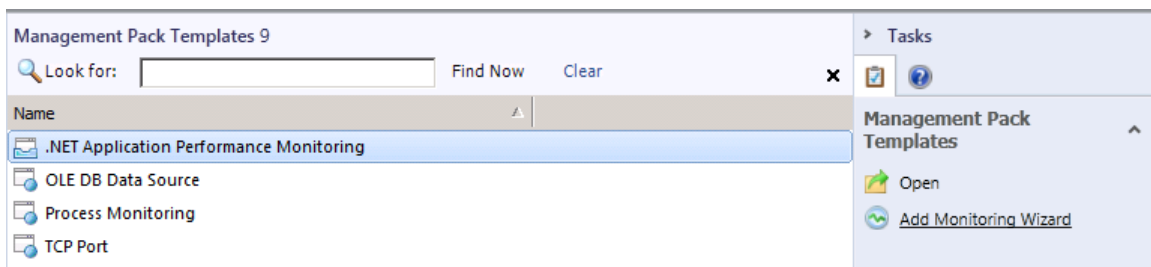
26. On the **Select Monitoring Type** page leave the **.NET Application Performance Monitoring** node selected and click **Next**.

Select the monitoring type

- .NET Application Performance Monitoring
- JEE Application Availability Monitoring
- JEE Application Performance Monitoring
- OLE DB Data Source
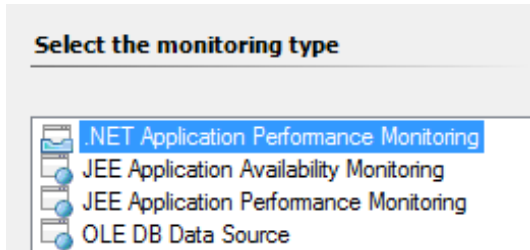
27. On the **General Properties** page type the name **TalkingHeads App Monitor** in the **Name** field.

28. Under **Management Pack** select the newly created **TalkingHeads Management Pack** from the dropdown list and click **Next**.

Enter a friendly name and description

Name:

TalkingHeads App Monitor

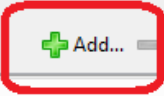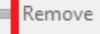Description:

Management pack

Select destination management pack:

TalkingHeads Management Pack | New...

29. On the **What to Monitor** window click the **Add…** button to locate the objects to monitor.

Add application components to monitor

Application group: TalkingHeads App Monitor

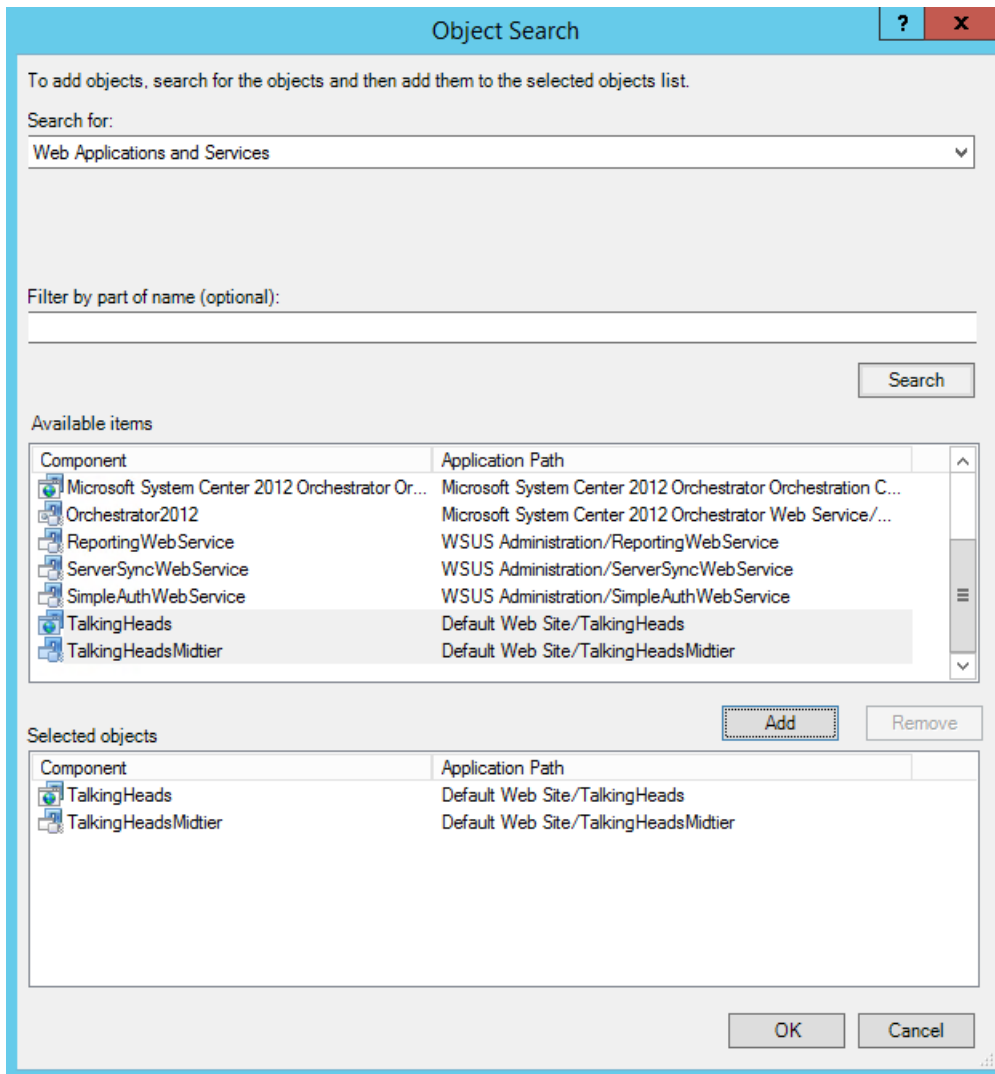Application components   Add... Remove

Component	Application Path

30. Click the **Search** button and then select the **TalkingHeads** application in the list of available items.
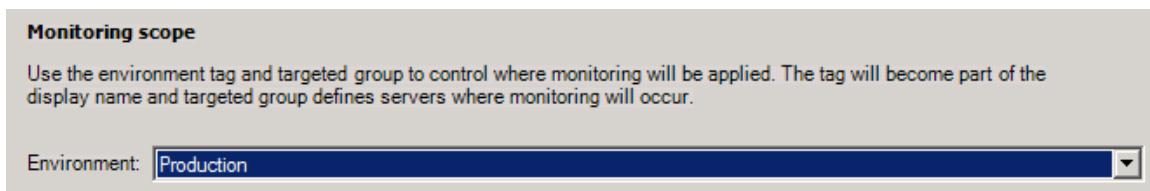

Filter by part of name (optional):

Search

31. Click the **Add** button to insert the **TalkingHeads** and **TalkingHeadsMidtier** to the **Selected objects** list and then click **OK**.

32. Under **Monitoring Scope** select **Production** from the **Environment** dropdown.

33. In the **Targeted group** section, click **Search**.

34. In the **Management pack** dropdown, select the **TalkingHeads Management Pack** and click **Search**.

35. Select the **TalkingHeads App Server Group** and click **OK**.

36. On the **What to Monitor** page, click **Next**.

37. On the **Server-Side Configuration** page, change the **Performance event threshold** to **3000** (ms) .

38. Click **Advanced Settings**.

Configure the default monitoring settings

Event monitoring

☑ Turn on performance event alerts
☑ Turn on exception events alerts

Configure performance event monitoring

Performance event threshold (ms):

3000

Use advanced settings to further customize the configuration for the application group

Advanced Settings...

☐ Enable additional configuration options for server-side and client-side monitoring

39. In the **Configure exception event monitoring** section, click **Application failure alerts** and **All exceptions**.

Configure exception event monitoring

☑ Security alerts   ○ Critical exceptions only   Exception Tracking ...
☑ Connectivity alerts   ◉ All exceptions   Critical Exceptions ...
☑ Application failure alerts

40. Click **OK**.

41. On the **Server-Side Configuration** page, click **Next**.

42. On the **Summary** page, click **Create** to set up this new Monitor object. This will take a few minutes to complete and the Wizard will disappear once it has finished.

Summary

Application Group:	TalkingHeads App Monitor - Production
Management Pack:	TalkingHeads Management Pack

Warnings:
⚠ IIS may need to be restarted.

Server-side monitoring defaults:

Monitored servers	TalkingHeads App Server Group
Performance event alerts	Enabled
Exception event alerts	Enabled
Performance event threshold	3000 ms
Monitors enabled	% Exception Events/sec exceeds threshold
	% Performance Events/sec exceeds threshold
	Average Request Time exceeds threshold

| Application Components:	2
TalkingHeads - Production	
Customized	False
Monitored servers	Server-side: TalkingHeads App Server Group
Client-side monitoring enabled	False
TalkingHeadsMidtier - Production	
Customized	False
Monitored servers	Server-side: TalkingHeads App Server Group

43. Open **Internet Information Services (IIS) Manager** by clicking Start and typing **IIS Manager** and clicking the shortcut.
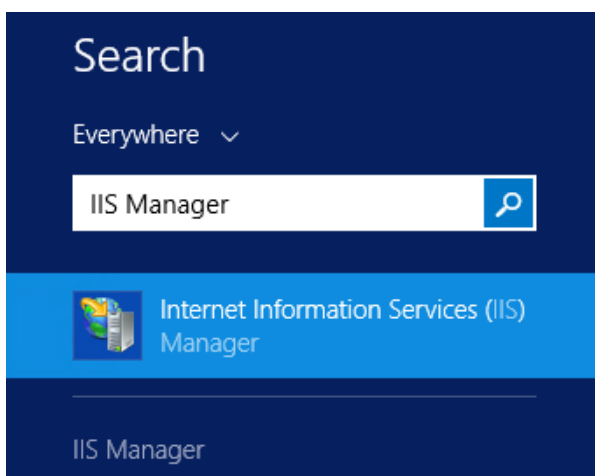
44. Under **Connections** in the left panel, select **SCOM01**. If prompted to get updates, click **No**.
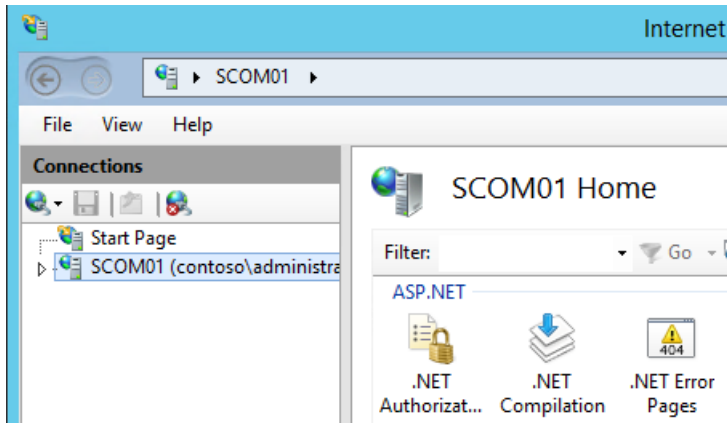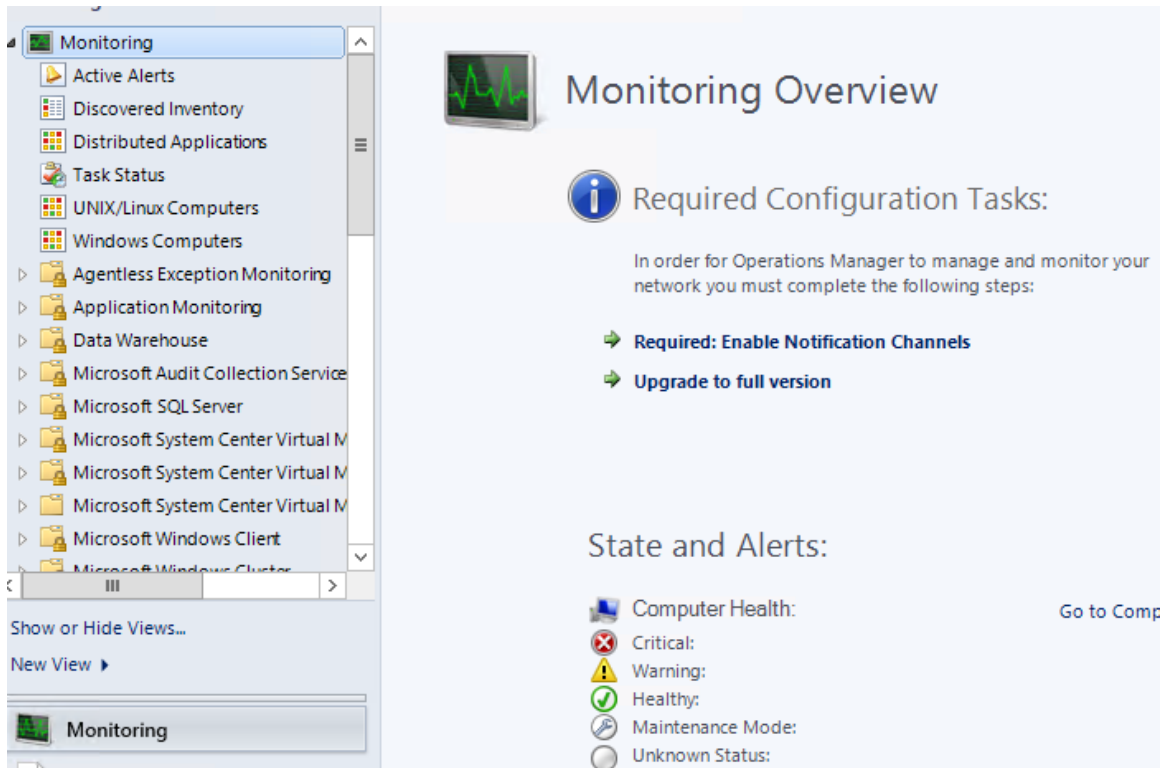
45. Under **Actions** in the right hand panel, click **Restart** to stop and then start the IIS Service.
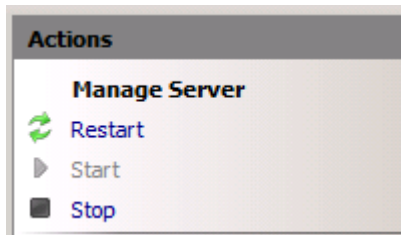
46. Close **Internet Information Services (IIS) Manager**.

47. Click the **Operations Manager** icon on the Taskbar and select **Monitoring** workspace on the Operations Manager Console.

48. Expand the **Application Monitoring |.NET Monitoring | TalkingHeads App Monitor - Production** node. If this is not visible, from the upper toolbar select **View | Refresh** until it appears. This may take awhile.
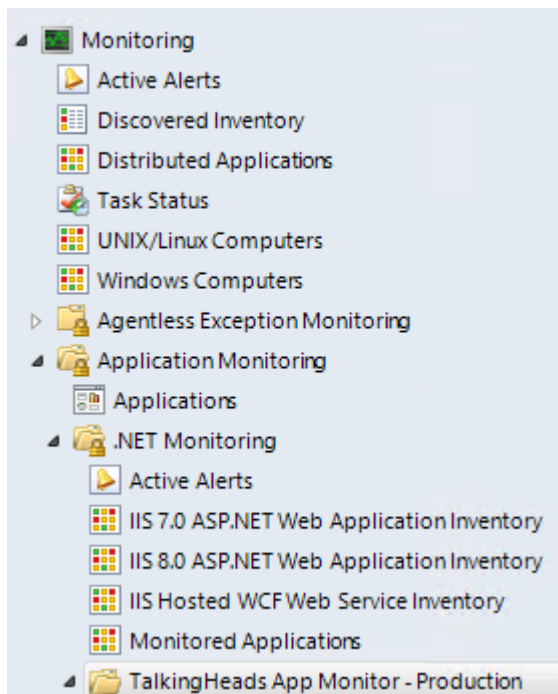
49. Click **TalkingHeads App Monitor** and confirm that the **APM ASP.NET Web Application Component** is in a healthy state, which is represented by a green 'check'. The application is now being monitored from the server-side. It may take several minutes to appear as **Healthy**. If this is not visible, from the upper toolbar select **View | Refresh** until it appears.

50. From the **Monitoring** workspace, expand the **Application Monitoring | .NET Monitoring | IIS 8.0 ASP.NET Web Application Inventory**.
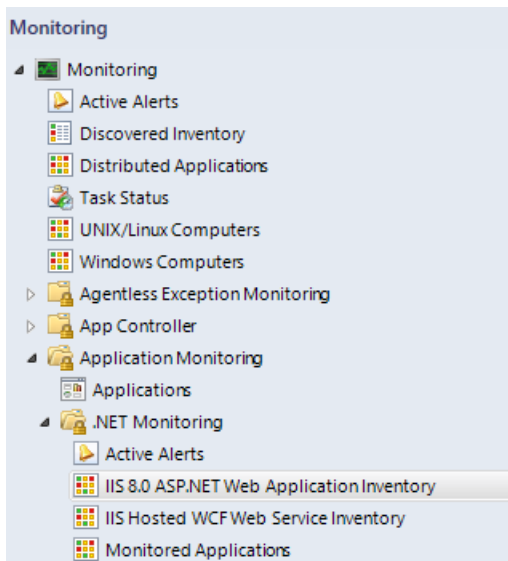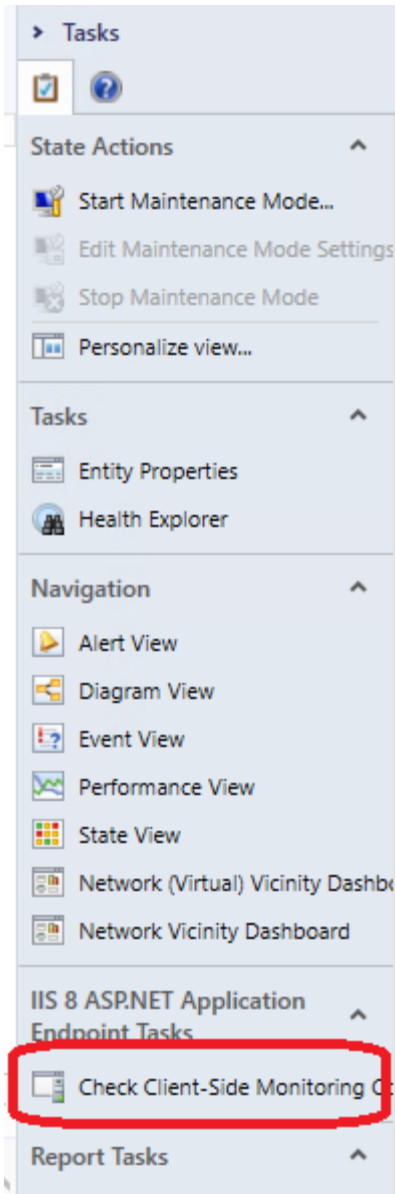

51. Click on the and confirm that the **Default Web Site/TalkingHeads** application is listed on **SCOM01**.

52. Click on the **Default Web Site/TalkingHeads** entry and then in the **Tasks** pane on the right, click **Check Client-Side Monitoring Compatibility**.

53. Click **Run** to initiate tests to confirm that the application can be monitored by injecting JavaScript code into the application.

Run Task - Check Client-Side Monitoring Compatibility

Help

Run the task on these targets

Target	Run Location
☑ Default Web Site/TalkingHeads	SCOM01.contoso.com;W3SVC/1

Task Parameters

Name	Value

Override

Task credentials

◉ Use the predefined Run As Account

○ Other :

    User name :

    Password :

    Domain : contoso

Task description

The task verifies that the web application can be safely monitored by using client-side monitoring. This task should be run against all ASP.NET applications that are to be configured for client-side monitoring through the .NET Application Performance Monitoring template.
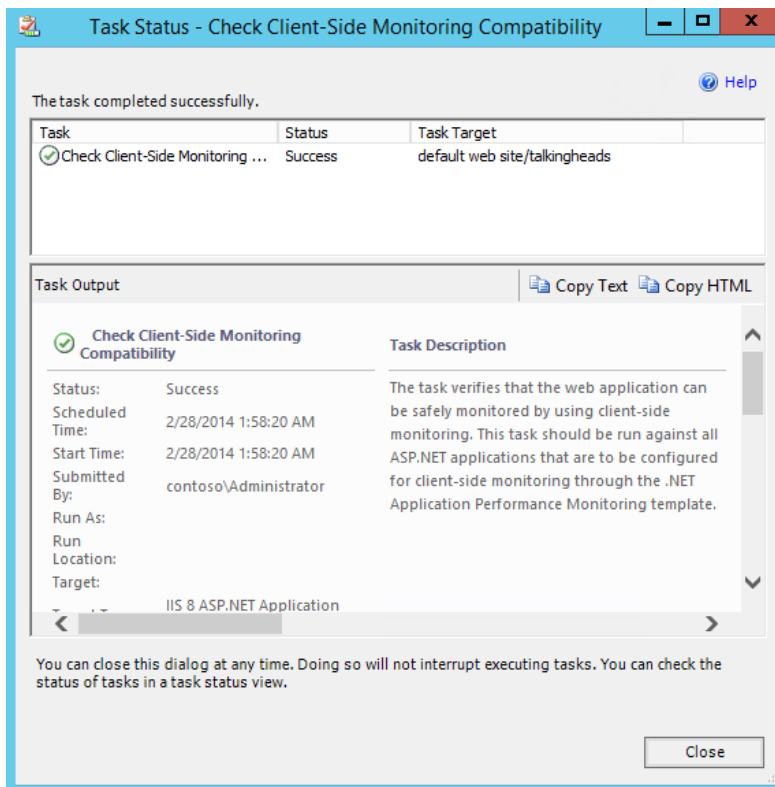
Task confirmation

☐ Don't prompt when running this task in the future
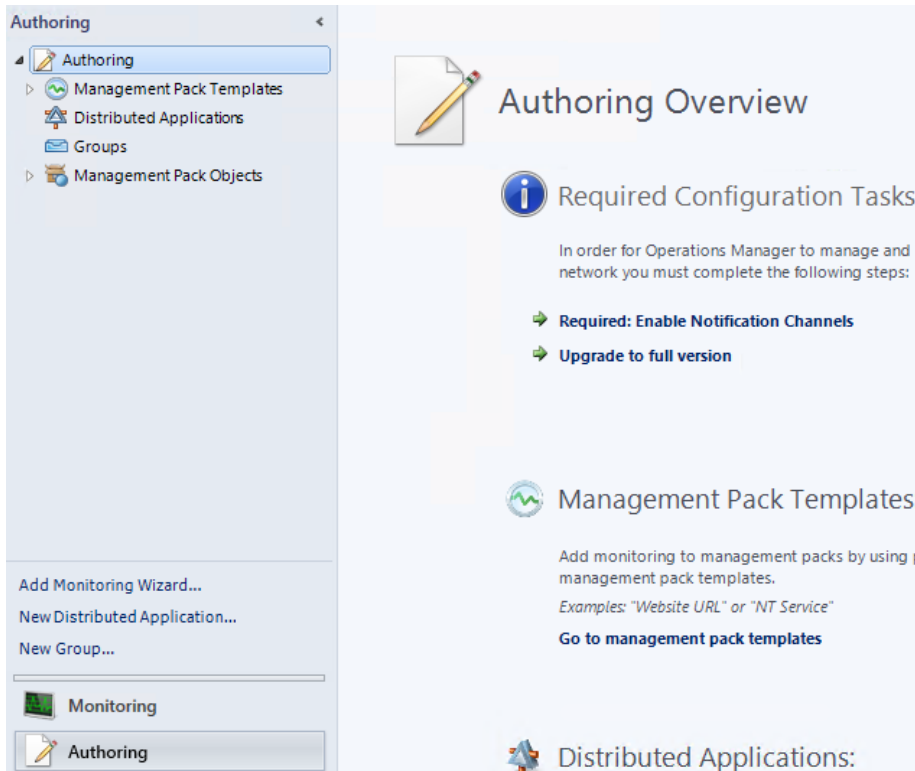
Run   Cancel

54. When the task completes, confirm that the **Status** reported is **Success** indicating that the application is compatible with Client Side Monitoring.
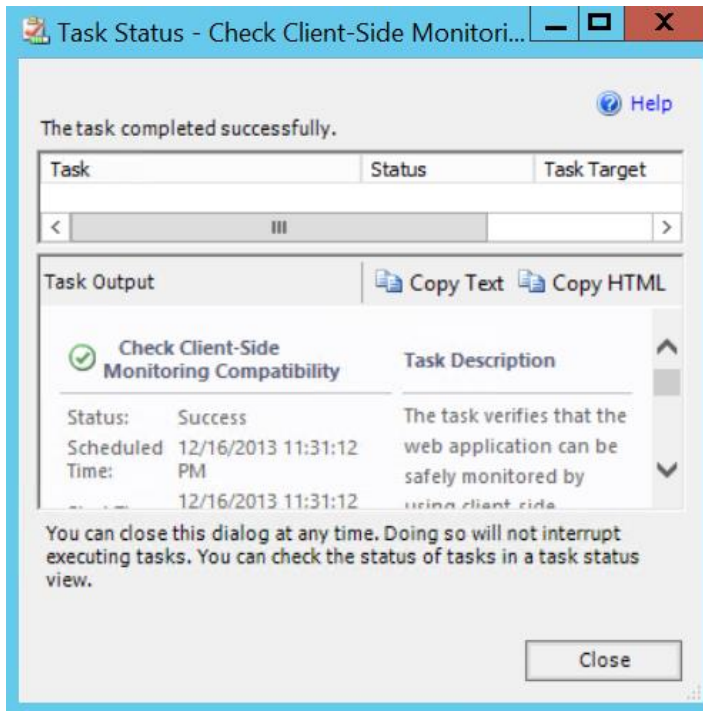
55. Click **Close** to clear the test window. Client-side Monitoring can now be safely configured for the TalkingHeads application.
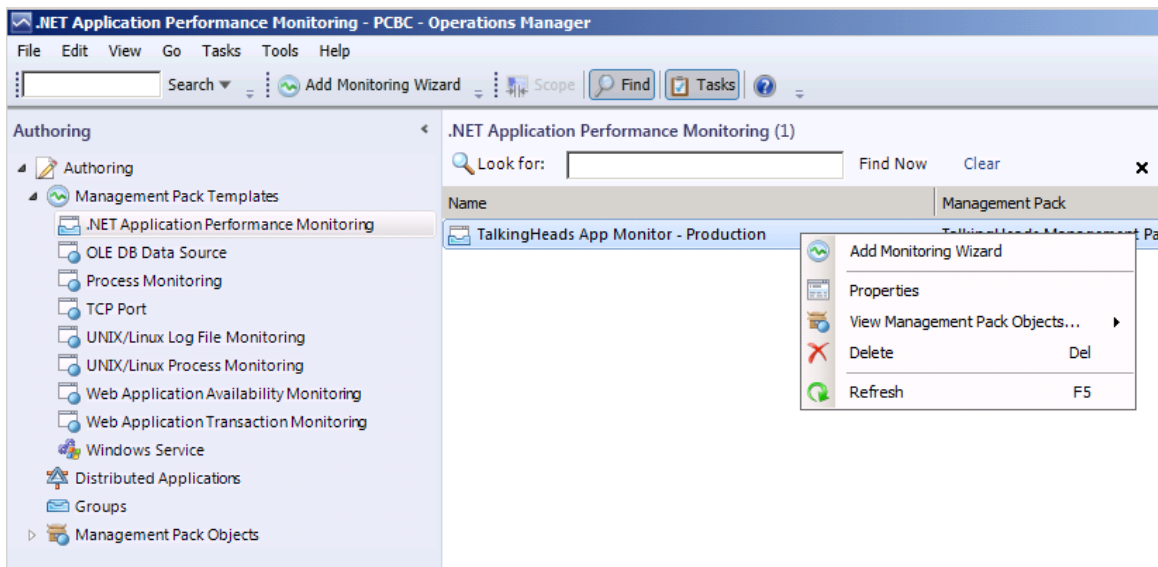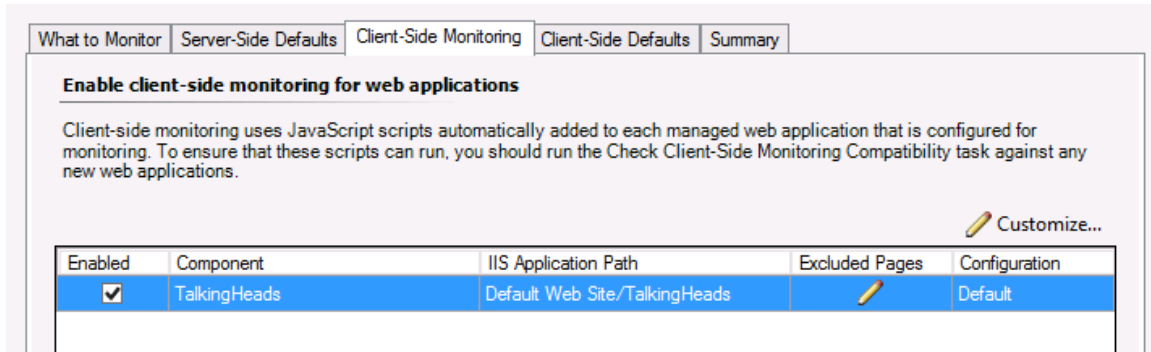
56. Select the **Authoring** workspace.

57. Expand **Management Pack Templates** and click **.NET Application Performance Monitoring**.

58. Right-click on the **TalkingHeads App Monitor -Production** monitor and select **Properties**.
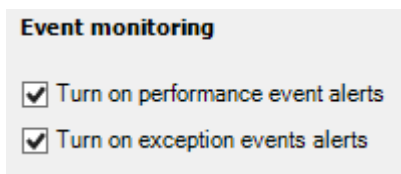

59. Click on the **Client-Side Monitoring** tab.

60. Click the **Enabled** checkbox to turn on CSM for this application.

61. Click the **Customize** button to open the settings window.

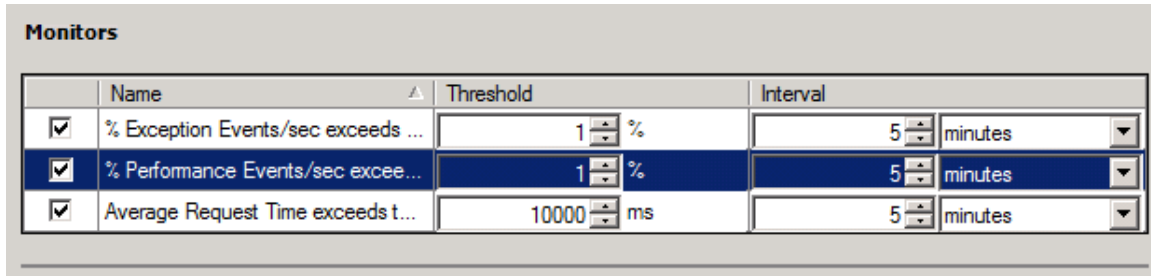62. Under Event monitoring check the box to enable **Turn on exception events alerts**.

63. Set the **Page load threshold (ms)** field to **3000**.

64. Set the **Ajax and WCF threshold (ms)** field to **3000**.

65. In the table titled **Configure the IP address filter** select each of the two lines in turn and use the **Remove** button to delete the lines from the table, leaving an empty table.
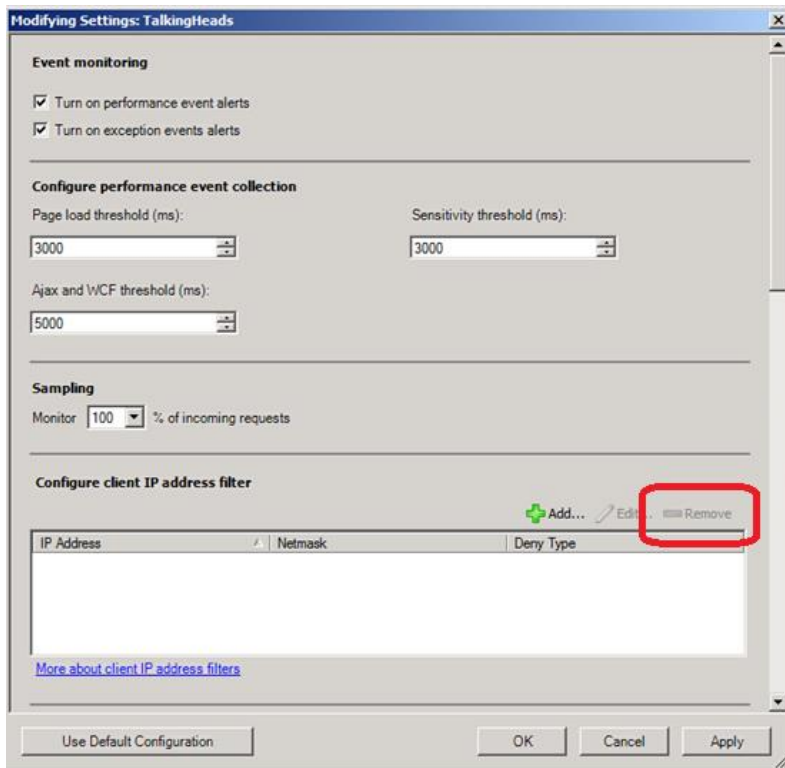
66. Scroll down to the **Monitors** area.

67. In the **% Exception Events/sec exceeds threshold** setting enter the value **1**. 1% is extremely low but will be useful to speed up the time to see alerts in this lab.

68. In the **% Performance Events/sec exceeds threshold** setting enter the value **1**.

69. Scroll further down to the **Transactions** section and click the **Add** button.

70. In the **Transaction Name** box enter **Home Page**.

71. In the **ASP.NET page** box enter **/TalkingHeads/Default.aspx**.

72. Under **Collect alerts by event type**, click to select the **Application failure** box.

73. In the **% Exception Events/sec exceeds threshold** setting enter the value **1**.

74. In the **% Performance Events/sec exceeds threshold** setting enter the value **1**.

75. Click **OK**.

76. Under **Monitored Servers** click **Search**.

77. In the Management Pack dropdown list select **TalkingHeads Management Pack** and press **Search**.

78. Select the **Talking Heads App Server Group** and then press **OK**.
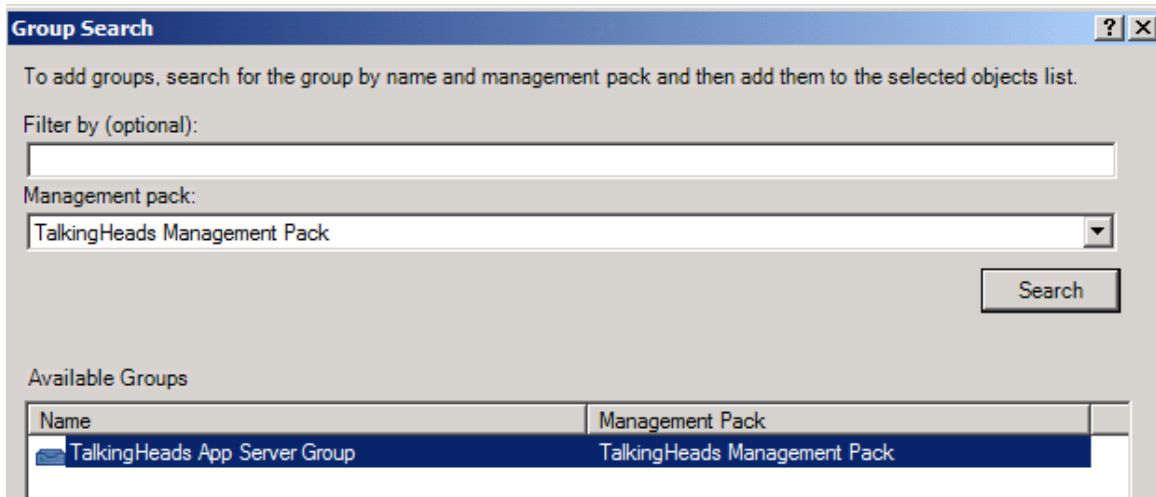
79. Press **OK** to close the **Modifying Settings: TalkingHeads** page.
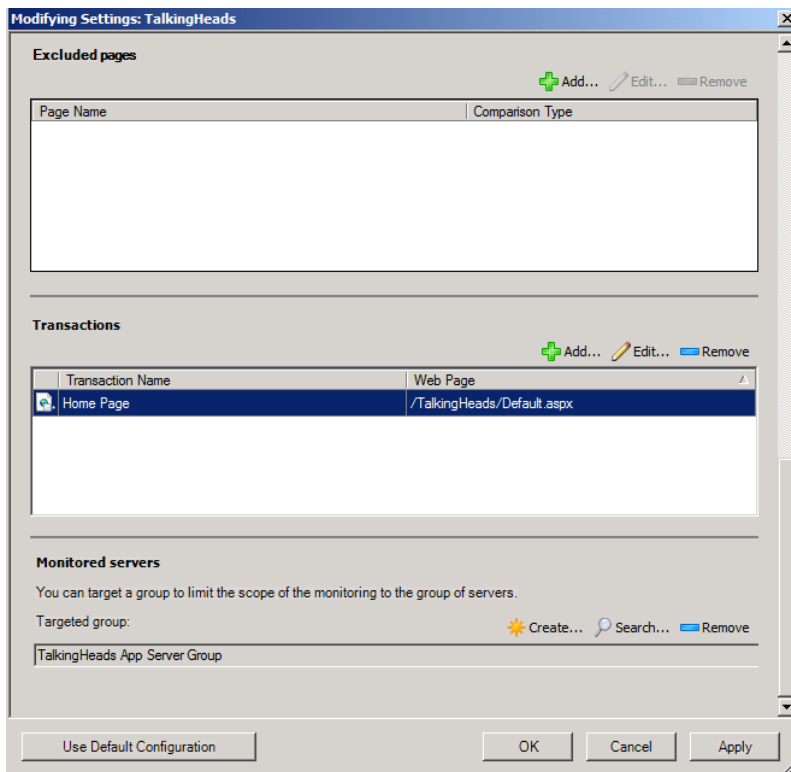
80. Click on the **Client-Side Defaults** tab.

81. Under **Event monitoring** check the box to enable **Turn on exception events alerts**.

82. Set the **Page load threshold (ms)** field to **250**.

83. In the table titled **Configure the IP address filter** select each of the two lines in turn and use the **Remove** button to delete the lines from the table, leaving an empty table.
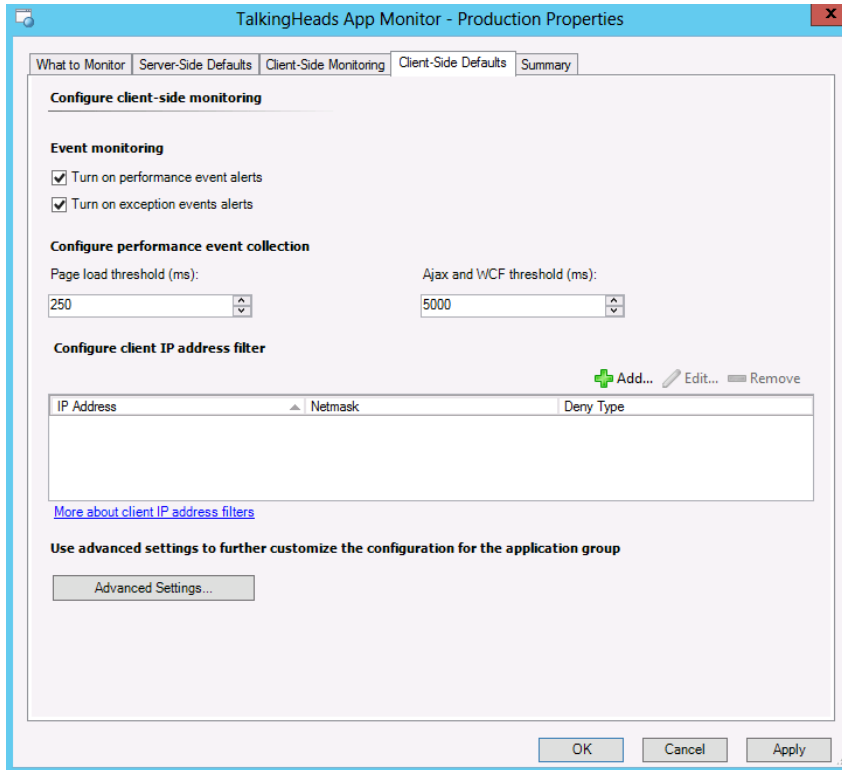
84. Click **OK** to close the **TalkingHeads App Monitor Production - Properties** dialog box. The folder will update, and this may take a few moments to complete. The properties page will disappear once it has completed.

85. Navigate to **Monitoring | Operations Manager | APM Agent Details | Active Alerts**.
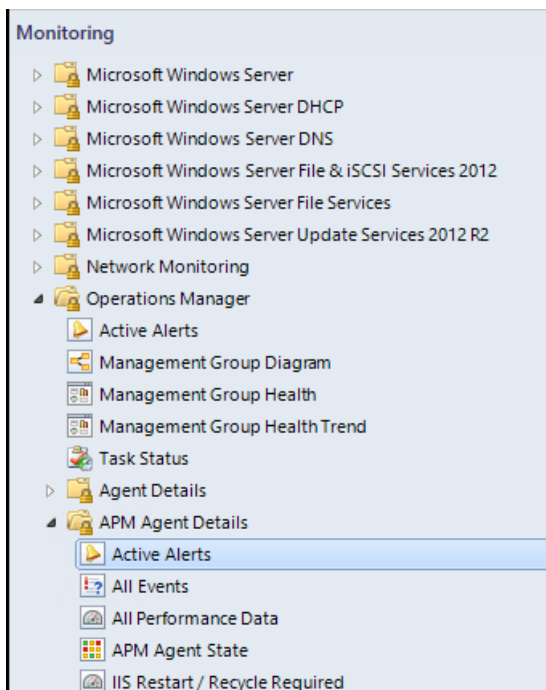
86. In the Active Alerts pane, wait until a Warning alert appears indicating that Application Pools require a recycle on DC01, or right-click on Active Alerts and select Refresh. When the Alert appears, select the **IIS Restart** is required alert.

⊿ **Severity: Warning (2)**
⚠ DC01.Contoso....   IIS Application Pools recycle is required   New
⚠ DC01.Contoso....   IIS Restart is required   New

87. In the details pane below, scroll down and click the **Restart IIS** link.

Alert Details   ⌄

running on the web server. This monitor transitions to an unhealthy state when IIS needs to be recycled.

Causes

When application monitoring settings are modified using the .NET Application Performance Monitoring template, IIS might need to be restarted for the new settings to take effect. An example of a scenario that requires restarting IIS is when you are configuring .NET application monitoring for the first application on the web server.

Resolutions

• You can restart IIS by clicking the following link: Restart IIS

• You can run the iisreset.exe command on the web server.

88. Ensure SCOM01**.Contoso.com** is selected and click **Run**.

89. When the Task completes, click **Close**.

90. Navigate to **Monitoring | Operations Manager | APM Agent Details** and click the **All Events** node.

91. Sort the Events by Event Number.

92. Notice E**vent 4001** in the list, this event indicates that the APM service has started.

93. On **SCOM01**, select **Internet Explorer** from the taskbar so that the Talking Heads website opens. If it does not, navigate to http://scom01.contoso.com/TalkingHeads.
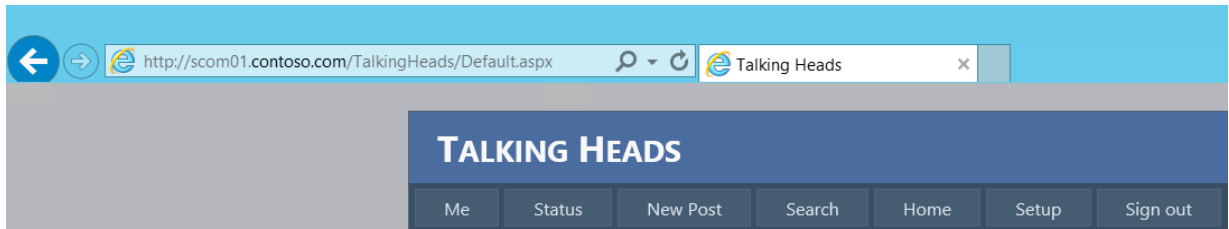
94. Click the **Home** tab to ensure that the webpage refreshes, which indicates that the IIS server restarted correctly.

95. **Minimize** Internet Explorer.

96. On the Desktop, double-click the **TalkingHeads** folder.
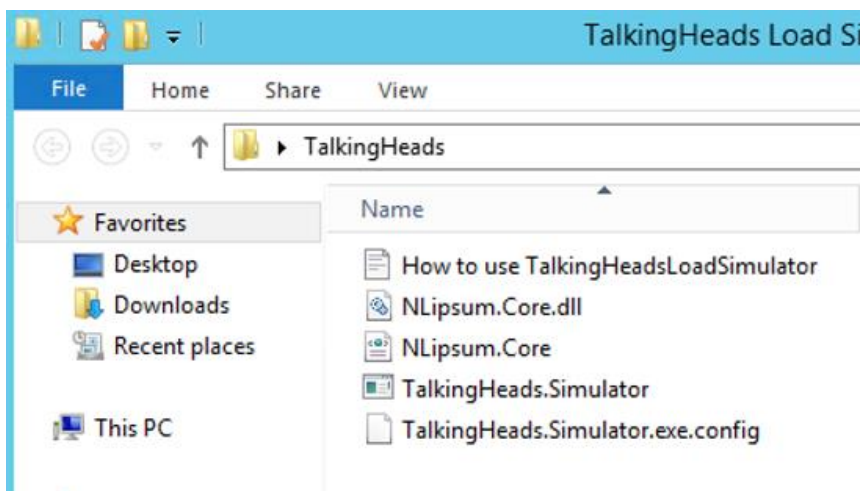
97. Double-click on **TalkingHeads.Simulator**, an executable application. If a publisher verification warning appears, click **Run** to continue.

98. Next to the **Scenario** button, click the dropdown and select **Default Scenario**.
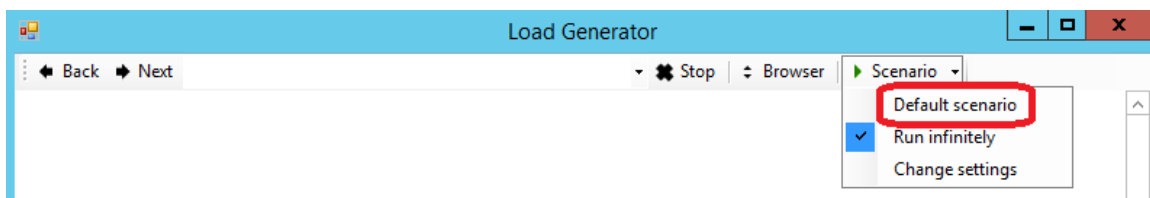
99. Once tests appear in the lower window, minimize the **Load Generator**. This runs scripts against the preconfigured bugs in the website to create application exceptions and performance issues on both the server and client side. Application Performance Monitoring will detect these issues and collect data which can be sent to a developer for debugging.

100. Open the Operations Manager Console click on the **Monitoring** workspace, and select **Operations Manager | APM Agent Details | All Events**.

101. Wait for Event **4003** to appear. When it does, click to select it and notice that the **APM Agent** started successfully in the details pane.

Log Name:	Operations Manager	Apm Agent started successfully.
Source:	Apm Agent	

102. Expand the **Application Monitoring | .NET Monitoring | TalkingHeads App Monitor – Production | TalkingHeads App Monitor** node. Note that the **Client Side Monitoring Application Component** is now active. It may take a few minutes for the current state of the Client-side Monitoring to appear, but when it does it will show as **Healthy**.
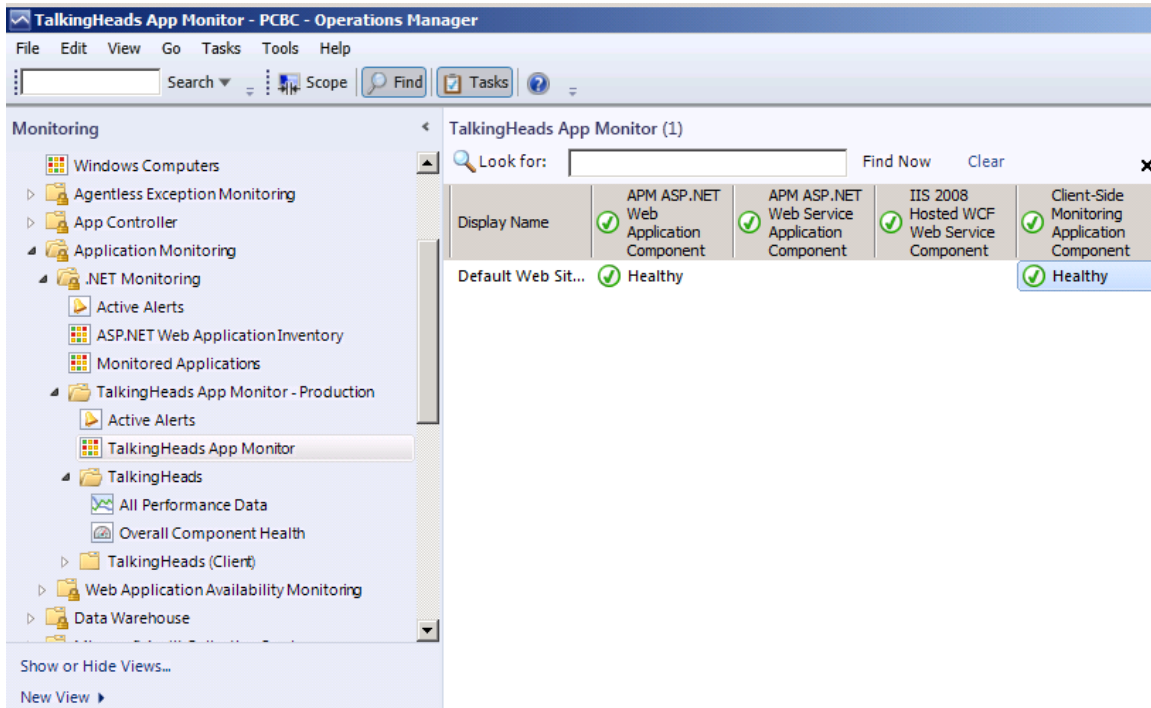
103. Navigate to the **Application Monitoring | .NET Monitoring | TalkingHeads App Monitor – Production | Active Alerts** node. After a few moments exceptions and performance alerts will begin to appear which confirms that APM was configured correctly.
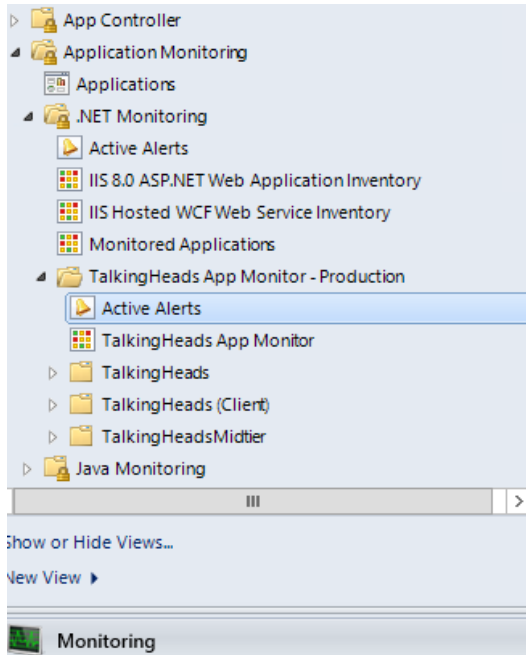
104. Wait until there is at least 1 alert in each of the following categories. This should take a few moments.

105. Client Application Exception

106. Client Performance Exception

107. Client Performance Exception

108. Server Performance Exception

109. Server Application Exception

110. Minimize **Operations Manager** and select the **Load Generator**.

111. Select **Stop**.
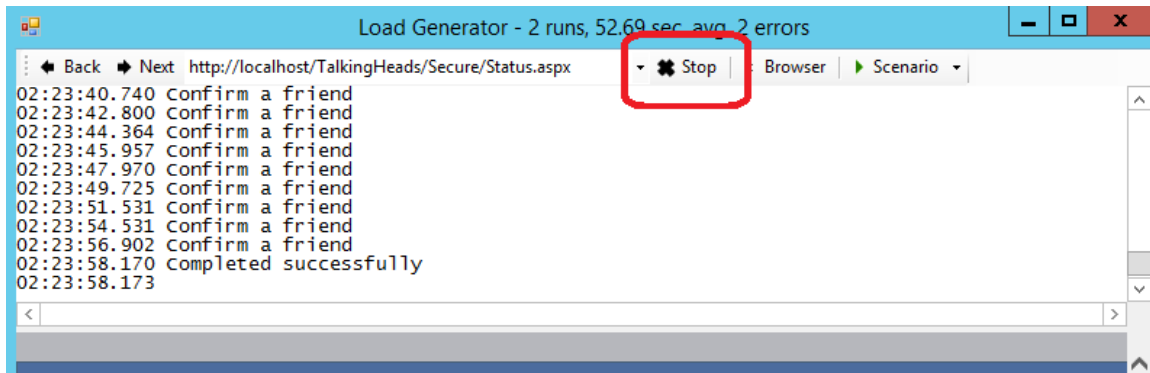
112. Close the **Load Generator**.

5.4.3 - SCOM: View Application Performance Monitoring Data

In this exercise Application Performance Monitoring (APM) information for a .NET web application will be reviewed. This can be used to identify code bugs and performance issues, which assists with application troubleshooting. This website, Talking Heads, is a simulated social network which some purposely placed code bugs to trigger Operations Manager alerts.

Estimated time to complete: 15 minutes

SCOM01

*Perform the following on **SCOM01***

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

2. Navigate to the **Monitoring** workspace.
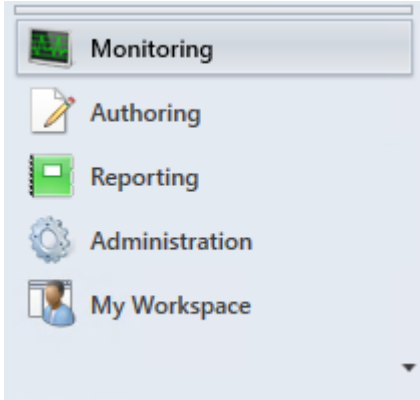
3. Expand **Monitoring** | **Application Monitoring | .NET Monitoring.**
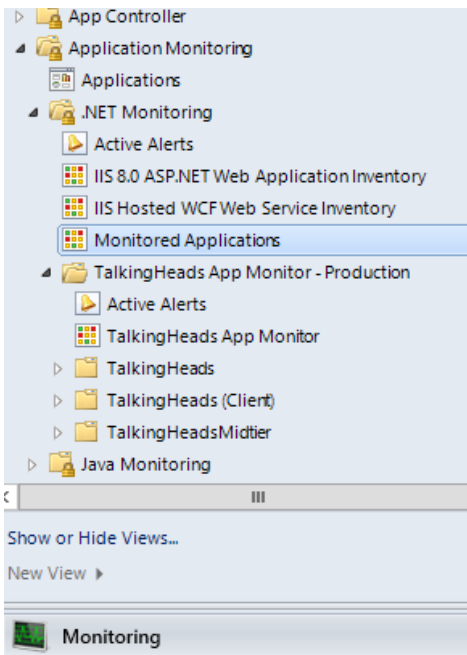
4. Select **Monitored Applications** and ensure that the state of the **TalkingHeads App Monitor - Production** is Healthy.
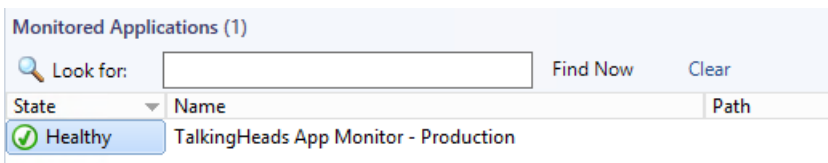
5. Navigate to the **Monitoring | Application Monitoring | .NET Monitoring | TalkingHeads App Monitor - Production | TalkingHeads**.
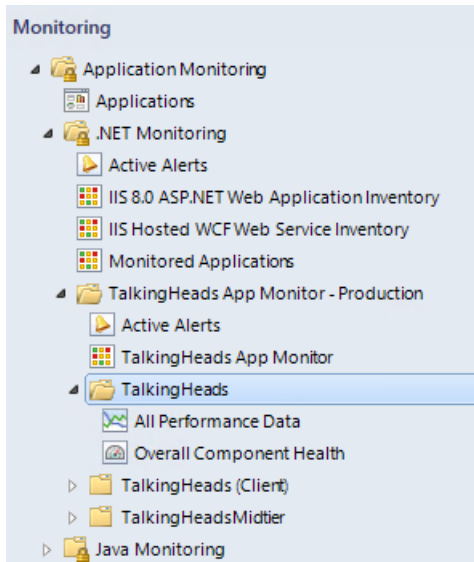
6. Select **Overall Component Health**. Note that the application is healthy, however there are several performance alerts.

7. Navigate to the **Monitoring | Application Monitoring | .NET Monitoring | TalkingHeads App Monitor - Production | Active Alerts**.

8. Find an alert with the name **Server Application Exception**.

9. Right-click it and select **Properties**. This error indicates that an application running on the server has had an issue.

10. Under **Alert Description**, click the **link** to launch Internet Explorer.

Alert Description:

'TalkingHeads - Production' on SCOM01.contoso.com has had an application failure occur. An exception of type 'System.ServiceModel.FaultException' with a message of 'System.ServiceModel.FaultException' was thrown in '/TalkingHeads/Secure/Post.aspx'. For additional details please use the following link:
http://SCOM01/AppDiagnostics/Pages/login.aspx?m=ev&uid=7d427a7c-78a5-43ab-acae-0117f254ffa1

11. When the Windows Internet Explorer Dialog appears, select **Yes** to close the window.

12. **Expand** the various components of the event by clicking the plus signs (+) and triangles and review the information. The information on this page can be used to reproduce the issue and provide information about how to resolve this error.

13. Select the **Similar events** tab at the top of the page. These are identical events that have happened in recent history.

14. Select the **Related events** tab at the top of the page. This displays events that are similar, but may not be identical to this particular failure.

15. Select the **Performance counters** tab. Toggle some of the values to see additional information which is collected about this performance issue.
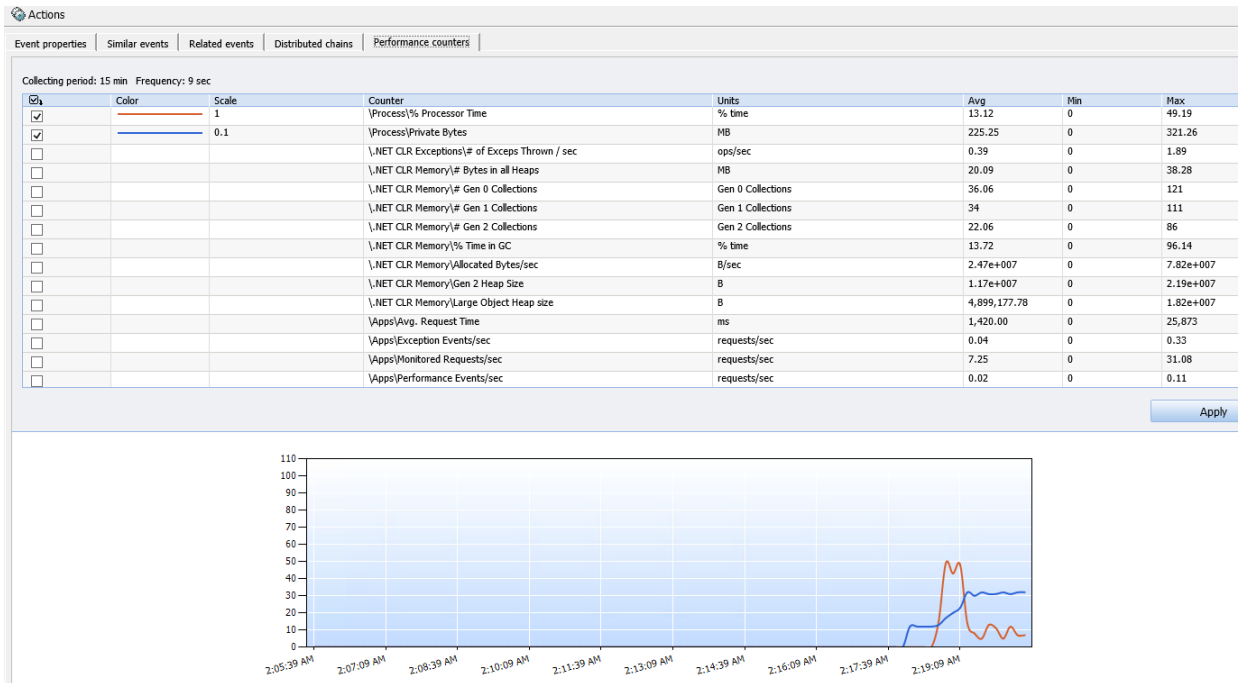
16. **Close** Internet Explorer.

17. After returning to the Alert Properties, under the section labeled **TFS Work Item Owner** select **Change**.

18. On the Select User dialog enter **Administrator** and select **Check Names**. Click **OK**.

19. Under **Alert Status**, click the dropdown and select **Scheduled**.

20. Click **OK** to close the Alert Properties.

21. After returning to the Active Alerts node, select a **Server Performance Exception** alert.

22. **Right-click** it and select **Properties**. This error indicates that an application running on the server has had a performance issue when a process exceeded its expected duration.

23. Under **Alert Description**, click the **link** to launch Internet Explorer.

Alert Description:

'/TalkingHeads/Secure/Search.aspx' has exceeded the configured threshold 3000 ms on: SCOM01.contoso.com. For additional details please use the following link: http://SCOM01/AppDiagnostics/Pages/login.aspx?m=ev&uid=5310623b-0b8c-0000-b809-000001527a9d

24. When the Windows Internet Explorer Dialog appears, select **Yes** to close the window.

25. **Expand** the various components of the event by clicking the plus signs (+) and triangles and review the information.
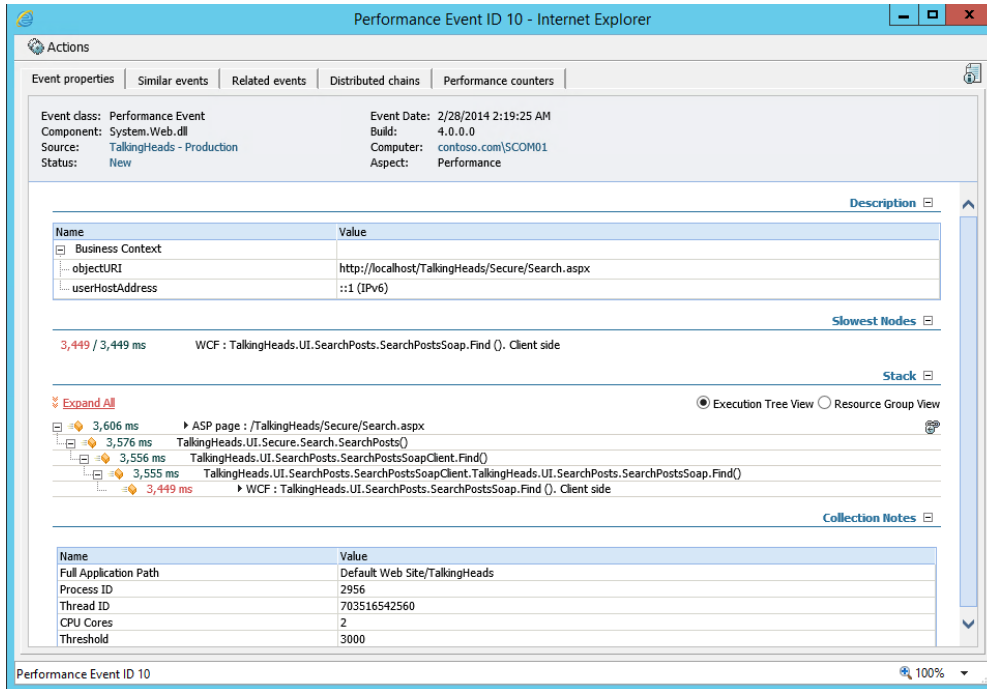
26. **Close** Internet Explorer.

27. After returning to the Alert Properties page, under **Alert Status** select **Closed** and click **OK**.

28. After returning to the Active Alerts node, select a **Client Application Exception** alert.

29. **Right-click** it and select **Properties**. This error indicates that a client received an error while using the application.

30. Under **Alert Description**, click the **link** to launch Internet Explorer.

Alert Description:

/TalkingHeads/Secure/Status.aspx failed with Web Page Client Side Exception has been detected in application TalkingHeads - Production on SCOM01.contoso.com. For additional details please use the following link:
http://SCOM01/AppDiagnostics/Pages/login.aspx?m=ev&uid=5DB036BA-DAD0-4D2B-B81E-0B4CF5B13FED

31. When the Windows Internet Explorer Dialog appears, select **Yes** to close the window.

32. **Expand** the various components of the event by clicking the plus signs (+) and triangles and review the information.
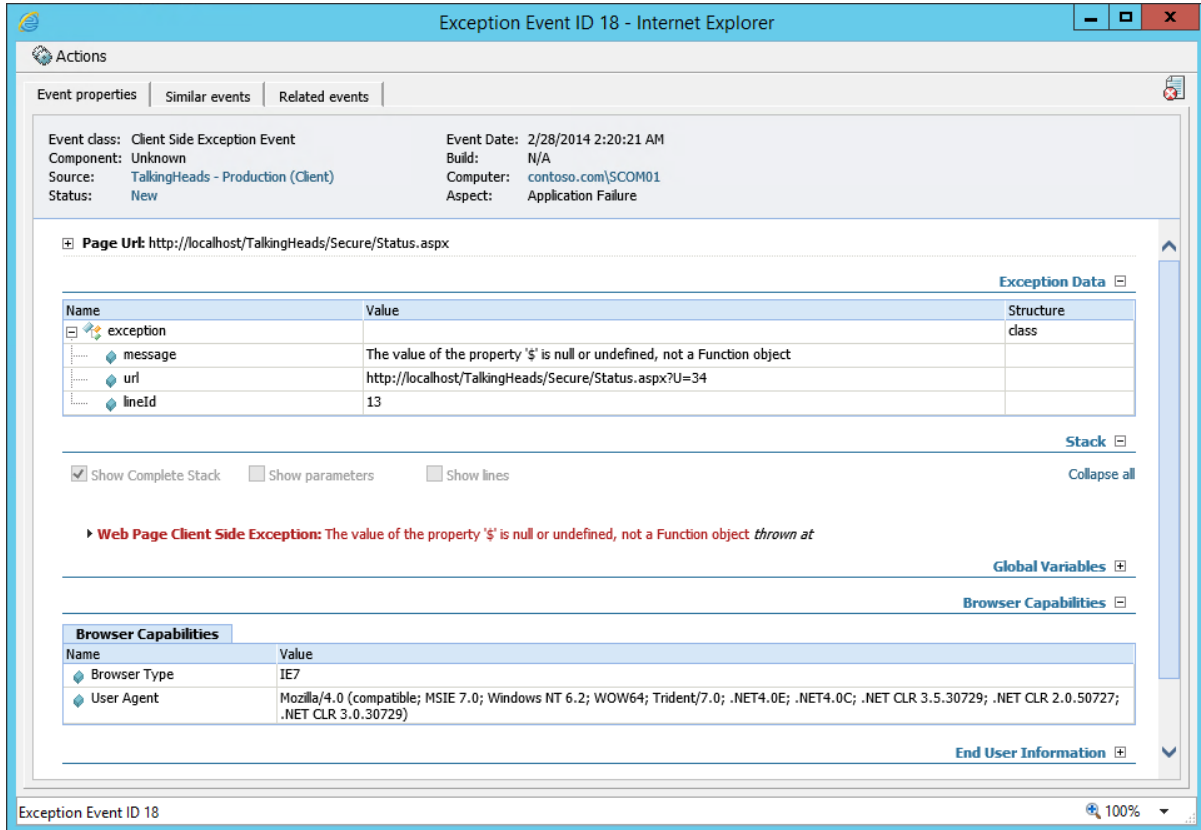
33. Under **Page Url**, note the exact URL which generated the exception event.

34. Under **Browser Capabilities** note the browser type and various user agents that were used when the event was generated. This can be used to reproduce and troubleshoot the event.
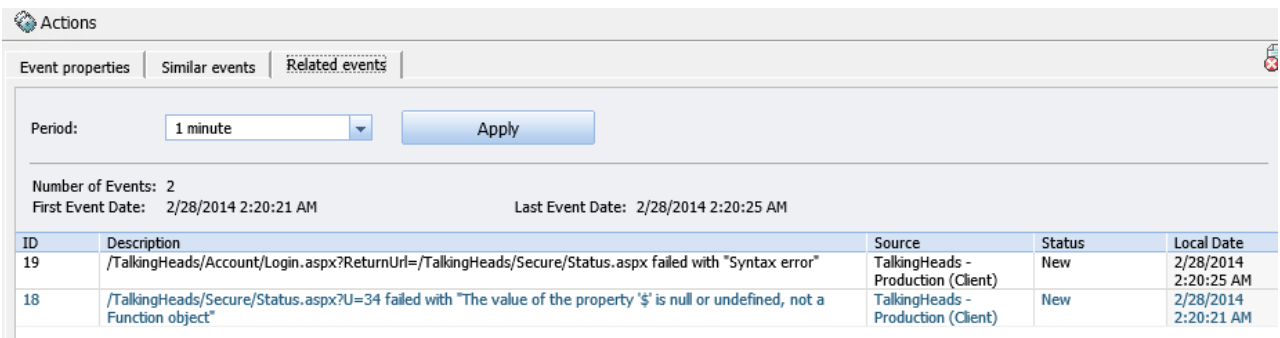
Browser Capabilities	
Name	**Value**
◆ Browser Type	IE7
◆ User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)

35. Select the **Similar events** tab at the top of the page, these are identical events that have happened in recent history.

⚙ Actions

| Event properties | Similar events | Related events |

Similar by:	🔍 Problem ▾
Problem:	/TalkingHeads/Secure/Status.aspx failed with Web Page Client Side Excep...
From:	2/14/2014 2:20:21 ▣ To: 2/28/2014 2:20:21 ▣ [Apply]

Number of Events: 2
First Event Date: 2/28/2014 2:19:50 AM   Last Event Date: 2/28/2014 2:20:21 AM

ID	Description	Source	Computer	Status	Local Date
18	/TalkingHeads/Secure/Status.aspx?U=34 failed with "The value of the property '$' is null or undefined, not a Function object"	TalkingHeads - Production (Client)	SCOM01	New	2/28/2014 2:20:21 AM
14	/TalkingHeads/Secure/Status.aspx failed with "The value of the property '$' is null or undefined, not a Function object"	TalkingHeads - Production (Client)	SCOM01	New	2/28/2014 2:19:50 AM

36. Select the R**elated events** tab at the top of the page, this displays events that are similar but may not be identical to this particular failure.

⚙ Actions

| Event properties | Similar events | Related events |

| Period: | 1 minute ▾   [Apply] |

Number of Events: 2
First Event Date: 2/28/2014 2:20:21 AM   Last Event Date: 2/28/2014 2:20:25 AM

ID	Description	Source	Status	Local Date
19	/TalkingHeads/Account/Login.aspx?ReturnUrl=/TalkingHeads/Secure/Status.aspx failed with "Syntax error"	TalkingHeads - Production (Client)	New	2/28/2014 2:20:25 AM
18	/TalkingHeads/Secure/Status.aspx?U=34 failed with "The value of the property '$' is null or undefined, not a Function object"	TalkingHeads - Production (Client)	New	2/28/2014 2:20:21 AM

37. **Close** Internet Explorer.

38. After returning to the Alert Properties, under the section labeled **TFS Work Item Owner**, select **Change**.

TFS Work Item ID:

TFS Work Item Owner:

| Owner: | [   ]   [Change...] |
| Ticket ID: | [   ] |

39. On the Select User dialog enter **Developer** and select **Check Names**. Click **OK**.

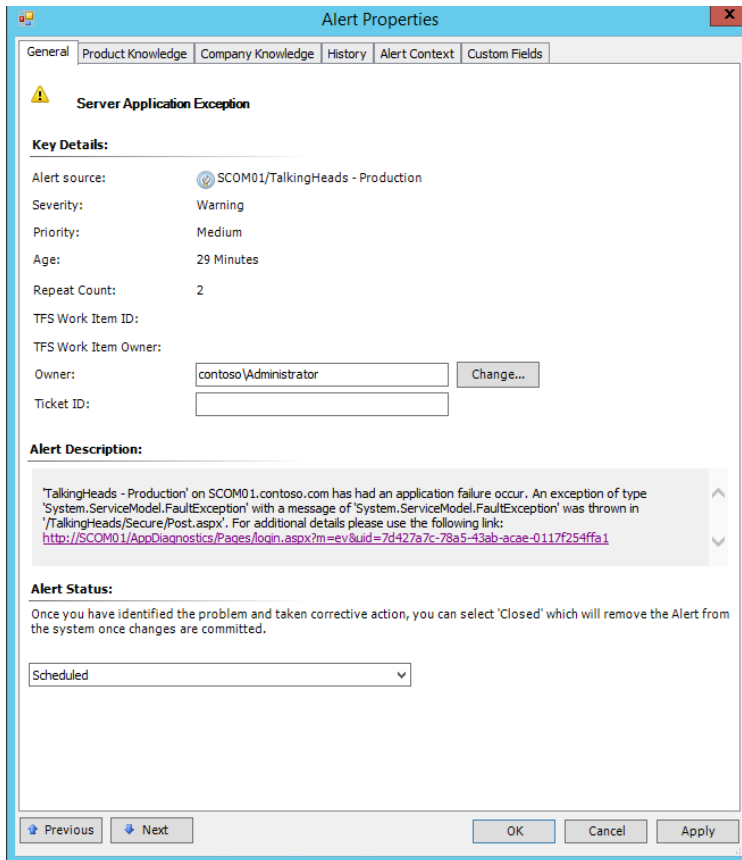40. Under **Alert Status**, click the dropdown and select **Assigned to Engineering** and click **OK**. Operations Manage can be connected to Team Foundation Server (TFS) so that any issues which are assigned to developers will appear in their bug database with all the relevant data which can be used to help resolve the issue.

41. After returning to the Active Alerts node, select a **Client Performance Exception** alert.

42. **Right-click** it and select **Properties**. This error indicates that a client received an error while loading a webpage.

43. Select the **Product Knowledge** tab. Review the information.

Alert Properties

General | **Product Knowledge** | Company Knowledge | History | Alert Context | Custom Fields

Summary

The object state is changed to unhealthy when the total number of client-side performance events for a configured transaction exceeds the monitor threshold.

Causes

Client-side performance alerts are generated when the page load time for the web application exceeds the configured threshold. The total timing is measured at the web browser, is correlated to server processing time, and then is separated into the following categories that are available in the event details:

When the page load time exceeds the threshold:

- Network request and response time
- Page redirects
- Server response time
- Document Object Model (DOM) loading time
- Peripheral loading – the amount of time that is spent loading page external resources, such as images and scripts
- Running time for Window.OnLoad() client-side event handlers

When the response time for AJAX calls exceed the threshold:

- Network request and response time
- Server response time
- JavaScript execution

Significant amount of time spent in one or a few categories might point to the root cause of the performance problem. For example, the time spent processing network requests and responses might suggest slow network connectivity. Long server response time might be caused by slowly-running server code, and can be further troubleshoot by investigating associated server-side performance alerts. Slow DOM loading might be linked to excessive complexity or size of the application page, or might also point to slow performance of the client browser. Long run times for the Window.OnLoad() event or slow AJAX JavaScript indicate inefficient code on the page or might be due to slow performance of client browser. A large number of page redirects might result from complex or inefficient application code.

Resolutions

Client-side performance alerts are generated when the run time exceeds the configured threshold. Typical application performance degradation causes might be slow performance of the web server, a slow network, or inefficient application code.

Previous | Next | OK | Cancel | Apply

---

44. Select the **General** tab.

45. Under **Alert Description**, click the **link** to launch Internet Explorer.

Alert Description:

Client Page : /TalkingHeads/Default.aspx is slow at Server Response Time. The configured threshold 1000 ms for TalkingHeads - Production on SCOM01.contoso.com for the transaction Home Page has been exceeded. For additional details please use the following link: http://SCOM01/AppDiagnostics/Pages/login.aspx?m=ev&uid=C3B0D8D2-F863-4E71-A1BC-580D58513E7E

46. When the Windows Internet Explorer Dialog appears, select **Yes** to close the window.

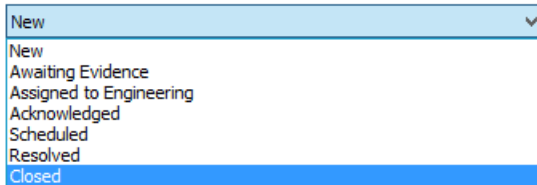47. **Expand** the various components of the event by clicking the plus signs (+) and triangles and review the information. The graph indicates the exact time that it took for each component of this webpage to load. In this example the threshold is set to 1ms as indicated by the red line and text in the lower part of the diagram. On the upper part of the diagram, note the times that it took for the network request to complete for the time to first byte(TTFB) for the time that it took the document. Object model (DOM) to be ready and the time that it took the page to be ready. This has exceeded the preconfigured threshold which resulted in this alert being generated.
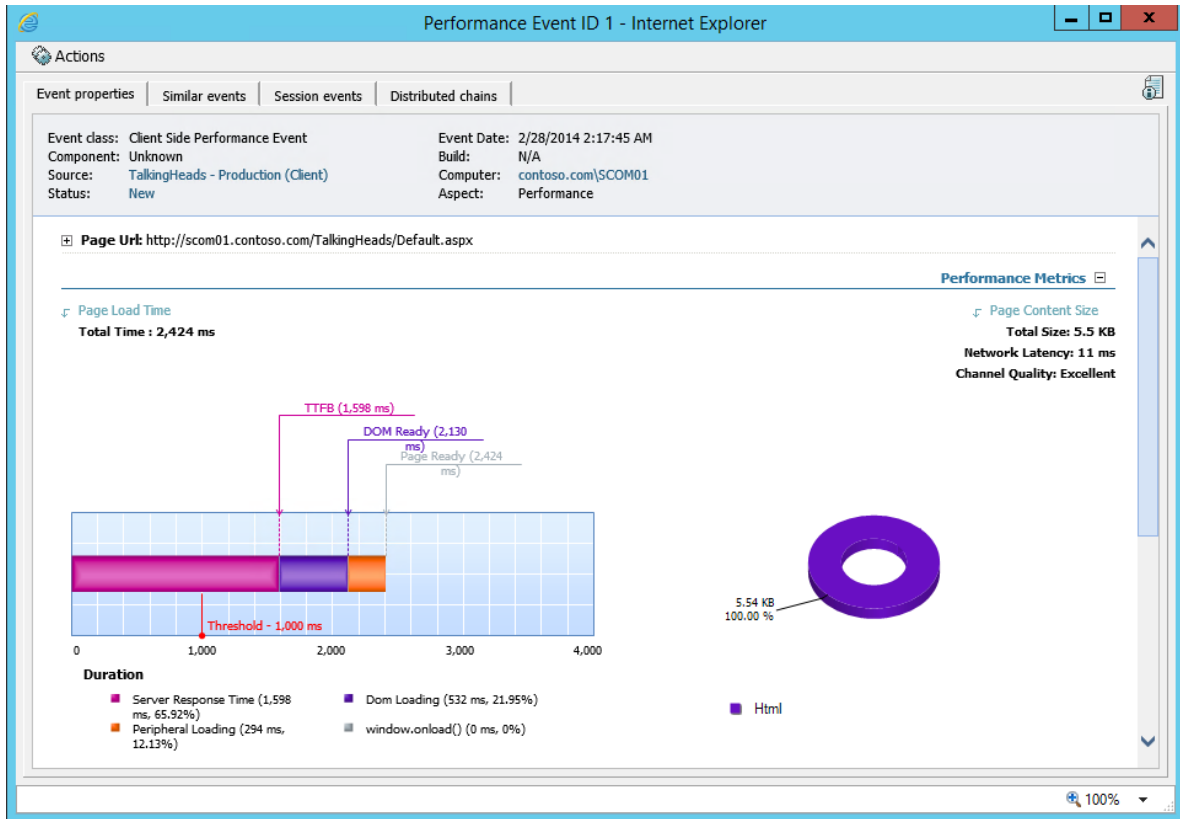
48. **Close** Internet Explorer.

49. After returning to the Alert Properties, under the section labeled **TFS Work Item Owner**, select **Change**.
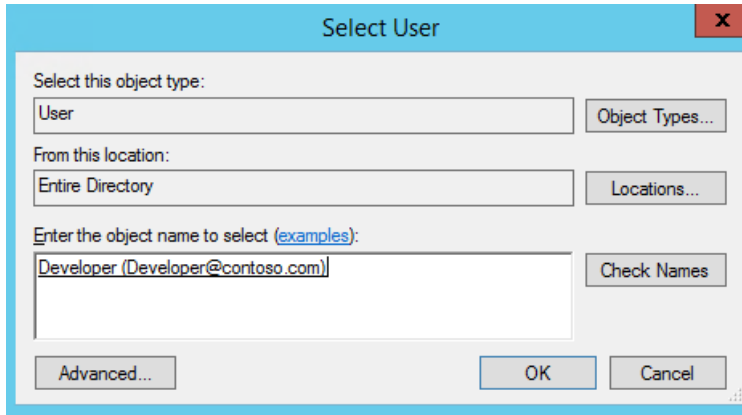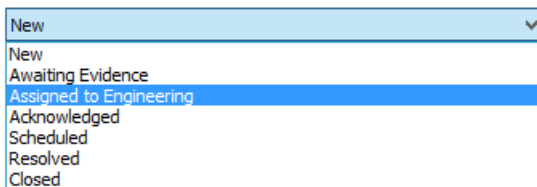

50. On the Select User dialog enter **Developer** and select **Check Names**. Click **OK**.

51. Under **Alert Status**, click the dropdown and select **Assigned to Engineering** and click **OK**. Operations Manage can be connected to Team Foundation Server (TFS) so that any issues which are assigned to developers will appear in their bug database with all the relevant data which can be used to help resolve the issue.

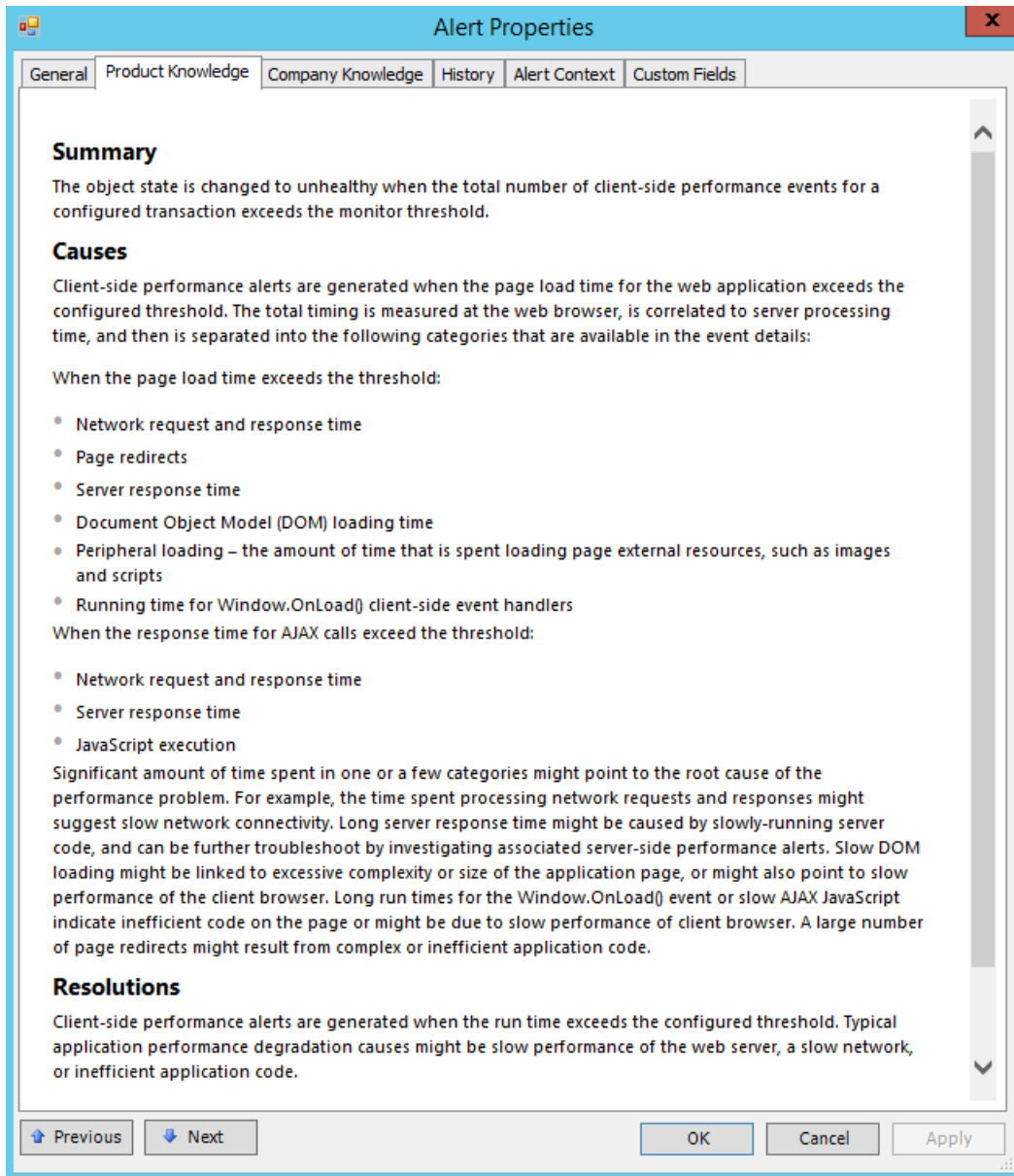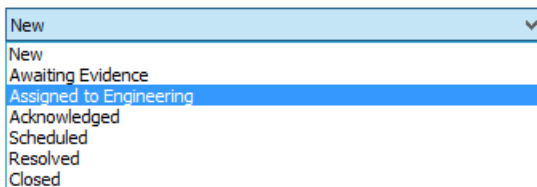52. Click **OK** to close the Alert.

5.5 - SCA & SCOM: Monitor Applications with Advisor

SCA & SCOM: 6.5.1 - Monitor SQL Server

In this exercise System Center Advisor alerts and recommendations about SQL Server 2012 will be viewed through Operations Manager. Advisor is a free cloud service which offers proactive monitoring and best practice recommendations to reduce downtime and resolve issues faster. For more information visit www.SystemCenterAdvisor.com.

Estimated time to complete: 10 minutes

SCOM01

*Perform the following on **SCOM01***

1. From **SCOM01**, open the **Operations Manager Console** by clicking the icon in the taskbar.

2. Navigate to the **Monitoring** workspace.

3. Go to **Monitoring** and then select the folder called **System Center Advisor** and select **Active Alerts**.

4. Select the **Name** column to sort the names by alphabetical order.

5. Select the critical alert which states **SQL Server security configuration does not allow System Center Advisor to function property**. Read the information in this alert. This alert is advising the administrator on how to optimize System Center Advisor so the Advisor service itself can perform better.

6. In the Tasks column under Tasks select **Set Resolution State | Assigned to Engineering**.
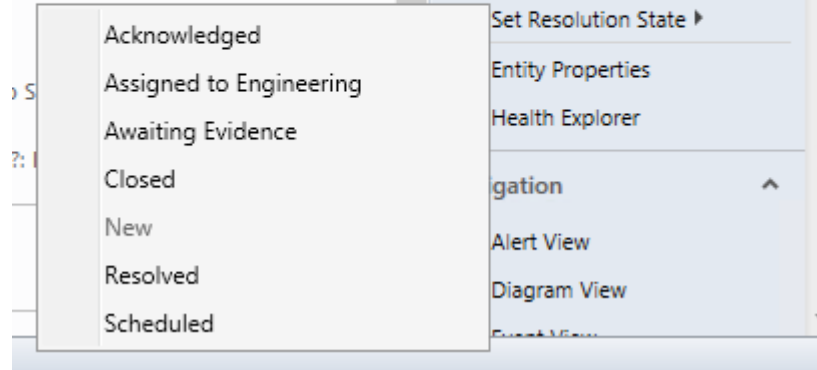
7. Under **Critical Alerts**, select the **Warning** with the name "**SQL Server Database configuration: number of temp db data files might result in blocking.**" In the right column under **Advisor Tasks**, note the option to **View Solution/KB Article**. Selecting this link would open the website, however there is no internet connection so an offline copy of this information will be used instead.

8. Minimize the **Operations Manager Console** window and from the Desktop open the folder named **Advisor Solutions**.

9. Select the webpage file with the identical name **SQL Server database configuration number of tempdb data files might result in blocking.** Open the webpage. Read the information on this webpage as an example of an Advisor best practice. Return to the Operations Manager Console.
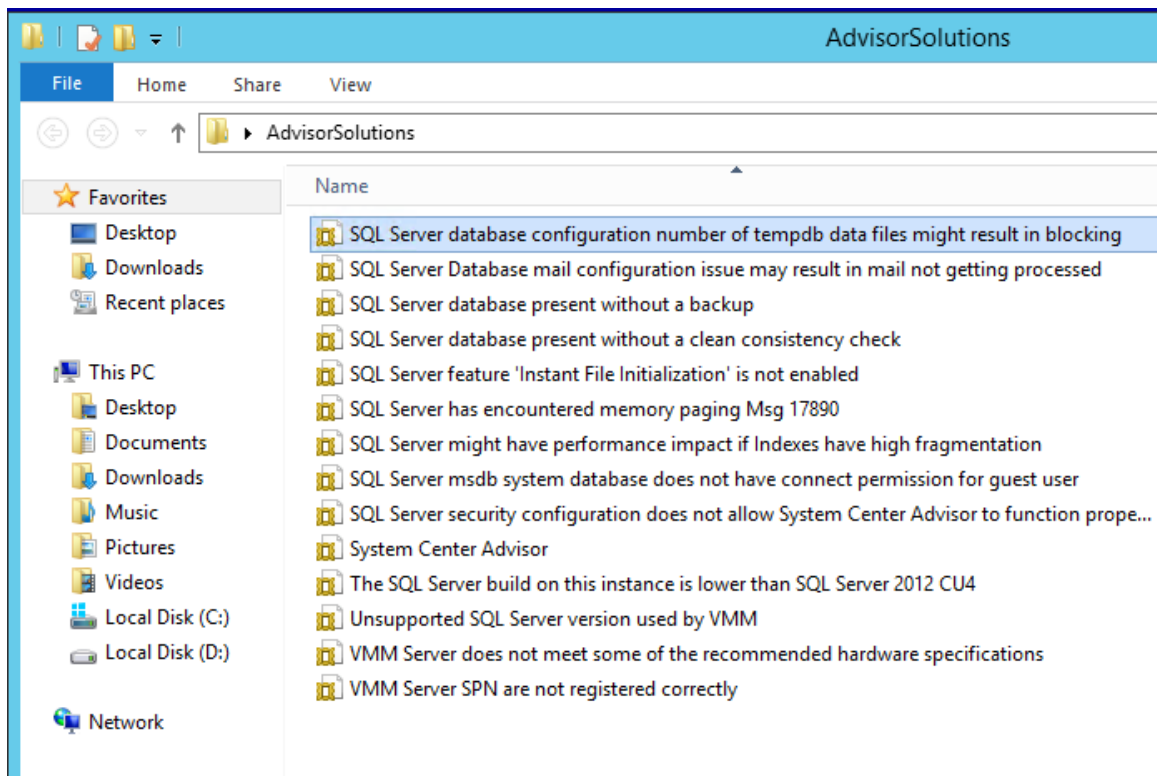
10. Return to the **Operations Manager Console** and with the alert still selected select **Close Alert** from the **Tasks** pane.

11. Select the **Warning** with the name, **"SQL Server database mail configuration issue may result in mail not getting processed."**

Active Alerts (28)

Source	Name
SCOM01.conto...	SQL Server might have performance impact if Indexes
SCOM01.conto...	SQL Server might have performance impact if Indexes
SCOM01.conto...	SQL Server has encountered memory paging: Msg 178!
SCOM01.conto...	SQL Server has encountered memory paging: Msg 178!
SCO01.contoso...	SQL Server feature "Instant File Initialization" is not ena
SCVMM01.cont...	SQL Server feature "Instant File Initialization" is not ena
SCOM01.conto...	SQL Server feature "Instant File Initialization" is not ena
SCDPM01.cont...	SQL Server database present without a clean consisten
SCCM01.conto...	SQL Server database present without a clean consisten
SCDPM01.cont...	SQL Server database present without a backup
SCCM01.conto...	SQL Server database present without a backup
SCDPM01.cont...	SQL Server Database mail configuration issue may resu
SCCM01.conto...	SQL Server Database mail configuration issue may resu
SCDPM01.cont...	SQL Server database configuration: number of tempdb

12. Return to the folder on the Desktop called **Advisor Solutions**.

13. Select the file with the name **SQL Server Database mail configuration issue may result in mail not getting processed.**

14. Open the webpage in **Internet Explorer** and briefly review the information.

15. Return to **Operations Manager.**

16. Under the **Tasks** pane, select **Alert Properties**.

Alert Properties

General | Product Knowledge | Company Knowledge | History | Alert Context | Custom Fields

⚠ SQL Server Database mail configuration issue may result in mail not getting processed.

Key Details:

Alert source:	SCCM01.contoso.com
Severity:	Warning
Priority:	Medium
Age:	39 Days, 16 Hours, 23 Minutes
Repeat Count:	2
TFS Work Item ID:	
TFS Work Item Owner:	
Owner:	[ ] Change...
Ticket ID:	[ ]

Alert Description:

In this SQL Server instance, Advisor detected a configuration issue with DBMail that can prevent DBMail from sending emails. Review the information below and see the KB article for more information.

Path: /MSSQLSERVER
Database Mail Status: false

Alert Status:

Once you have identified the problem and taken corrective action, you can select 'Closed' which will remove the Alert from the system once changes are committed.

[New   ▾]

⬆ Previous   ⬇ Next   OK   Cancel   Apply

17. Under **Owner**, select the **Change** button.

18. In the **Select Use**r dialog, under **Enter the object name to select**, enter **Tier2** and click the **Check Names** button to resolve the object to **Tier2@contoso.com**. Click **OK**.
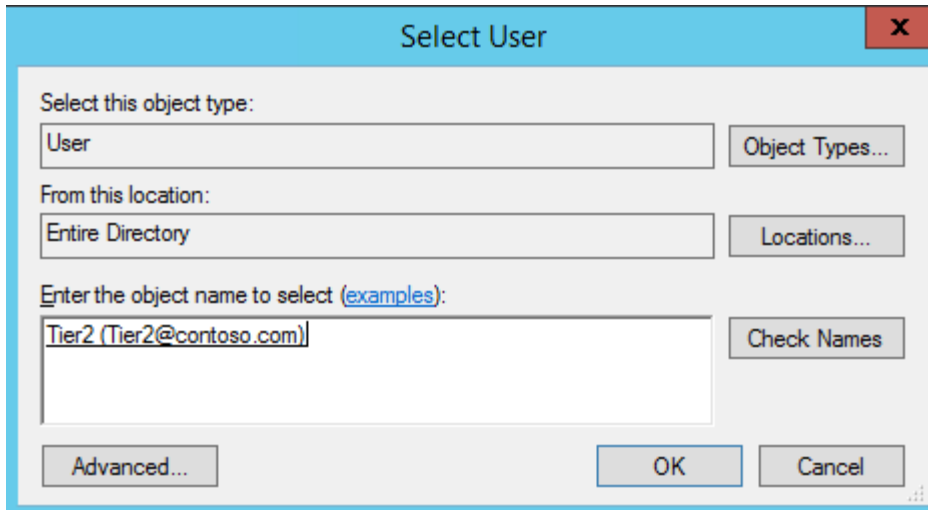
19. Under **Ticket ID** enter **Mail1**

20. Under **Alert Status** in the dropdown, choose **Scheduled**.

Alert Properties

General | Product Knowledge | Company Knowledge | History | Alert Context | Custom Fields

⚠ SQL Server Database mail configuration issue may result in mail not getting processed.

Key Details:

Alert source: SCCM01.contoso.com
Severity: Warning
Priority: Medium
Age: 39 Days, 16 Hours, 23 Minutes
Repeat Count: 2
TFS Work Item ID:
TFS Work Item Owner:
Owner: Tier2@contoso.com [Change...]
Ticket ID: Mail1

Alert Description:

In this SQL Server instance, Advisor detected a configuration issue with DBMail that can prevent DBMail from sending emails. Review the information below and see the KB article for more information.

Path: /MSSQLSERVER
Database Mail Status: false

Alert Status:

Once you have identified the problem and taken corrective action, you can select 'Closed' which will remove the Alert from the system once changes are committed.

Scheduled ▾

⬆ Previous | ⬇ Next | OK | Cancel | Apply

21. Click **OK**.

22. **Select** the warning that says **SQL Server database present without a backup.**

SCCM01.conto...	SQL Server database present without a backup	New	1/10/2014 8:17:36 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server Database mail configuration issue may result in mail not getting processed.	New	1/10/2014 8:11:17 PM	39 Days, 16 Ho...
SCCM01.conto...	SQL Server Database mail configuration issue may result in mail not getting processed.	Scheduled	1/10/2014 8:17:35 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server database configuration: number of tempdb data files might result in blocking	New	1/12/2014 9:31:41 PM	37 Days, 15 Ho...

Alert Details

⚠ SQL Server database present without a backup

Source: SCCM01.contoso.com
Full Path Name: SCCM01.contoso.com\SCCM01.contoso.com
Alert Rule: System Center Advisor Alert
Created: 1/10/2014 8:17:36 PM

Alert Description

A SQL Server database has not been backed up since it was created. Backups are essential to recover from damaged or corrupted database. Without a valid backup, you can lose the data that was stored in the database. Review the database that does not have a backup and set up a maintenance plan to perform backups at regular intervals.

Path: /MSSQLSERVER/CM_HQ1
Database name: CM_HQ1
Database creation time: Jan 4 2014 6:22PM
Time elapsed without a backup: 6

23. Go to the **AdvisorSolutions** folder on the Desktop.

24. **Open** the webpage with the same name, **SQL Server database present without a backup.** This KB article includes best practices and other helpful information to optimize the performance of the SQL database.

25. Return to the **Operations Manager console**.

26. **Select** the warning with the name **SQL Server feature "Instant File Initialization" is not enabled.** Review the information in the details pane under the Alert description. See how this can help optimize the performance of SQL server.

SCO01.contoso...	SQL Server feature "Instant File Initialization" is not enabled	New	1/10/2014 8:14:49 PM	39 Days, 16 Ho...
SCVMM01.cont...	SQL Server feature "Instant File Initialization" is not enabled	New	1/10/2014 8:15:58 PM	39 Days, 16 Ho...
SCOM01.conto...	SQL Server feature "Instant File Initialization" is not enabled	New	1/10/2014 8:17:34 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server database present without a clean consistency check	New	1/10/2014 8:09:23 PM	39 Days, 16 Ho...
SCCM01.conto...	SQL Server database present without a clean consistency check	New	1/10/2014 8:17:36 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server database present without a backup	New	1/10/2014 8:09:22 PM	39 Days, 16 Ho...
SCCM01.conto...	SQL Server database present without a backup	New	1/10/2014 8:17:36 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server Database mail configuration issue may result in mail not getting processed.	New	1/10/2014 8:11:17 PM	39 Days, 16 Ho...
SCCM01.conto...	SQL Server Database mail configuration issue may result in mail not getting processed.	Scheduled	1/10/2014 8:17:35 PM	39 Days, 16 Ho...
SCDPM01.cont...	SQL Server database configuration: number of tempdb data files might result in blocking	New	1/12/2014 9:31:41 PM	37 Days, 15 Ho...

Alert Details

⚠ SQL Server feature "Instant File Initialization" is not enabled

Source: SCO01.contoso.com
Full Path Name: SCO01.contoso.com\SCO01.contoso.com
Alert Rule: System Center Advisor Alert
Created: 1/10/2014 8:14:49 PM

Alert Description

The SQL Server instance is not using the Instant File Initialization feature. When Instant File Initialization is enabled, SQL Server can perform database data file maintenance and creation operations quickly. Without this feature, when SQL Server has to create or grow a file, the new file portion has to be zeroed out before it can be used by SQL Server. This can slow down the file growth or creation operations. This can affect the performance of database creation, database restore and file growth operations. During SQL Server startup, tempdb database creation can take a long time. Note that the SQL Server service startup account needs the user right "perform volume maintenance tasks" to be able to use the Instant File Initialization feature.

Path: /MSSQLSERVER
SQL Server service startup account: CONTOSO\sql
SQL Server service startup account is granted the user right "perform volume maintenance tasks": false
Instant File Initialization is disabled explicitly: false

27. **Browse** several other alerts from Advisor then **navigate** to the folder on the Desktop named **AdvisorSolutions**.

28. Open the webpage with the same name as the alert you chose and review. Use the saved webpages in this folder since there is not an active outbound Internet connection available from within the virtual lab environment.

29. **Close** the **AdvisorSolutions** folder.